MD-2068, CHIŞINĂU, STR. STUDENŢILOR, 9/7, TEL: 022 50-99-63, www.utm.md

MANAGEMENTUL SECURITĂȚII INFORMAȚIONALE

1. Date despre unitatea de curs

Facultatea	Calculatoare, Informatică și Microelectronică				
Catedra/Departamentul	Ingineria Software și Automatică				
Ciclul de studii	Studii superioare de licenţă, ciclul II				
Programul de studii	Tehnologia informației pentru afaceri				
Anul de studii	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
II (învățământ cu frecvență);	3	E-examen	S – unitate de curs de specialitate	A - unitate de curs opțională	5

2. Timpul total estimat

Total ore în planul de învăţământ	**Din care**				
	Ore auditoriale		**Lucrul individual**		
	Curs	**practice**	**Proiect de an**	**Studiul materialului teoretic**	**Pregătire aplicaţii**
150	20	20	-	110	-

3. Precondiţii de acces la unitatea de curs

Conform planului de învăţământ	Etica profesională și bazele comunicării, Bazele securității informaționale
Conform competenţelor	Explicarea soluțiilor prin utilizarea conceptelor, metodologiilor și principiilor din științele aplicative

4. Condiţii de desfăşurare a procesului educaţional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector și calculator
Laborator/Seminar	Se vor prezenta etapele SMSI conform condițiilor impuse

5. Competenţe specifice acumulate

Competenţe profesionale	C1 Operarea cu concepte și metode ale domeniului Tehnologiei Informației C2 Aspecte organizaționale și informaționale ale sistemelor C5 Managementul produselor și al serviciilor TIC în concordanța cu cerințele pieței
Competenţe transversale	CT1. Aplicarea principiilor, normelor și valorilor eticii profesionale CT2. Identificarea, descrierea și derularea activităților organizate într-o echipă cu dezvoltarea capacităților de comunicare și colaborare, dar și cu asumarea diferitelor roluri (de execuție și conducere) CT3. Demonstrarea spiritului de inițiativă și acțiune pentru actualizarea propriilor cunoștințe profesionale, economice și de cultura organizațională

6. Obiectivele unităţii de curs

Obiectivul general	Însușirea conceptelor, metodelor și politicilor de gestionare a riscurilor informaționale
Obiectivele specifice	Să înțeleagă și să descrie componentele sistemului de management al securităţii 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. Conţinutul unităţii de curs

Tematica cursului	Nr. ore învăţământ cu frecvenţă
1. Cadrul de management al securităţii informaţiei Noţiuni şi concepte de bază. Standarde internaţionale în domeniu: familia de standarde ISO 27000, NIST, PCI DSS. Relaţia între standarde şi aplicabilitatea lor.	4
2. 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
3. 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
4. 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
5. Legislaţia aplicabilă. Programe de securitate, modele, politici și proceduri. Managementul securității informaționale la nivel de stat: principii generale. Metodologii de management al riscurilor informaționale utilizate de infrastructura locală. 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 ore curs:	**20**
Tematica lucrărilor de laborator/seminarelor	
1. Sistemul de management al securității informației. Contextul organizației. Definirea scopului și perimetrelor de securitate pentru SMSI. Declarația de aplicabilitate ISO 27002, CIS Controls. Intsrumente informatice de conformitate (MSAT, Condor)	4
2. Managementul activelor. Managementul vulnerabilităților și identificarea amenințărilor. Inventarierea activelor și stabilirea interdependenţei lor. Clasificarea activelor. Nomenclatorul activelor. Nomenclatorul amenințărilor şi vulnerabilităţilor	4
3. Managementul riscurilor informaționale. Determinarea impactului și probabilităţii riscurilor informaționale. Evaluarea riscurilor informaționale. Nomenclatorul riscurilor informaționale	4
4. Tratarea riscurilor informaționale. Identificarea şi selectarea măsurilor de control. Eaborarea planului de tratare a riscurlor identificate.	4
5. Sistemul de management al securității informației. Documentarea Sistemului de management al securității informaționale. Monitorizarea. Revizuirea. Îmbunatațirea. Optimizare.	4
Total ore practice:	**20**

8. Referinţe bibliografice

Principale	1. Al. Astahov, *Искусство управления информационными рисками*, ДМК, Москва, 2010. – 316 p. 2. Nicolas Mayer, *Model-based Management of Information System Security Risk*, Namur, Belgium, 2009. – 295 p. 3. M.E. Whitman, H.J.Mattord, *Management of Information Security*, 3rd Edition, Course Technology, 2010. 4. A.Calder, S.Watkins, *A Manager's Guide to Data Security and ISO 27001/ISO27002*, 4th Edition, Kogan Page, 2008. 5. D.Landool, *The Security Risk Assessment Handbook*, Auerbach Publications, 2006.
Suplimentare	1. Benjamin Graham, David L. Dodd, Security analysis. Principles and Technique, Sixth Edition, Columbia University, The McGraw-Hill Companies, 2009. – 818 p. 2. Familia de standarde ISO 2700k – Sistemul de management al securității informaționale.

9. Evaluare

Periodică		Curentă	Studiu individual	Proiect/teză	Examen
EP 1	EP 2				
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
Evaluare periodică I	Conținut teoretic, teme 1-2	Test pe MOODLE	100%	**10%**
Evaluare periodică II	Conținut teoretic, teme 3-5	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	Teme individuale	Prezentare/discurs public	100%	**30%**
Evaluarea finală	Conținut teoretic și practic	Test pe MOODLE. Notare conform baremului	100%	**40%**