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

2. Date despre disciplină

2.1. Denumirea disciplinei	**PROTOCOALE DE SECURITATE (PS) – MASD112**						
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=sinteză DOB=obligatorie

3. Timpul total estimat

3.1. Numărul de ore pe săptămână	4	din care 3.2. curs	2	3.3. Laborator	2
3.4. Total ore din planul de învăţământ	56	din care 3.5. curs	28	3.6. Laborator	28
Distribuţia fondului de timp					**Ore**
Studiul după manual, suport de curs, bibliografie şi notiţe					28
Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate					28
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					28
Tutoriat					6
Examinări					4
Alte activităţi					-

3.7. Total ore studiu individual	94
3.8. Total ore pe semestru	150
3.9. Numărul de credite	6

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	Sisteme de operare, Securitate informatică, Administrarea rețelelor locale, Rețele de calculatoare
4.2. de competenţe	Utilizarea bazelor teoretice ale informaticii şi a reţelelor de calculatoare; Înțelegerea mecanismelor de funcționare a protocoalelor de comunicație; Cunoașterea principiilor fundamentale de securitate: confidențialitate, integritate, disponibilitate

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Sală de curs dotată cu videoproiector; Calculator/laptop pentru cadrul didactic; Acces la internet pentru demonstrații și prezentarea unor studii de caz actuale din domeniul securității; Acces la platformă e-learning pentru distribuirea materialelor și comunicarea cu studenții
5.2. de desfăşurare a laboratorului	Laborator de informatică dotat cu calculatoare conectate în rețea și acces la internet; Medii virtualizate pentru simularea scenariilor de atac și protecție; Instrumente de analiză și securitate (ex. OpenSSL, firewall software, IDS/IPS, instrumente de testare a vulnerabilităților);

6. Obiectivele disciplinei - rezultate așteptate ale învățării la formarea cărora contribuie parcurgerea și promovarea disciplinei

Cunoștințe	La finalizarea disciplinei, studentul: Cunoaște principiile fundamentale ale securității informației (confidențialitate, integritate, disponibilitate, autentificare, non-repudiere); Înțelege mecanismele criptografice utilizate în protocoalele de securitate (criptografie simetrică și asimetrică, funcții hash, semnături digitale, certificate digitale); Înțelege mecanismele de autentificare, autorizare și control al accesului; Cunoaște metodele de protecție a comunicațiilor în rețele locale și distribuite.
Abilități	La finalizarea disciplinei, studentul este capabil să: Configureze și implementeze protocoale securizate pentru comunicații în rețea; Aplice mecanisme criptografice pentru protejarea datelor; Configureze și gestioneze conexiuni securizate (VPN, IPSec, TLS); Proiecteze soluții de securizare adaptate unor scenarii reale din mediul organizațional.
Responsabilitate și autonomie	Își asumă responsabilitatea pentru configurarea și administrarea securizată a infrastructurilor de comunicații; Aplică principii etice și legale în utilizarea tehnologiilor de securitate; Respectă standardele profesionale și bunele practici în domeniul securității cibernetice.

7. Conţinuturi

7.1. Curs	**Metode de predare**	**Observaţii**
1. Vulnerabilităţi informatice. Politici de securitate informatică	Expunerea interactivă, problematizarea, conversaţia euristică, documentarea pe web, exemplificarea.	Analiza studiilor de caz privind incidente reale
2. Securitatea în Internet: vulnerabilitatea reţelelor, protecţia transmisiei prin criptare, securitatea serviciilor Internet, securitatea prin firewall, tratarea incidentelor de securitate	Expunere interactivă, studiu de caz, dezbatere, analiză comparativă	Corelare cu atacuri reale și mecanisme de prevenție
3. Protocoale de securitate la nivel reţea. IPv6 IPSec . Reţele VPN	Explicație, modelare, analiză arhitecturală	Integrarea mecanismelor de criptare în infrastructuri distribuite
4. Protocoale de securitate la nivel transport. SSL şi TLS	Expunere, analiză protocol, exemplificare	Corelare cu HTTPS și securizarea comunicațiilor web
5. Protocoale de securitate la nivel aplicaţie. Securitatea aplicaţiilor uzuale în Internet: SSH, HTTPS, securitatea poştei electronice	Studiu de caz, demonstrație conceptuală	Analiza certificatelor digitale și a mecanismelor PKI
6. Algoritmi de criptare bazaţi pe cheie publică şi cheie privată	Explicație teoretică, modelare matematică, exemplificare	RSA, ECC, semnături digitale
7. Utilizarea schimbului de chei în sistemul Kerberos pentru sisteme distribuite	Expunere, analiză de protocol, modelare	Corelare cu autentificarea centralizată
8. Mecanisme si scheme de autentificare. Kerberos	Problem solving, analiză arhitecturală	Autentificare mutuală și Single Sign-On
9. Sisteme electronice de plăţi. Protocolul Secure. Electronic Transaction (SET): caracteristici, criptografia sistemului SET	Expunere, studiu de caz	Analiza mecanismelor criptografice în tranzacții
10. Securitate în sistemul bancar şi plăţi electronice în Internet	Dezbatere, analiză de risc, studii comparative	Corelare cu standarde moderne (ex. 3D Secure)
11. Metodologii de auditare a securităţii; instrumente pentru testarea securităţii reţelelor	Expunere interactivă, exemplificare practică, analiză de scenarii	Introducere în testare de penetrare și evaluare vulnerabilități
12. Auditarea și securizarea unei infrastructuri distribuite	Expunere, studiu de caz	Integrare: VPN + TLS + autentificare + politici + criptografie + audit

13. Proiect final complet descris 14. Recapitulare, Finalizare proiecte	Proiectarea și implementarea unei arhitecturi securizate pentru un sistem distribuit	Proiectul urmărește dezvoltarea competențelor avansate de analiză, proiectare și implementare a protocoalelor de securitate în contexte reale

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. V. V. Patriciu, M. Ene-Pietrosanu, C.Vaduva, I.Bica, N.Voicu, Securitatea Comertului Electronic, Ed. ALL 2006
6. V. V. Patriciu, M. Ene-Pietrosanu, I. Bica, J. Priescu, Semnaturi Electronice si Securitate Informatica, Ed. ALL, 2006
7. E. Rescorla, HTTP Over TLS, RFC 2818, May 2000
8. Harold F. Tipton, Micki Krause – Information Security Management Handbook, Auerbach Publications, CRC Press LLc, 2000
9. T. Ylonen, C. Lonvick, The Secure Shell (SSH) Protocol Architecture, RFC 4251, January 2006
10. A.R. Martinez, R.F. Lopez, F.P. Garcia, "Architectures and Protocols for Secure Information Technology Infrastructures", IGI Global, 2013
11. P:W. Singe,r A. Friedman, "Cybersecurity and Cyberwar: What Everyone Needs to Know" , Oxford Press, 2014
12. 2. D. Antonucci, "The Cyber Risk Handbook. Creating and Measuring Effective Cybersecurity Capabilities." , Wiley, 2017.
13. Kerberos: The Network Authentication Protocol, http://web.mit.edu/Kerberos/ (accesat 10 martie 2022);
14. Ethernet Standard: IEEE 802.3 CSMA/CD (ETHERNET), http://www.ieee802.org/3/ (accesat 10 martie 2022)

7.2. Seminar/laborator	**Metode de predare/învăţare**	**Observaţii**
1. - Algoritmi de criptare clasici Codul Caesar / Codificări simple / Roata alfabetică / Pig Latin	Exerciţiul, discuţiile şi dezbaterea, modelarea, proiectul, lucrul în grup organizat	Introducere în conceptele fundamentale de criptografie
2. Algoritmi de criptare clasici Tabela Viginere / Tabela Porta / Codificări matrice / Codificări Bifid	Exercițiu aplicativ, analiză comparativă, lucru în echipă	Evidențierea limitărilor criptografiei clasice
3. Algoritmi moderni de criptare: - DES / Triplu DES / RC5	Exercițiul, modelare, studiu de caz	Analiza vulnerabilităților istorice
4. Algoritmi moderni de criptare: - AES / RSA	Modelare matematică, aplicații practice	Compararea criptării simetrice și asimetrice
5. Cerintele unei infrastructuri bazata pe chei publice şi private	Exercițiul, dezbatere, modelare	Fundamentarea conceptului de PKI
6. Detalierea mecanismelor complete de comunicare în cadrul unei PKI. Functionalitatea autorităţii de certificare. Mecanisme de protecţie a cheii private a autorităţii de certificare	Studiu de caz, analiză arhitecturală	Structura unei infrastructuri reale
7. Generarea de certificate digitale. Securitatea chei private a unui utilizator din cadrul PKI. Semnarea acestora de către autoritatea de certificare.	Exercițiu practic, simulare	Implementare într-un mediu virtualizat
8. Semnarea documentelor folosind cheia privată	Aplicații practice, modelare	Utilizarea OpenSSL sau echivalent
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	Exercițiu practic, analiză protocol	Lanțul de încredere
10. Anularea unui certificat digital emis. Liste de revocare a certificatelor (CRL).	Demonstrație practică, analiză scenarii	Gestionarea incidentelor de securitate
11. Posibile soluţii de dezvoltare şi îmbunătăţiri ulterioare a insfrastructurii PKI dezvoltate. Integrarea acesteia cu mecanisme web-based.	Studiu de caz, problem solving	Integrare cu aplicații HTTPS
12. Auditarea și securizarea unei infrastructuri distribuite	Expunere, studiu de caz, analiză aplicativă, dezbatere, lucru în echipă	Integrare: VPN + TLS + mecanisme de autentificare

13. Proiect – Proiectarea unei infrastructuri PKI pentru o organizație distribuită 14. Implementare, testare și audit al infrastructurii PKI dezvoltate. Prezentare finală	Învățare prin proiect, lucru în echipă, mentorat	Evaluare finală integrată (configurare, validare, analiză vulnerabilități)

Bibliografie

1. Shafi Goldwasser, Mihir Bellare - Lecture Notes on Cryptography, 2001
2. Kevin D. Mitnick, W.L. Simon , "The Art of Deception: Controlling the Human Element of Security" , 2003
3. Stallings W.- Cryptography and Network Security, Principles and Practice –, Third Edition, Prentice Hall,2003
4. A.R. Martinez, R.F. Lopez, F.P. Garcia, "Architectures and Protocols for Secure Information Technology Infrastructures", IGI Global, 2013
5. D. Antonucci, "The Cyber Risk Handbook. Creating and Measuring Effective Cybersecurity Capabilities.", Wiley, 2017

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

Conținuturile disciplinei sunt elaborate în concordanță cu direcțiile actuale de cercetare și dezvoltare din domeniul securității comunicațiilor, criptografiei aplicate și protecției infrastructurilor distribuite. Tematica privind protocoalele de securitate la nivel rețea, transport și aplicație (IPSec, TLS/SSL, SSH, VPN), infrastructurile PKI, mecanismele de autentificare și auditarea securității reflectă standardele și bunele practici promovate de comunitatea academică și organizațiile profesionale din domeniul IT&C și securității cibernetice. Conținuturile sunt corelate cu evoluțiile tehnologice actuale (sisteme distribuite, cloud, comunicații securizate, autentificare centralizată), asigurând relevanța profesională a absolvenților pe piața muncii.

9. Evaluare

Tip de activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
9.1. Curs	Evaluarea are în vedere următoarele categorii de cunoştinţe: - cunoştinţe generale şi cunoştinţe de detaliu, evaluate printr-o examinare orală (discuţie) cuprinzând întrebări orientate spre noţiunile cheie predate - utilizarea noţiunilor teoretice, evaluate într-un context dat sau pe o aplicaţie concretă	Examinare scrisă/orală; participare activă la activităţile de curs	50%
9.2. Laborator	Evaluarea are în vedere următoarele categorii de cunoştinţe: - cunoştinţe generale şi cunoştinţe de detaliu, evaluate printr-o examinare orală (discuţie) cuprinzând întrebări orientate spre înţelegerea conceptelor generice ale standardelor şi protocoalelor de securitate; înţelegerea diverselor tehnici folosite în standardele de securitate, - aplicarea conceptelor de securitate din protocoalele analizate, în contextul realizării unor standard.	Evaluarea temelor, activităţilor adiţionale; Evaluarea activităţii la laborator; Participarea activă la activităţile de laborator	50%

9.3. Standard minim de performanţă

Pentru obținerea notei minime de promovare (5), studentul trebuie să demonstreze următoarele competențe minimale:

- Însușirea noțiunilor fundamentale privind principiile securității informației (confidențialitate, integritate, disponibilitate);
- Cunoașterea mecanismelor de bază ale criptografiei simetrice și asimetrice;
- Utilizarea unui mediu de simulare sau virtualizare pentru implementarea unui mecanism de securizare (ex. conexiune VPN, configurare TLS sau generare certificat digital);
- Demonstratea capacității de configurare elementară a unui protocol securizat.

Data completării
20.09.2025

Titular de disciplină
Conf.univ.dr. Alin-Daniel MUNTEANU

Data avizării în departament
26.09.2025

Director de departament
Conf.univ.dr. Victoria IORDAN