MD-2045, CHIȘINĂU, STR. STUDENȚILOR, 7/9, TEL: 022 50-99-01 | FAX: 022 50-99-05, www.utm.md

TEHNOLOGII ALE SECURITĂȚII INFORMAȚIONALE

1. Date despre unitatea de curs/modul

Facultatea	Calculatoare, Informatică și Microelectronică				
Catedra/departamentul	Informatică și Ingineria Sistemelor				
Ciclul de studii	Studii superioare de licenţă, ciclul I				
Programul de studiu	**0612.2 Managementul informației**				
Anul de studiu	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opționalitate**	**Credite ECTS**
I (învăţământ cu frecvenţă);	4	E	S – unitate de curs de specialitate	A - unitate de curs la alegeri	4

2. Timpul total estimat

Total ore în planul de învăţământ	Din care				
	Ore auditoriale		Lucrul individual		
	Curs	Laborator/seminar	Proiect de an	Studiul materialului teoretic	Pregătire aplicaţii
120	30	30		30	30

3. Precondiţii de acces la unitatea de curs/modul

Conform planului de învăţământ	Matematici speciale și matematica computațională, Programarea calculatoarelor, Structuri de date si algoritmi, Programare procedurală, Programare interactivă
Conform competenţelor	Informarea studenţilor cu cele mai noi probleme privind securitatea şi protecţia informaţiei cât şi cu utilizarea celor mai noi metode de protecţie

4. Condiţii de desfăşurare a procesului educaţional pentru

Curs	Pentru prezentarea materialului teoretic în sala de curs este nevoie de proiector şi calculator. Nu vor fi tolerate întârzierile studenţilor, precum şi convorbirile telefonice în timpul cursului.
Laborator/seminar	Studenţii vor perfecta rapoarte conform condițiilor impuse de indicaţiile metodice. Termenul de predare a lucrării de laborator – o săptămână după finalizarea acesteia. Pentru predarea cu întârziere a lucrării aceasta se depunctează cu 1pct./săptămână de întârziere.

5. Competenţe specifice acumulate

In conformitate cu grila și matricea de corelare a programului de studii vor fi acumulate următoarele competențe:

CP1. Managementul nivelului de servicii

K1 Documentația SLA (Service Level agreement).
K2 Cum se compară și se interpreteze datele de management.
K3 Elementele care formează matricea acordurilor la nivel de servicii.
K4 Cum funcționează infrastructurile de furnizare a serviciilor.
K5 Impactul nerespectării nivelului de serviciu asupra performanței afacerii.
K6 Standardele de securitate în TIC.
K7 Standardele privind calitatea

CP2. Proiectarea și dezvoltarea aplicațiilor

K1 Programe/module software adecvate.
K2 Componente hardware, instrumente și arhitecturi hardware.
K3 Proiectarea funcțională și tehnică.
K4 Tehnologiile de ultimă oră.
K5 Limbaje de programare.
K6 Baze de date (DBMS).
K7 Sisteme de operare și platforme software.
K8 Mediul de dezvoltare integrat (IDE - integrated development environment).
K9 Dezvoltarea rapidă a aplicațiilor.
K10 Problemele legate de drepturile de proprietate intelectuală (IPR).
K11 Tehnologia de modelare tehnică și limbaje.
K12 Limbajele de definire a interfeței (IDL).
K13 Probleme de securitate

CP3. Integrarea componentelor

K1 Componente/module hardware/software, indiferent dacă sunt vechi, existente sau noi.
K2 Impactul integrării unui sistem asupra organizației sau a sistemului existent.
K3 Tehnici de interfațare între module, sisteme și componente.
K4 Tehnici de testare a integrării.
K5 Instrumentele de dezvoltare (ex. mediul de dezvoltare, gestionare, control al modificărilor și accesul la codul sursă).
K6 Bune practici de design

CP5. Furnizarea de servicii

K1 Modul de interpretare a cerințelor privind prestarea de servicii IT.
K2 Cele mai bune practici și standarde pentru prestarea serviciilor informatice.
K3 Metodele și modul de control al prestării de servicii.
K4 Metode de înregistrare a prestării de servicii și detectare a defecțiunilor.
K5 Cele mai bune practici, norme și standarde în gestionarea securității informației.
K6 Specificul tehnologiilor legate de web, cloud și instrumente mobile.

CP6. Managementul informațiilor și a cunoștințelor

K1 Metodele de analiză a informațiilor și a proceselor de business.
K2 Dispozitive și instrumente informatice aplicabile pentru stocarea și recuperarea datelor.
K3 Provocările legate de dimensiunea masivelor de date (Big Data).
K4 Provocările legate de date nestructurate (de exemplu, Data Analytics)

6. Obiectivele unităţii de curs/modulului

Obiectivul general	Studierea problemelor privind securitatea şi protecţia informaţiei cât şi obținerea abilități de utiliza celor mai noi metode de protecţie.
Obiectivele specifice	Să înţeleagă şi să descrie metodele și tehnici de securitate. Să cunoască sisteme și algoritmi de criptare/decriptare Să selecteze procedee adecvate pentru elaborarea și analiza a modelului de securitate.

7. Conţinutul unităţii de curs/modulului

Tematica activităţilor didactice	Numărul de ore	
	învăţământ cu frecvenţă	învăţământ cu frecvenţă redusă
Tematica prelegerilor		
T1. Securitatea informației. Noțiuni și definiții de baza. Amenințări și atacuri. Riscul de securitate. Bresele de securitate. Metode de asigurarea a integrității informației.	6	
T2. Date cu caracter personal. Date instituționale. Tipuri de atacatori. Război cibernetic.	2	
T3. Protejarea datelor și a confidenţialităţii on-line. Protejarea instituțiilor.	4	
T4. Cubul de securitate cibernetica. Triada CIA. Stările datelor și semnificațiile lor, Steganografia ca metoda de ascundere a informatiei	4	
T5. Clase și tipuri de atacuri . Controlul accesului în sistemele informatice. Modele de securitate.	2	
T6. Securitatea informației şi criptografia. Sisteme de criptare. Principiul Kerckhoff. Clasificarea algoritmilor de criptare. Cifruri de substituție și cifruri cu permutare/transpoziție. Cifruri clasice. Atacuri criptanalitice	4	
T7. Critografie moderna. Cifruri simetrice și asimetrice. Schimbul de chei Diifie-Helman. Cifruri simetrice DES și AES. Critografie asimentrica: cifrul RSA	6	
T8.Semnătura electronica Infrastructura cu chei publice PKI. Certificate digitale.	4	
Total prelegeri:	**30**	

Tematica activităţilor didactice	Numărul de ore	
	învăţământ cu frecvenţă	învăţământ cu frecvenţă redusă
Tematica lucrărilor de laborator		
LL1. Controlul a integrității datelor cu ajutorul funcțiilor hash	2	
LL2. Brețele de securitate.	2	
LL3.Reguli de creare a parolelor puternice	2	

LL4. Crearea și gestionarea copiilor de rezerva	2	
LL5. Asigurarea securității datelor stocate on-line	2	
LL6. Detectarea comportamentul online riscant	2	
LL7. Cifruri monoalfabetice	2	
LL8. Criptanaliza cifrurilor monoalfabetice	2	
LL9. Cifruri polialfabetice	4	
LL10. Cifrul RSA	4	
LL11. Semnătura digitala	6	
Total lucrări de laborator:	**30**	

8. Referinţe bibliografice

Principale	1. Gutmann, P., Cryptography and Data Security, http://www.cs.auckland.ac.nz/apgut001. 2. Bellovin, S.M., Security Problems in the TCP/IP Protocol Suite, AT&T Bell Lab. Murray Hill, New Jersey, 07974, 2002. 3. Fergusson, N., Schneier, B., A Cryptografic Evaluation of IP sec., http://www.counterpaine.com, 2000. 4. Gligorovski, D., Markovski, S., Kocarev, L., New Directions in Coding: From Statistical Physics to Quasigroup String Transformation, NOLTA 2004, Japan, Nov 29-Dec 3, 2004
Suplimentare	1. Dimovski, A., Gligorovski, D., Attacks on the Polyalphabetic Substitution Cipher Using a Parallel Genetic Algorithm, Tech. Rep. SCOPES project, March 2003, Ohoid, Macedonia 2. Dimovski, A., Gligorovski, D., Attacks on the Transposition Cipher Using Optimization Heuristics, Proc. Of ICEST 2003, Oct 2003, Sofia, Bulgaria

9. Evaluare

Forma de învățământ	Periodică		Curentă	Lucrul individual	Examen final
	Atestarea 1	Atestarea 2			
Cu frecvență	15%	15%	15%	15%	40%
Standard minim de performanţă					
Prezenţa şi activitatea la prelegeri şi lucrări de laborator Obţinerea notei minime de „5” la fiecare dintre evaluări şi lucrări de laborator					