GESTIUNEA SECURITĂȚII INFORMAȚIONALE

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 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	-	50	60

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Pentru a atinge obiectivele cursului masteranzii trebuie să posede abilităţi de analiză și testare a soluțiilor informaționale, să cunoască a instala și configura setările necesare, a planifica și a implementa un SMSI. Aceste competenţe sunt formate de următoarele unităţile de curs: Etica profesională și bazele comunicării, Analiza şi proiectarea algoritmilor, Programarea în limbajul C++, Programe malițioase și antivirus, Bazele securității informaționale
Conform competențelor	Explicarea soluțiilor inginerești 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 şi calculator. Nu vor fi tolerate întârzierile, precum şi convorbirile telefonice în timpul cursului.
Practice	Se va perfecta documentul SMSI conform condiţiilor impuse. Termenul de predare a lucrării – o săptămână după finalizarea acesteia. Pentru predarea cu întârziere a lucrării aceasta se depunctează cu 1pct./săptămână de întârziere.

5. Competențe specifice acumulate

Competențe profesionale	**C2 Cercetarea științifica privind aspectele organizaționale și informaționale ale securității** C2.1 Identificarea și definirea conceptelor, teoriilor și metodelor folosite în realizarea de *analize focusate pe protecția oamenilor și informației* privind sistemele ce operează la nivel de organizații C2.2 Explicarea conceptelor și metodelor folosite în realizarea de analize privind sistemele de management și de securitate ce operează la nivel de organizații C2.3 Aplicarea conceptelor, teoriilor și metodelor de bază pentru *pregătirea informațiilor necesare elaborării* SMSI-iurilor care să opereze la nivel de organizații C2.4 Alegerea criteriilor și metodelor de evaluare a calității, performanțelor și limitelor *SMSI-ului* în corespundere cu necesitățile organizației de studiu, inclusiv celor necesare pentru definirea unui sistem de management al calității și securității C2.5 Elaborarea unui proiect (specificație de sistem) în condițiile existenței unui sistem de management al calității și securității. **C3 Modelarea sistemelor complexe de securitate şi implementarea lor prin sisteme informatice** C3.1 Identificarea și definirea conceptelor, procedeelor și metodelor de securitate a informației folosite în realizarea *măsurilor de control ce reies din necesități* ale activității umane C3.2 Explicarea tehnologiilor potrivite pentru realizarea sistemelor de securitate necesare în activitățile organizațiilor C3.3 Utilizarea tehnologiilor moderne în definirea soluțiilor de securitate C3.4 Utilizarea de criterii și metode determinate de tehnologii pentru evaluarea conformității cu

	standardele de interoperabilitate C3.5 Dezvoltarea măsurilor de control și securitate utilizând tehnologii moderne de transmitere, stocare și procesare date în corespundere cu necesitățile unei organizații **C5 Managementul sistemelor de securitate în concordanța cu cerințele pieței** C5.1 Identificarea și definirea de componente arhitecturale hardware, software și de comunicații, precum și celor necesare la *descrierea obiectivelor sistemului de management al SI* C5.2 Explicarea interacțiunii și funcționării componentelor arhitecturale și de infrastructură specifice domeniului securității C5.4 Utilizarea de criterii și metode de *evaluare a caracteristicilor funcționale și nefuncționale ale componentelor* sistemului de management al securității C5.5 Implementarea unui SMSI în baza unor constrângeri enunțate de proiectele din domeniul securității
Competenţe 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 și a securității informaționale.
Obiectivele specifice	Prezentarea aspectelor teoretice şi practice ale unui sistem de menagement al securității informaționale. Dezvoltarea capacității de analiză, comparare și de descriere a elementelor SMSI. Evaluarea corecta a amenințărilor și vulnerabilităților unui sistem informațional. Planificarea, implementarea, revizuirea și îmbunătățirea SMSI-ului. Crearea documentului SMSI

7. Conținutul disciplinei/modulului

Tematica activităților didactice	**Numărul de ore învățământ cu frecvență**
Tematica cursurilor	
T1. Cadrul de management al securităţii informaţiei Sistemul integrat de management. Standarde internaţionale în domeniu: familia de standarde ISO 27000, NIST, PCI DSS. Relaţia între standarde şi aplicabilitatea lor.	**2**
T2. Sistemul de Management al Securității Informației Componentele și mecanismele unui SMSI. Etapele procesului de implementare a SMSI conform ISO 27001. Controale de securitate ISO 27002, CIS Controls.	**4**
T3. Analiza şi evaluarea riscurilor de securitate Noțiuni generale privind managementul riscurilor securității informațieionale. Inventarierea activelor. Amenințări și vulnerabilități. Etapele procesului de analiză şi evaluare riscuri conform ISO 27005. Evaluarea cantitativă și calitativă.	**4**
T4. Metodologii și instrumente de analiza a riscurilor informaționale Metodologia Microsoft. Metodologia CRAMM. Metodologia MEHARI. Metodologia Ebios. Metodologia Octave. Metodologia IT- Grundschutz. Instrumentele Ebios, GSTool, Grif, RiskWatch, Cramm.	**4**
T5. Legislația aplicabilă Managementul securității informaționale la nivel de stat: principii generale. Metodologii de management al riscurilor informaționale utilizate de infrastructura locală.	**2**
T6. Programe de securitate, modele, politici și proceduri Modele de securitate multinivel și multilaterale. Modele de politici de securitate. Exemple de politici de securitate. Aspecte practice ale politicii de securitate. Recomandări de dezvoltare a diferitelor componente ale politicilor de securitate conform SANS	**4**
Total curs:	**20**
Tematica lucrărilor practice	
LP1. Sistemul de management al securității informației. Contextul organizației. Definirea scopului și perimetrelor de securitate pentru SMSI	2
LP2. Politici și proceduri de securitate. Documentarea Sistemului de management al securității informaționale	2
LP3. Evaluarea conformitatilor dupa diferite norme si standarde. Declarația de aplicabilitate ISO 27002, CIS Controls.	2
LP4. Managementul activelor. Inventarierea activelor și stabilirea interdependenţei lor. Clasificarea activelor. Nomenclatorul activelor	4

Tematica activităților didactice	Numărul de ore învățământ cu frecvență
LP5. Managementul vulnerabilităților și identificarea amenințărilor. Nomenclatorul amenințărilor și vulnerabilităților	4
LP6. Managementul riscurilor informaționale. Determinarea impactului și probabilității riscurilor informaționale. Evaluarea riscurilor informaționale. Nomenclatorul riscurilor informaționale	2
LP7 Tratarea riscurilor informaționale. Identificarea și selectarea măsurilor de control. Eaborarea planului de tratare a riscurlor identificate.	4
Total lucrări practice:	**20**

8. Referințe bibliografice

Principale	1. Mark Stamp, *Information security. Principles and Practice,* Second Edition, SanJose State University, AJOHN WILEY&SONS, USA, 2011. - 608 p. 2. Aurel Şerb, Constantin Baron, Narcisa Isăilă, *Securitatea informatică în societatea informaţională*, Bucureşti : Pro Universitaria, 2013. – 546 p. 3. Dumitru Oprea, *Protecţia şi securitatea informaţiilor*. Ed. II, Polirom, Iaşi, 2007. – 445 p. 4. Popa Sorin Eugen, Securitatea sistemelor informatice, Bacău, 2007. – 136 p. 5. Ion I. Bucur, *Tehnologii, structuri și managementul rețelelor de calculatoare,* - resursă electronică. 6. Al. Astahov, *Искусство управления информационными рисками*, ДМК, Москва, 2010. – 316 p. 7. Nicolas Mayer, *Model-based Management of Information System Security Risk*, Namur, Belgium, 2009. – 295 p. 8. M.E. Whitman, H.J.Mattord, *Management of Information Security*, 3rd Edition, Course Technology, 2010. 9. A.Calder, S.Watkins, *A Manager's Guide to Data Security and ISO 27001/ISO27002*, 4th Edition, Kogan Page, 2008. 10. D.Landool, *The Security Risk Assessment Handbook*, Auerbach Publications, 2006. 11. HOTĂRÎRE GUVERN Nr. 201 din 28.03.2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică. Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărîrea Guvernului nr. 811 din 29 octombrie 2015.
Suplimentare	1. NIST, NIST 800-30 Risc Management Guide for Information Technology Systems, http://www.csrc.nist.gov/publications 2. OECD, *Guidelines for the Security of Information Systems and Networks — Towards a Culture of Security. Paris: OECD, July2002.* www.oecd.org http://www.isaca.org/cobit/

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 1-3	Test electronic pe platforma else.fcim.utm.md	100%	**15%**
Evaluare periodică II	Conținut teoretic Teme 4-6	Test electronic pe platforma else.fcim.utm.md	100%	**15%**
Evaluare curentă	Participare, lucrări practice, rapoarte	Participarea la activități, calitatea și acuratețea realizării lucrărilor practice, pregătirea și susținerea rapoartelor	100%	**15%**
Studiul individual	Prezentarea unui articol științific	Prezentare orală/discurs la tema articolului în fața colegilor; evaluarea coerenței, clarității și documentării	100%	**15%**
Evaluarea finală	Conținut teoretic și practic	Test electronic pe platforma else.fcim.utm.md	100%	**40%**