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

TEHNOLOGII ALE SECURITĂȚII INFORMAȚIONALE

1. Date despre disciplină

Facultatea	Calculatoare, Informatică şi Microelectronică				
Catedra/departamentul	Informatică şi Ingineria Sistemelor				
Ciclul de studii	Studii superioare de licenţă, ciclul I				
Programul de studiu	***0613.5 Informatica Aplicată***				
Anul de studiu	**Semestrul**	**Tip de evaluare**	**Categoria formativă**	**Categoria de opţionalitate**	**Credite ECTS**
II (învăţământ cu frecvenţă);	4	E	D – unitate de curs de specialitate	O - unitate de curs obligatorie	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 disciplină

Conform planului de învăţământ	Analiză matematică, Matematică discretă, 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

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

CPL 1. Proiectarea aplicațiilor (A6)**

K1 Tehnici de modelare a cerințelor și tehnici de analiză a nevoilor.
K2 Metodele de dezvoltare a software-ului și argumentarea acestora (de exemplu, prototipuri, metode agile, retroinginerie etc.).
K3 Metricile care se referă la dezvoltarea aplicațiilor.
K4 Principiile de proiectare a interfeței pentru utilizator.
K5 Limbajele pentru formalizarea specificațiilor funcționale.
K6 Aplicațiile existente și arhitectura lor aferentă.
K7 Sisteme de gestionare a bazelor de date (DBMS), depozite de date, informaţii de business etc.
K8 Tehnologiile mobile

CPL 2. Proiectarea și dezvoltarea aplicațiilor (B.1)

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.

CPL 4. Testarea aplicațiilor (B.3)

K1 Tehnicile, infrastructura și instrumentele necesare utilizate în procesul de testare.
K2 Ciclul de viață al unui proces de testare.
K3 tipurile de teste (funcțional, de integrare, performanță, utilizabilitate, sarcină etc.).
K4 Standardele naționale și internaționale care definesc criteriile de calitate pentru testare.
K5 specificul tehnologiilor legate de web, cloud, instrumente mobile și de probleme de mediu.

6. Obiectivele disciplinei

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 disciplinei

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 și 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 lucrărilor de laborator		
LL1. Controlul a integrității datelor cu ajutorul funcțiilor hash	2	
LL2. Breșele 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. 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 competenților profesionale.

10. Evaluare

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