MINISTERUL EDUCAŢIEI
UNIVERSITATEA "TIBISCUS" DIN TIMIŞOARA
FACULTATEA DE CALCULATOARE ŞI INFORMATICĂ APLICATĂ
STR. LASCĂR CATARGIU NR.6, TIMIŞOARA 300559
TEL/FAX: 0256 220 687
E-mail: fcia@tibiscus.ro Web: www.fcia.tibiscus.ro

FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea „Tibiscus" din Timişoara
1.2. Facultatea	Calculatoare şi Informatică Aplicată
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Master
1.6. Programul de studii/Calificarea	Administrarea Sistemelor Distribuite / *Programator (COR 251202), Inginer de sistem în informatică (COR 251203), Programator de sistem informatic (COR 251204), Manager proiect informatic (COR 251206), Specialist în domeniul proiectării asistate de calculator (COR 251401), Specialist în proceduri şi instrumente de securitate a sistemelor informatice (COR 251402), Consultant în informatică (COR 251901), Administrator baze de date (COR 252101), Administrator de reţea de calculatoare (COR 252301)*

2. Date despre disciplină

2.1. Denumirea disciplinei	**PROTOCOALE DE SECURITATE – MAS112**						
2.2. Titularul activităţii de curs	Conf.univ.dr. Alin Munteanu						
2.3. Titularul activităţii de seminar	Conf.univ.dr. Alin Munteanu						
2.4. Anul de studiu	1	2.5. Semestrul	1	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	DS

3. Timpul total estimat

3.1. Numărul de ore pe săptămână	4	din care 3.2. **curs**	2	3.3. seminar/**laborator**	2
3.4. Total ore din planul de învăţământ	56	din care 3.5. curs	28	3.6. seminar/**laborator**	28
Distribuţia fondului de timp					**Ore**
Studiul după manual, suport de curs, bibliografie şi notiţe					31
Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate					30
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					28
Tutoriat					28
Examinări					2
Alte activităţi					-
3.7. Total ore studiu individual					119
3.8. Total ore pe semestru					175
3.9. Numărul de credite					7

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	-
4.2. de competenţe	Utilizarea bazelor teoretice ale informaticii şi a reţelelor de calculatoare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Online: Google Classroom, Meet, ZOOM Sală de curs climatizată dotată corespunzător: tablă albă, SmartBoard 660 incluzând videoproiector şi calculator legat la Internet, software adecvat
5.2. de desfăşurare a seminarului/laboratorului	Online: Google Classroom, Meet, ZOOM Sală de laborator climatizată, dotată corespunzător: tablă, laptop/proiector, calculatoare, reţea, legătură internet, software adecvat

6. Competenţe specifice acumulate

6.1. Competenţe profesionale	- Însuşirea conceptelor de bază în reţele de calculatoare - Dezvoltarea abilităţilor de exploatare a unor tehnici de analiză a securităţii în reţele de calculatoare pentru potenţiali utilizatori
6.2. Competenţe transversale	- Îmbunătăţirea abilităţilor în utilizarea calculatoarelor şi în administrarea reţelelor de calculatoare

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1. Obiectivul general al disciplinei	• Dobândirea de cunoştinţe pentru implementarea unor politici de securitate în reţelele de calculatoare şi cunoaşterea principalilor algoritmi de criptare a informaţiilor
7.2. Obiectivele specifice	• Însuşirea algoritmilor de criptare simetrici/asimetrici • Cunoaşterea mecanismelor de generare a cheilor publice/private şi a modului de administrare a acestora • Principiile de bază ale securităţii reţelelor

8. Conţinuturi

8.1. Curs	**Metode de predare**	**Observaţii**
1. Vulnerabilităţi informatice. Politici de securitate informatică	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea	Cursurile se desfășoară pe platforma de e-learning Google Classroom, unde vor fi disponibile toate resursele necesare învățării (cursuri, alte materiale de suport). Pentru videoconferințe va fi folosită aplicația ZOOM
2. Securitatea în Internet: vulnerabilitatea reţelelor, protecţia transmisiei prin criptare, securitatea serviciilor Internet, securitatea prin firewall, tratarea incidentelor de securitate		
3. Protocoale de securitate la nivel reţea. IPv6 IPSec . Reţele VPN		
4. Protocoale de securitate la nivel transport. SSL şi TLS		
5. Protocoale de securitate la nivel aplicaţie. Securitatea aplicaţiilor uzuale în Internet: SSH, HTTPS, securitatea poştei electronice		
6. Algoritmi de criptare bazaţi pe cheie publică şi cheie privată		
7. Utilizarea schimbului de chei în sistemul Kerberos pentru sisteme distribuite		
8. Mecanisme si scheme de autentificare. Kerberos		
9. Sisteme electronice de plăţi. Protocolul Secure. Electronic Transaction (SET): caracteristici, criptografia sistemului SET		
10. Securitate în sistemul bancar şi plăţi electronice în Internet		
11. Metodologii de auditare a securităţii; instrumente pentru testarea securităţii reţelelor		

Bibliografie:

1. T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, April 2006
2. Mostafa Hashem, Protocols for Secure Electronic Commerce, CRC Press, 2004
3. P. Hoffman, SMTP Service Extension for Secure SMTP over TLS, RFC 2487, January 1999
4. S. Kent, Security Architecture for the Internet Protocol, RFC 2401, S. Kent, R. Atkinson
5. Lars Klander - Anti Hacker. Ghidul securitătii reţelelor de calculatoare"- Editura All Educational, 1998
6. V. V. Patriciu, M. Ene-Pietrosanu, C.Vaduva, I.Bica, N.Voicu, Securitatea Comertului Electronic, Ed. ALL 2006
7. V. V. Patriciu, M. Ene-Pietrosanu, I. Bica, J. Priescu, Semnaturi Electronice si Securitate Informatica, Ed. ALL, 2006
8. E. Rescorla, HTTP Over TLS, RFC 2818, May 2000
9. Harold F. Tipton, Micki Krause – Information Security Management Handbook, Auerbach Publications, CRC Press LLc, 2000
10. T. Ylonen, C. Lonvick, The Secure Shell (SSH) Protocol Architecture, RFC 4251, January 2006
11. Kerberos: The Network Authentication Protocol, http://web.mit.edu/Kerberos/;
12. Ethernet Standard: IEEE 802.3 CSMA/CD (ETHERNET), http://www.ieee802.org/3/
13. Wireless Ethernet Standard: IEEE 802.11 http://standards.ieee.org/getieee802/802.11.html
14. http://www.interhack.net/pubs/network-security.pdf
15. www.cybercash.com

8.2. Seminar/laborator	Metode de predare/învățare	Observaţii
1. - Algoritmi de criptare clasici - Codul Caesar - Codificări simple - Roata alfabetică - Pig Latin	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat	1 săptămână – 2 ore
2. Algoritmi de criptare clasici - Tabela Viginere - Tabela Porta - Codificări matrice - Codificări Bifid		1 săptămână – 2 ore
3. Algoritmi moderni de criptare: - DES - Triplu DES - RC5		1 săptămână – 2 ore
4. Algoritmi moderni de criptare: - AES - RSA		1 săptămână – 2 ore
5. Cerintele unei infrastructuri bazata pe chei publice şi private		1 săptămână – 2 ore
6. Detalierea mecanismelor complete de comunicare în cadrul unei PKI. Functionalitatea autorităţii de certificare. Mecanisme de protecţie a cheii private a autorităţii de certificare		1 săptămână – 4 ore
7. Generarea de certificate digitale. Securitatea chei private a unui utilizator din cadrul PKI. Semnarea acestora de către autoritatea de certificare.	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat	1 săptămână – 4 ore
8. Semnarea documentelor folosind cheia privată		1 săptămână – 2 ore
9. Verificarea semnăturilor digitale folosind cheia publică a semnatarului. Validarea cheii publice a semnatarului şi a certificatului său digital cu ajutorul cheii publice a autorităţii de certificare		1 săptămână – 4 ore
10. Anularea unui certificat digital emis. Liste de revocare a certificatelor (CRL).		1 săptămână – 2 ore
11. Posibile soluţii de dezvoltare şi îmbunătăţiri ulterioare a insfrastructurii PKI dezvoltate. Integrarea acesteia cu mecanisme web-based.		1 săptămână – 2 ore

Bibliografie

1. Stallings W.- Cryptography and Network Security, Principles and Practice –, Third Edition, Prentice Hall,2003
2. Shafi Goldwasser, Mihir Bellare - Lecture Notes on Cryptography, 2001

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

Conţinutul disciplinei corespunde curriculei din alte centre universitare, din ţară sau Uniunea Europeană. Conţinuturile practice (lucrări de laborator) corespund cerinţelor de pe piaţa muncii locală.

10. Evaluare

Tip de activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Evaluarea are în vedere următoarele categorii de cunoştinţe: • cunoştinţe generale şi cunoştinţe de detaliu, evaluate printr-un test cuprinzând întrebări orientate spre noţiunile cheie predate	Examinare scrisă; participare activă la activităţile de curs	50%

	• utilizarea noţiunilor teoretice, evaluate printr-un test cuprinzând un set de probleme		
10.5. Seminar / laborator	Temele de la laborator Elaborarea unui referat din tematica securităţii de calculatoare Testarea continuă pe parcursul semestrului	Evaluarea temelor, activităţilor adiţionale; Evaluarea activităţii la laborator; Participarea activă la activităţile de laborator	50%
10.6. Standard minim de performanţă			
Examinare scrisă: • Pentru nota 5 este necesară obţinerea unui punctaj superior (minim 60%) pentru cunoştinţele generale, precum şi dovedirea unui nivel minim de înţelegere şi aplicare a unora dintre noţiunilor prezentate la curs (minim 40%) Probe practice şi activitate de laborator: • Pentru nota 5 este necesară obţinerea unui nivel superior (minim 60%) pentru cunoştinţele generale, precum şi a unui nivel minim de înţelegere şi utilizare a cunoştinţelor de detaliu prezentate anterior.			

Data completării	**Semnătura titularului de curs**	**Semnătura titularului de laborator**
24.09.2021	**.....**	**.....**

Data avizării în departament	**Semnătura directorului de departament**
.....	**.....**