MD-2045, CHIŞINĂU, str. STUDENŢILOR, 9/7, TEL: 022 50-99-08 www.utm.md

CRIPTOGRAFIE ŞI SECURITATE

1. Date despre unitatea de curs/modul

Facultatea	Calculatoare, Informatică și Microelectronică				
Catedra/departamentul	Ingineria Software și Automatică				
Ciclul de studii	Studii superioare de licență, ciclul I				
Programul de studiu	0613.3 Ingineria software				
Anul de studiu	Semestrul	Tip de evaluare	Categoria formativă	Categoria de opționalitate	Credite ECTS
III (învățământ cu frecvență)	5	E	S – unitate de curs de specialitate	O - unitate de curs obligatorie	5

2. Timpul total estimat

Total ore în planul de învățământ	Din care				
	Ore auditoriale		Lucrul individu al		
	Curs	Laborator/seminar	Proiect de an	Studiul materialului teoretic	Pregătire aplicații
120	30	30/15	-	30	30

3. Precondiții de acces la unitatea de curs/modul

Conform planului de învățământ	Matematica superioară, Matematica discretă, Structuri de date şi algoritmi, Analiza şi proiectarea algoritmilor, Programarea în limbajul C++
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 și calculator. Nu vor fi tolerate întârzierile studenților, precum și convorbirile telefonice în timpul cursului.
Laborator/seminar	Studenții vor perfecta rapoarte conform condițiilor impuse de indicațiile 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. Competențe specifice acumulate

Competențe profesionale	**C1 Privind fundamentele științifice și inginerești ale tehnologiilor informaționale** • Identificarea și definirea conceptelor, teoriilor și metodelor de științe fundamentale și aplicative suport pentru ingineria tehnologiilor informaționale. • Explicarea soluțiilor inginerești prin utilizarea tehnicilor, conceptelor și principiilor din științele exacte și aplicative . • Rezolvarea prob-lor din domenii de activitate umană prin aplicarea în special al tehnicilor și metodelor de calcul numeric . • Alegerea criteriilor și metodelor pentru analiza avantajelor și dezavantajelor metodelor și procedeelor aplicate la soluționarea problemelor de calcul numeric. • Modelarea unor probleme tip din științele aplicative folosind aparatul matematic. • Identificarea și aplicarea metodelor și algoritmilor învățați pentru probleme tip ale științelor fundamentale și aplicative. **C3 Privind tehnologiile aplicațiilor** • C3.1 Identificarea și definirea conceptelor, procedeelor și metodelor de procesare a informației folosite în realizarea de aplicații ce reies din necesități ale activității umane • C3.2 Explicarea tehnologiilor potrivite pentru realizarea de aplicații necesare în activitățile organizațiilor • C3.3 Utilizarea tehnologiilor moderne în definirea aplicațiilor software • C3.4 Utilizarea de criterii și metode determinate de tehnologiile aplicațiilor pentru evaluarea conformității cu standardele de interoperabilitate • C3.5 Dezvoltarea de aplicații software utilizând tehnologii moderne de transmitere, sto care și procesare date în corespundere cu necesitățile unei organizații **C5 Privind arhitectura și infrastructura sistemelor de calcul** • Identificarea și definirea de componente arhitecturale hardware, software și de comunicații, precum și celor necesare la descrierea unei infrastructuri de calcul. • Explicarea interacțiunii și funcționării componentelor arhitecturale și de infrastructură. • Aplicarea metodelor de bază pentru specificarea de soluții arhitecturale și de infrastructură pentru probleme tipice de calcul. • Utilizarea de criterii și metode de evaluare a caracteristicilor funcționale și nefuncționale ale componentelor de sistem . • Implementarea unei soluții arhitecturale și de infrastructură în baza unor constrângeri enunțate de proiect. • Identificarea componentelor hardware, software și de comunicații destinate aplicațiilor specifice domeniului selectat.
Competențe 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 unității de curs/modulului**

Obiectivul general	Însușirea conceptelor, metodelor și tehnologiilor de securitate informaționlă.
Obiectivele specifice	Să înțeleagă și să descrie conceptele de bază ale Securităţii informaţionale Să cunoască tipurilor de amenințări asupra infrastructurii informaționale Să însuşească și să selecteze tehnologiilor adecvate protecției informaţionale Să cunoască metodele de securitate a reţelelor de calculatoare Să aplice corect metodele de protecție in baza legislației din domeniul Securității informaționale

7. **Conținutul unității de curs/modulului**

Tematica activităților didactice	Numărul de ore Învățământ cu frecvență
Tematica prelegerilor	
T.1. Concepte generale privind Securitatea informaţională Scurtă istorie a Securităţii informaţionale. Principiile Securităţii informaţionale. Nivelele de structurare a conceptului de Securitate informaţională.	2
T.2. Forme de manifestare a pericolelor în sistemele informaționale Ameninţări şi atacuri. Identificarea ameninţărilor. Programe malițioase.	4
T.3. Controlul accesului în sistemele informaționale Tipuri de control al accesului. Identificarea, autentificarea și autorizarea. Managementul parolelor. Tehnologii SSO și OTP. Protecția informațiilor prin clasificarea lor.	2
T.4. Securitatea sistemelor informaționale Securitatea SO. Securitatea BD. Securitatea server-elor. Noțiuni și sisteme de backup-uri. Restabilirea informațiilor. Sisteme antimalware și de jurnalizare.	4
T.5. Principii de securitate privind dezvoltarea programelor Principiile privilegii minime, setări implicite, economia mecanismului, mijloc complet, proiectare deschisa, separarea privilegiilor, reducerea mecanismelor comune,	2
acceptabilitate psihologică.	
T.6. Tehnologii de protecție a informației electronice Criptarea. Steganografia. Filigranarea. Tehnologii criptografice. Sisteme simetrice și asimetrice de criptare.	4

T.7. Semnătura digitală și comerțul electronic Definiţia şi rolurile semnăturii. Infrastructura cheilor publice (PKI). Componentele şi funcţiile PKI. Politica de utilizare a certificatelor SSL. Comerțul electronic.	4
T.8. Securitatea informaţiei în reţelele de calculatoare Iniţiere în securitatea reţelelor. Protocoale de securitate. Tehnologii de protecţie a reţelelor de calculatoare. Firewall. Proxy server. VPN. IDS/IPS.	4
T.9. Aspecte juridice privind securitatea informațională Reglementări legislative pe plan național și internațional privind protecția datelor cu caracter personal și accesul la informații. Legislația internațională privind securitatea și protecția în spațiul cibernetic. Protecția drepturilor de autor (Copyright).	4
Total prelegeri:	**30**
Tematica activităților didactice	Numărul de ore Învățământ cu frecvență
Tematica lucrrilor de laborator	
LL.1. Gestionarea drepturilor de acces la fișiere și dosare (SO Windows, Linux) Tipuri de conturi de utilizator. Drepturi de acces la fișiere și dosare. Politicile de securitate privind conturile utilizatorilor. Information rights management (IRC).	4
LL.2. Managementul parolelor Sisteme de management al parolelor (KeePass, eWallet, LastPass, 1Password, RoboForm etc.). Crearea unui manager de parole și autentificarea la 3 servicii Web/aplicații.	4
LL. 3. Autentificare bazată pe mai mulți factori Crearea unui token de securitate (Rohos Logon Key, Rohos face Logon). Autentificarea utilizând token-ul de securitate creat. Soliția One-Time Password. Soluția Single Sign One.	4
LL.4. Copiile de siguranță și restabilirea informațiilor (Backup&Restore) Bakup&Restore în sistemele de operare: Windows Bakup&Restore, Linux Ubuntu {Deja Dup}. Sisteme de Backup&Restore//Recovery - caracteristici, configurare, executare și restaurare.	4
LL.5. Tehnologii de criptare Criptare simetrica (prin substituție, prin transpoziție). Criptare asimetrica. Semnătura digitală. Certificate SSL. Stenografia. Filigranarea.	4
LL.6. Tehnologii de protectie a rețelelor de calculatoare Firewall (Windows, Linux etc.). Proxy server (Windows, Linux etc.). IDS/IPS (Windows, Linux etc.).	4

LL.7. Rețele virtual-private (VPN). Instrumente VPN. Open VPN (Windows, Mac, Linux). LogMeIn Hamachi (Windows, Mac, Linux).Protocoale de securitate. VPN de tip IPSec.	6
Total lucrări de seminare:	**30**
Tematica activităților didactice	Numărul de ore
	Învățământ cu frecvență
Tematica lucrrilor de seminarelor	
LL. 3. Autentificare bazată pe mai mulți factori Crearea unui token de securitate (Rohos Logon Key, Rohos face Logon). Autentificarea utilizând token-ul de securitate creat. Soliția One-Time Password. Soluția Single Sign One.	4
LL.4. Copiile de siguranță și restabilirea informațiilor (Backup&Restore) Bakup&Restore în sistemele de operare: Windows Bakup&Restore, Linux Ubuntu {Deja Dup}. Sisteme de Backup&Restore//Recovery - caracteristici, configurare, executare și restaurare.	5
LL.5. Tehnologii de criptare Criptare simetrica (prin substituție, prin transpoziție). Criptare asimetrica. Semnătura digitală. Certificate SSL. Stenografia. Filigranarea.	2
LL.6. Tehnologii de protectie a rețelelor de calculatoare Firewall (Windows, Linux etc.). Proxy server (Windows, Linux etc.). IDS/IPS (Windows, Linux etc.).	2
LL.7. Rețele virtual-private (VPN). Instrumente VPN. Open VPN (Windows, Mac, Linux). LogMeIn Hamachi (Windows, Mac, Linux).Protocoale de securitate. VPN de tip IPSec.	2
Total lucrări de laborator/seminare:	**15**

8. **Referințe bibliografice**

Principale	1. Aurel Şerb, Constantin Baron, Narcisa Isăilă, Securitatea informatică în societatea informaţională, Bucureşti : Pro Universitaria, 2013. – 546 p. 2. Constantinescu Zoran, Gabriela Moise, Criptarea informaţiei : ghid practice, Ploieşti : Ed. Univ. 2. Petrol-Gaze din Ploieşti, 2013. – 120 p. 3. Stelian Flonta, Victor Valeriu Patriciu, Liviu Cristian Miclea, Metode criptografice pentru sisteme structurate, Cluj-Napoca : U.T.Press, 2011. – 260 p. 4. Dumitru Oprea, Protecţia şi securitatea informaţiilor. Ed. II, Polirom, Iaşi, 2007. – 445 p. 5. Popa Sorin Eugen, Securitatea sistemelor informatice, Bacău, 2007. – 136 p. 6. N.Ploteanu, S.Maftea, R.Griniuc, A.Coţofană, Pasul II în ciberspaţiu: Securitatea Informaţională, Academia „Ştefan cel Mare”, Chişinău, 2008. – 336 p. 7. Mark Stamp, Information security. Principles and Practice, Second Edition, SanJose State University, AJOHN WILEY&SONS, USA, 2011. - 608 p. 8. Luminița Scripcariu, Ion Bogdan etc., Securitatea rețelelor de comunicații, Casa de editură Venus, Iași, 2008. - 193 p.

Suplimentare	9. Ion Bica, Victor Valeriu Patriciu, Securitatea Comertului Electronic, Editura All, București, 2001. 10. Valentin Matyger, Securitatea Informaţiei în reţelele de calculatoare, Endava, 2010. 11. Ion I. Bucur, Tehnologii, structuri și managementul rețelelor de calculatoare, - resursă electronică. 12. Protecția datelor cu caracter personal, Documente ale Consiliului Europei, Chișinău, Biroul de Informații al Consiliului Europei în Moldova, 2001. 13. Constantin Popescu, Introducere in Criptografie, http://webhost.uoradea.ro/cpopescu/ 14. С. И. Макаренко, Информационная безопасность, Ставрополь СФ МГГУ им. М. А. Шолохова, 2009. 15. С. А. Нестеров, Информационная безопасность и защита информации, СанктПетербург, Издательство Политехнического университета, 2009. 16. Безбогов А.А., А.В. Яковлев, Ю.Ф. Мартемьянов, Безопасность операционных систем : учебное пособие, М. : "Издательство Машино-строение-1", 2007. 17. А. Петров, Компьютерная безопасность, ДМК, Москва, 2000. Europene, nr.185 // www.coe.int.
Acte normative	18. Legea Republicii Moldova despre accesul la informaţie nr.982-XIV din 11.05.2000 // MO nr. 88-90/664 din 28.07.2000. 19. Legea Republicii Moldova privind protecţia datelor cu caracter personal, nr.133 din 08.07.2011//MO nr.170-175 din 14.10.2011 20. Legea Republicii Moldova privind comerţul electronic, nr.284-XV din 22.07.2004. 21. Legea Republici Moldova cu privire la documentul electronic şi semnătura digitală, nr.264XV din 15.07.2004. 22. Legea privind dreptul de autor şi drepturile conexe, nr.293-XIII din 23.11.94. 23. Legea cu privire la secretul de stat, nr. 106-XIII din 17.05.94 // MO nr.2/5 din 25.08.1994. 24. Legea privind prevenirea şi combaterea criminalităţii informatice, nr. 20-XVI din 03.02.09 // MO nr.11-12/17 din 26.01.2010. 25. Codul penal al Republicii Moldova, din 18.04.2002 // MO nr.128-129 din 2002. 26. Convenția privind infracționalitatea în domeniul informaticii din 23.11.2001 în Seria Tratatelor

9. Evaluare

Curentă		Examen final
Atestarea 1	Atestarea 2	
30%	30%	40%
Standard minim de performanță		
Prezența și activitatea la prelegeri și lucrări de laborator; Obținerea notei minime de „5” la fiecare dintre atestări și lucrări de laborator; Demonstrarea în lucrarea de examinare finală a cunoașterii conceptelor, metodelor și tehnologiilor de securitate a sistemelor informaționale și a rețelelor de comunicații.		