AUDITUL 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	-	60	50

3. Precondiții de acces la disciplină/modul

Conform planului de învățământ	Etica profesională și bazele comunicării, Programe malițioase și antivirus, Bazele securității informaționale, Managementul securității informaționale, Cadrul organizațional-legal al securității informaționale, Rețele de calculatoare
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 vor perfecta rapoarte conform condiţiilor impuse de indicaţiile metodice. 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 metodelor folosite în realizarea Auditului securității informaționale privind sistemele ce operează la nivel de organizații C2.2 Explicarea conceptelor, teoriilor și metodelor folosite în realizarea Auditului sistemelor ce operează la nivel de organizații C2.3 Aplicarea conceptelor, teoriilor și metodelor de bază pentru *pregătirea chestionarelor necesare elaborării* Auditului sistemelor de securitate care să opereze la nivel de organizații C2.4 Alegerea criteriilor și metodelor de evaluare a calității, performanțelor și limitelor *sistemelor de securitate* în corespundere cu necesitățile organizației de studiu C2.5 Elaborarea Raportului de audit în condițiile existenței unui sistem de management al calității și securității. **C3 Modelarea sistemelor complexe de securitate și implementarea lor prin sisteme informatice** C3.2 Explicarea tehnologiilor potrivite pentru realizarea Auditurilor sistemelor de securitate necesare în activitățile organizațiilor C3.3 Utilizarea tehnologiilor moderne în definirea Auditurilor de securitate C3.4 Utilizarea de criterii și metode determinate de tehnologii pentru evaluarea conformității cu standardele de interoperabilitate C3.5 Dezvoltarea Auditurilor de securitate privind tehnologiile 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 la realizarea Auditului de securitate C5.2 Explicarea interacțiunii și funcționării componentelor la realizarea Auditului în domeniul securității

	C5.3 Aplicarea metodelor de bază pentru specificarea de soluții privind probleme tipice de securitate C5.4 Utilizarea de criterii și metode de *evaluare rezultatelor Auditului* și generarea rapoartelor de Audit C5.5 Recomandarea soluțiilor arhitecturale și de infrastructură în baza unor constrângeri enunțate de Raportul de Audit din domeniul securității
Competenţe transversale	**CT1.** Comportarea onorabilă, responsabilă, etică, în spiritul legii, pentru a asigura reputația profesiei

6. Obiectivele disciplinei/modulului

Obiectivul general	Asigurarea unui anumit nivel de cunoștințe teoretice și practice necesare pentru ca specialiștii programului "Securitate informațională" să poată evalua starea securității informaționale în cadrul organizației
Obiectivele specifice	Prezentarea aspectelor teoretice şi practice ale unui audit în domeniul securității informaționale. Dezvoltarea capacității de analiză, comparare și de descriere a unor fenomene din perspectiva auditării securității informaționale. Evaluarea corecta a amenințărilor și vulnerabilităților unui sistem informațional. Dobândirea de cunoștințe privind securitatea informațională. Dobândirea de cunoștințe privind auditarea securității informaționale. Planificarea, petrecerea și închiderea unui audit. Crearea raportului de audit.

7. Conținutul disciplinei/modulului

Tematica activităților didactice	**Numărul de ore învățământ cu frecvență**
Tematica cursurilor	
T1. Cadrul conceptual general. Definiția, scopul, destinația și locul ASI ca serviciu universal pentru creșterea nivelului securității companiei. Succint istoric. Tipuri de ASI: *intern* și *extern, audit activ, audit expert, audit privind conformitatea cu standardele.* Frecvența ASI.	**4**
T2. Cadrul normativ internațional de referință. Standardul internațional de audit ISO 27001. COBIT. ITIL. ISACA. Cadrul național și intern de referință. Legislația Republicii Moldova în domeniul auditului. Regulamente și instrucțiuni interne	**4**
T3. Metode și instrumente pentru efectuarea auditului securității informațiilor. Liste de verificare, machete și chestionare. Documentare și certificare.	**4**
T4. Cadrul procedural de evaluare a securității informaționale a diferitelor active informatice și resurse informaționale. Proceduri de audit a securității echipamentelor, suporturilor de date, a datelor, a aplicațiilor informatice, a rețelelor/comunicațiilor interne, a securității web și atacurilor externe de pe Internet	**4**
T5. Cadrul procedural de evaluare a securității informaționale a diferitelor active informatice și resurse informaționale. Proceduri de audit a securității echipamentelor, suporturilor de date, a datelor, a aplicațiilor informatice, a rețelelor/comunicațiilor interne, a securității web și atacurilor externe de pe Internet	**4**
Total curs:	**20**
Tematica lucrărilor practice	
LP1. Studiu de caz 1. Explorarea unor proceduri de audit a diferitelor resurse informaționale/active informatice	**4**
LP2. Studiu de caz 2. Realizarea auditului securității IT	**4**
LP3. Studiu de caz 3. Auditul/controlul securității unui sistem informatic	**4**
LP4. Studiu de caz 4. Realizarea ASI pentru un obiect ipotetic	**8**
Total lucrări practice:	**20**

8. Referinţe bibliografice

Principale	1. Mark Stamp, *Information security. Principles and Practice,* Second Edition, SanJose State University, AJOHN WILEY&SONS, USA, 2011. - 608 p. 2. Luminița Scripcariu, Ion Bogdan etc., *Securitatea rețelelor de comunicații*, Casa de editură Venus, Iași, 2008. - 193 p. 3. Al. Astahov, *Искусство управления информационными рисками*, ДМК, Москва, 2010. – 316 p. 4. M.E. Whitman, H.J.Mattord, *Management of Information Security*, 3rd Edition, Course Technology, 2010. 5. A.Calder, S.Watkins, *A Manager's Guide to Data Security and ISO 27001/ISO27002*, 4th Edition, Kogan Page, 2008. 6. C.A.F.R., Audit financiar 2006 – Standarde. Codul privind conduita etică şi profesională, 2006. 7. GAO, Government Auditing Standards, GAO, United States Government Accountability Office, by

	the Comptroller General of the United States, July 2007 Revision
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**				
Învăţământ cu frecvenţă					
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. Demonstrarea în lucrarea de examinare finală a cunoaşterii condiţiilor de aplicare a procedeelor de modelare constructivă.					

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 3-5	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%**