FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Transilvania din Braşov
1.2 Facultatea	Matematică şi Informatică
1.3 Departamentul	Matematică şi Informatică
1.4 Domeniul de studii de masterat [1)]	Matematică şi ştiinţe ale naturii
1.5 Ciclul de studii[2)]	Masterat
1.6 Programul de studii/ Calificarea	Tehnologii moderne în ingineria sistemelor soft / Informatician

2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea sistemelor IT							
2.2 Titularul activităților de curs								
2.3 Titularul activităților de seminar/ laborator/ proiect								
2.4 Anul de studiu	2	2.5 Semestrul	3	2.6 Tipul de evaluare	E	2.7 Regimul disciplinei	Conținut[2)]	DAP
							Obligativitate[3)]	DO

3. Timpul total estimat (ore pe semestru al activităților didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 seminar/ laborator/ proiect	**0/2/0**
3.4 Total ore din planul de învățământ	56	din care: 3.5 curs	28	3.6 seminar/ laborator/ proiect	0/28/0

Distribuția fondului de timp	ore
Studiul după manual, suport de curs, bibliografie şi notițe	30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	30
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri	53
Tutoriat	0
Examinări	6
Alte activități.....	0

3.7 Total ore de studiu individual	119
3.8 Total ore pe semestru	175
3.9 Numărul de credite[5)]	7

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	• Cunoştinţe IT de bază, • Noţiuni de reţelistică, • Noţiuni de siteme de operare, • Noţiuni de criptografie
4.2 de competențe	• Configurare și monitorizare de echipamente de rețea (switch-uri, routere, firewall-uri). • Cunoştinţe de Windows si Linux • Înțelegerea algoritmilor criptografici (AES, RSA, SHA)

5. Condiții (acolo unde este cazul)

5.1 de desfăşurare a cursului	• Videoproiector, tablă, laptop, conexiune la Internet
5.2 de desfăşurare a	Resurse software necesare:

seminarului/ laboratorului/ proiectului	• Mașini virtuale pentru testare (ex. VirtualBox, VMware). • Acces la medii simulate de securitate, cum ar fi Hack The Box, TryHackMe sau alte platforme de tip CTF (Capture The Flag). Resurse hardware necesare: • Calculator/laptop • Acces la o rețea de test (virtuală sau izolată) pentru exerciții practice.

6. Competențe specifice acumulate (conform grilei de competențe din planul de învățământ)

Competențe profesionale	CP1. Evalueaza interactiunea utilizatorilor cu aplicatiile TIC, integreaza componente ale sistemului CP2. Stabileste procese de date, administreaza sisteme de colectare a datelor, dezvolta aplicatii de procesare de date, implementeaza procese privind calitatea datelor, realizeaza extragerea informatiilor din date CP3. Gandeste in mod abstract, tine pasul cu cele mai recente solutii privind sistemele informatice CP4. Creaza specificatii de proiect, asigura managementul de proiect, gestioneaza proiectul de TIC, dezvolta prototipul pentru software, dezvolta instrumente de inginerie software asistata de calculator, verifica specificatiile oficiale pentru TIC, creaza diagrama de proces CP5. Utilizeaza biblioteci de software, utilizeaza baze de date, creaza softuri, proiecteaza interfete intre componente, utilizeaza sabloane de proiectare software
Competențe transversale	CT1. Aplica competente de baza in materie de programare, opereaza echipamente hardware digitale CT2. Utilizeaza software de comunicare si colaborare, efectueaza cautari pe Internet CT3. Identifica probleme, solutioneaza probleme CT4. Demonstreaza angajament, gandeste rapid, gandeste analitic, isi mentine concentrarea pentru perioade lungi de timp CT5. Lucreaza in echipe, organizeaza informatii, obiecte si resurse, da dovada de dorinta de invatare, se adapteaza la schimbare, face fata stresului

7. Obiectivele disciplinei (reieșind din competențele specifice acumulate)

7.1 Obiectele generale ale disciplinei	• Dezvoltarea competențelor fundamentale în securitatea cibernetică • Familiarizarea cu amenințările și vulnerabilitățile IT • Integrarea securității în proiectarea și administrarea sistemelor IT • Formarea abilității de a analiza incidente de securitate și de a propune soluții eficiente.
7.2 Obiectivele specifice	• Cunoașterea normelor și standardelor de securitate • Identificarea și gestionarea amenințărilor cibernetice • Aplicarea criptografiei în protecția datelor • Proiectarea și implementarea de politici de securitate • Analiza și testarea vulnerabilităților • Răspunsul la incidente și planificarea continuității • Experimentarea în medii simulate prin dezvoltarea de scenarii de atac si aparare pentru a înţelege mai bine perspectivele adversarilor

8. Conținuturi

8.1 Curs	Metode de predare	Număr de ore	Observații
Noțiuni fundamentale în securitatea IT: istoria securitatii, amenintari, riscuri si metode de Securitate IT	Expunere	2	

Amenințări și atacuri cibernetice: clasificarea atacurilor si exemple celebre de atacuri, precum si impactul lor asupra echipamentelor IT	Expunere, explicație, exemplificare	2	
Fundamentele criptografiei: principii, algoritmi criptografici, certificate digitale si semnatura electronica	Expunere, explicație, exemplificare	2	
Securitatea rețelelor: principii de baza, protocoale de securitate, monitorizarea si detectarea anomaliilor din retea	Expunere, explicație, exemplificare	2	
Securitatea sistemelor de operare: vulnerabilitati commune pentru diferite sisteme de operare, configurarea politicilor de Securitate pentru utilizatorii unui SO	Expunere, explicație, exemplificare	2	
Securitatea aplicațiilor web: prevenirea atacurilor SQL Injection, XSS și CSRF, precum si testarea securității aplicațiilor web.	Expunere, explicație, exemplificare	2	
Instrumente și tehnici de pen-testing: introducere in acest tip de testare, prezentarea instrumentelor de testare si prezentarea etapelor unui test de penetrare	Expunere, explicație, exemplificare	2	
Securitatea datelor: asigurarea confidentialitatii si integritatii datelor, implementarea de politici de recuperare si backup	Expunere, explicație, exemplificare	2	
Securitatea în cloud computing: provocari si riscuri in mediile clowd, solutii de securitate in AWS, Azure si Google Cloud	Expunere, explicație, exemplificare	2	
Răspunsul la incidente de securitate: detectarea și investigarea incidentelor; tehnici de remediere și recuperare, rolul echipelor CSIRT/SOC	Expunere, explicație, exemplificare	2	
Managementul riscurilor și politici de securitate: identificare, evaluare, dezvoltare si implementare de politici de securitate	Expunere, explicație, exemplificare	2	
Securitatea dispozitivelor IoT și mobile: vulnerabilitati specific si solutii de protectie	Expunere, explicație, exemplificare	2	
Tendințe moderne în securitatea IT: utilizarea ML si AI in detectia amenintarilor, securitate in blockchain si criptomonede	Expunere, explicație, exemplificare	2	
Prezentarea unui scenariu simulat de atac al unei organizatii impreuna cu un plan de securitate IT	Expunere, explicație, exemplificare	2	

Bibliografie

1. William Stallings - *Cryptography and Network Security: Principles and Practice, 2020*
2. Michael E. Whitman, Herbert J. Mattord - *Principles of Information Security, 2021*
3. Bruce Schneier - *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 1995*
4. Rafeeq Rehman - *Penetration Testing with Kali Linux: Step-by-Step Guide, 2015*
5. OWASP (Open Web Application Security Project) - *OWASP Top 10, 2021*

8.2 Seminar/ laborator/ proiect	Metode de predare-învățare	Număr de ore	Observații
Aplicatia 1: Configurarea unui mediu securizat. • Configurarea unei mașini virtuale (VM) securizate (ex. folosind VirtualBox sau VMware). • Instalarea unui sistem de operare (Linux sau Windows) și aplicarea configurațiilor de securitate de bază. • Setarea utilizatorilor și permisiunilor.	Exemplificare, proiecte, teme de laborator	4	
Aplicația 2: Analiza și detectarea vulnerabilităților • Scanarea unui sistem pentru vulnerabilități utilizând instrumente precum Nessus, OpenVAS sau Nmap. • Interpretarea rezultatelor scanării și identificarea problemelor critice.	Exemplificare, proiecte, teme de laborator	4	
Aplicația 3: Criptografie practică • Implementarea criptării și decriptării fișierelor folosind algoritmi simetrici (ex. AES) și asimetrici (ex. RSA). • Generarea și utilizarea cheilor private și publice. • Crearea unui certificat digital simplu utilizând OpenSSL.	Exemplificare, proiecte, teme de laborator	4	
Aplicația 4: Securitatea rețelelor • Configurarea unui firewall software (ex. iptables pe Linux sau Windows Defender Firewall). • Simularea și prevenirea unui atac DoS/DDoS într-un mediu izolat. • Configurarea unei conexiuni VPN folosind OpenVPN sau altă soluție similară.	Exemplificare, proiecte, teme de laborator	4	
Aplicația 5: Detectarea și prevenirea atacurilor web • Simularea unui atac SQL Injection și prevenirea acestuia prin validarea inputurilor într-o aplicație web simplă. • Analiza vulnerabilităților XSS folosind un script demonstrativ. • Utilizarea Burp Suite pentru testarea securității unei aplicații web.	Exemplificare, proiecte, teme de laborator	4	
Aplicația 6: Investigarea unui incident de securitate • Analiza unui fișier jurnal (log) pentru detectarea unor activități neautorizate (ex. acces suspect, erori critice). • Identificarea unui atac de tip brute-force asupra parolelor. • Crearea unui raport de răspuns la incident și propunerea de măsuri de remediere.	Exemplificare, proiecte, teme de laborator	4	

Aplicația 7: Proiect final - Implementarea unui plan de securitate IT • Elaborarea și prezentarea unui plan de securitate IT pentru o organizație simulată. • Include măsuri pentru: o Protecția rețelei. o Securitatea sistemelor de operare. o Protecția datelor și backup. o Managementul utilizatorilor și accesului.	Exemplificare, proiecte, teme de laborator	4	

Bibliografie

1. M. Dumitrescu, D. Simionovici - Securitatea rețelelor și a sistemelor informatice. Implementarea directivei NIS în România, 2019
2. T.O. Adam, L. Gabudeanu, V.V. Rotaru - Managementul riscului, protecția datelor personale și securitatea informației în cadrul organizației. Ghid practice, 2019
3. S. Popa - Securitatea sistemelor informatice, 2008
4. R. Nastase - Introducere în Securitate Cibernetică, 2019
5. M. Sikorski, A. Honig - Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software, 2012
6. K. Graves - CEH Certified Ethical Hacker Study Guide, 2010

9. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunităților epistemice, asociațiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

Conținuturile sunt în concordanță cu problematica monografiilor apărute în ultimii ani în literatura de specialitate.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Evaluarea însuşirii noțiunilor predate la curs	Evaluare finală prin probă scrisă	25 %
10.5 Seminar/ laborator/ proiect	Acumularea competențelor vizate prin conținutul disciplinei	Evaluarea aplicațiilor realizate la orele de laborator şi a activităților participative	75 %
10.6 Standard minim de performanță			
• Să obțină minim nota 5 la fiecare tip de evaluare • **Curs**: studentii trebuie să poată efectua o evaluare de bază a vulnerabilităților unui sistem informatic şi să fie în măsură să elaboreze un raport de securitate, oferind recomandări pentru îmbunătățirea sistemului IT analizat. • **Laborator**: studentii trebuie să fie capabili să configureze și să securizeze un server Linux/Windows împotriva atacurilor commune, să configureze o maşină virtuală, un firewall, o conexiune VPN, sa evite atacurile SQL Injection in aplicatiile web si sa testeze securitatea unei aplicatii web			

Prezenta Fișă de disciplină a fost avizată în ședința de Consiliu de departament din data de 26/09/2024 și aprobată în ședința de Consiliu al facultății din data de 26/09/2024

Decan Conf. dr. Gabriel STAN	Director de departament Conf. dr. Nicuşor MINCULETE
Lect. univ. dr. Corina-Ştefania NĂNĂU Titular de curs	Lect. univ. dr. Corina-Ştefania NĂNĂU Titular de laborator

Notă:

[1)] Domeniul de studii - se alege una din variantele: Licență/ Masterat/ Doctorat (se completează conform cu Nomenclatorul domeniilor şi al specializărilor/ programelor de studii universitare în vigoare);

[2)] Ciclul de studii - se alege una din variantele: Licență/ Masterat/ Doctorat;

[3)] Regimul disciplinei (conținut) - se alege una din variantele: **DF** (disciplină fundamentală)/ **DD** (disciplină din domeniu)/ **DS** (disciplină de specialitate)/ **DC** (disciplină complementară) - pentru nivelul de licență; **DAP** (disciplină de aprofundare)/ **DSI** (disciplină de sinteză)/ **DCA** (disciplină de cunoaştere avansată) - pentru nivelul de masterat;

[4)] Regimul disciplinei (obligativitate) - se alege una din variantele: **DI** (disciplină obligatorie)/ **DO** (disciplină opțională)/ **DFac** (disciplină facultativă);

[5)] Un credit este echivalent cu 25 – 30 de ore de studiu (activități didactice şi studiu individual).