

FIȘA DISCIPLINEI

1. Date despre program

1.1. Instituția de învățământ superior	Universitatea „Tibiscus” din Timișoara
1.2. Facultatea	Calculatoare și Informatică Aplicată
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Licență
1.6. Programul de studii/Calificarea	Informatică

2. Date despre disciplină

2.1. Denumirea/codul disciplinei	SECURITATE INFORMATICĂ (SI) - (OPȚIONAL5) LIN327						
2.2. Titularul activității de curs	Conf.univ.dr. Alin-Daniel MUNTEANU						
2.3. Titularul activității de seminar	Valenin MARIA						
2.4. Anul de studiu	3	2.5. Semestrul	2	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	Conținut ¹ =DS Obligativitate ² =DOP

3. Timpul total estimat

3.1. Numărul de ore pe săptămână	4	din care 3.2. curs	2	3.3. laborator	1
3.4. Total ore din planul de învățământ	36	din care 3.5. curs	24	3.6. laborator	12
Distribuția fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					12
Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate și pe teren					28
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					24
Tutoriat					-
Examinări					4
Alte activități					-
3.7. Total ore studiu individual	64				
3.8. Total ore pe semestru	100				
3.9. Numărul de credite	4				

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Programare, Structuri de date și algoritmi, BRC (Bazele Rețelelor de Calculatoare), ARL (Arhitectura Rețelelor de Calculatoare), Baze de date (noțiuni introductive)
4.2. de competențe	Capacitatea de a utiliza limbaje de programare pentru dezvoltarea aplicațiilor software. Înțelegerea principiilor de funcționare ale sistemelor informatice și ale rețelelor de calculatoare. Abilitatea de a analiza vulnerabilitățile sistemelor informatice și de a identifica riscurile de securitate.

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Sală de curs dotată cu tablă și videoproiector pentru prezentarea conceptelor teoretice și a exemplurilor din domeniul securității informatice. Acces la materiale didactice în format electronic - Google Classroom Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfășurare a laboratorului	Laborator de informatică dotat cu calculatoare conectate la rețea și acces la internet. Acces la instrumente software specifice securității informatice pentru analiza vulnerabilităților și testarea mecanismelor de protecție. Participarea activă la activitățile practice și realizarea temelor sau proiectelor aplicative. Prezență la laborator minim 50% pentru admiterea la examenul final.

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

Cunoștințe	Cunoașterea conceptelor fundamentale privind securitatea informației și securitatea sistemelor informatice. Înțelegerea principalelor amenințări, vulnerabilități și tipuri de atacuri informatice. Cunoașterea metodelor și mecanismelor de protecție a datelor și a sistemelor informatice. Înțelegerea principiilor de autentificare, control al accesului și criptare.
Abilități	Capacitatea de a identifica și analiza vulnerabilitățile sistemelor informatice. Abilitatea de a aplica metode și instrumente pentru protecția datelor și a sistemelor informatice. Utilizarea unor instrumente software pentru analiza și testarea securității sistemelor informatice. Capacitatea de a implementa măsuri de securitate pentru prevenirea accesului neautorizat și a atacurilor informatice.
Responsabilitate și autonomie	Aplicarea responsabilă a cunoștințelor și tehnologiilor utilizate în domeniul securității informatice. Respectarea principiilor de etică profesională și utilizare responsabilă a instrumentelor informatice. Capacitatea de a lucra individual sau în echipă pentru analiza și rezolvarea problemelor de securitate. Manifestarea autonomiei în documentarea și actualizarea cunoștințelor privind securitatea informatică.

7. Conținuturi

7.1. Curs	Metode de predare	Observații
1. Fundamentele securității cibernetice	Expunere interactivă, demonstrație, problematizare, discuții	Introducere în conceptele fundamentale ale securității informatice
2. Securitatea cibernetică a utilizatorilor individuali	Expunere, studii de caz, discuții	Exemple de amenințări și metode de protecție pentru utilizatori
3. Securitatea cibernetică a organizațiilor	Expunere, studii de caz, problematizare	Politici și mecanisme de securitate în mediul organizațional
4. Protecția datelor personale și securitatea cibernetică	Expunere, discuții, analiză de exemple	Aspecte privind protecția datelor și confidențialitatea informațiilor
5. Vulnerabilități specifice sistemelor de operare	Expunere, demonstrație, studii de caz	Identificarea și analiza vulnerabilităților sistemelor de operare
6. Auditul de securitate, politici de securitate. Modele	Expunere, problematizare, analiză de caz	Metode de evaluare a securității sistemelor informatice
7. Standarde în securitatea cibernetică	Expunere, discuții, exemplificare	Prezentarea standardelor și bunelor practici în securitate
8. Internet of Things –oportunități, provocări, pericole și posibile soluții	Expunere, studii de caz, discuții	Analiza riscurilor de securitate în ecosistemele IoT
9. Standarde de securitate în mediul IoT	Expunere, analiză comparativă, discuții	Prezentarea standardelor și protocoalelor de securitate IoT
10. Tehnologii de asigurare a securității, intimității și încrederii în lumea digitală. Securizarea infrastructurii și a controlului industrial	Expunere, demonstrație, studii de caz	Exemple de tehnologii utilizate pentru protejarea infrastructurilor critice

Bibliografie

- [1]. Antonucci, D. The Cyber Risk Handbook. Creating and Measuring Effective Cybersecurity Capabilities, Wiley, 2017
- [2]. Bejtlich, R., The Practice of Network Security Monitoring: Understanding Incident Detection and Response No Starch Press, 2013
- [3]. Berzakov, P., Understanding Database Administration, Create Space Independent Publishing Platform, 2010
- [4]. Bishop, M., Computer Security: Art and Science, Addison - Wesley Professional, 2002
- [5]. Casey, E., Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, Academic Press, 2011

- [6]. Cole, E., Network Security Bible, Wiley, 2009
 [7]. Moore, R., Cybercrime: Investigating High-Technology Computer Crime, Anderson, 2010
 [8]. Owens, T., The theory and craft of digital preservation, Johns Hopkins University Press, 2018
 [9]. Stallings, W., Network Security Essentials: Applications and Standards (ed. 4, 5), Prentice Hall, 2010, 2013
 [10]. Stallings, W., Brown, L., Computer Security: Principles and Practice, Prentice Hall, 2011
 [11]. Vacca, J. R.: Computer and Information Security Handbook , Morgan Kaufmann, 3 edition , 2017

7.2. Laborator	Metode de Predare/ învățare	Observații
1. Topologie în mediul de simulare de recapitulare a notiunilor învățate la disciplinele BRC și ARL	Demonstrații practice, exerciții aplicative, discuții interactive, lucru individual	Configurarea topologiilor de bază în mediul de simulare; temele vor fi disponibile pe Google Classroom
2. Comunicarea în rețea și între rețele.	Demonstrații practice, exerciții aplicative, studii de caz	Analiza mecanismelor de comunicare și configurarea parametrilor de rețea
3. Switch Security	Demonstrații practice, exerciții aplicative	Configurarea mecanismelor de securitate la nivelul switch-ului
4. Securizarea porturilor unui switch	Exerciții practice, lucru individual	Implementarea mecanismelor de protecție pentru porturile unui switch
5. DHCP Snooping și DAI	Demonstrații practice, exerciții aplicative	Analiza și prevenirea atacurilor bazate pe DHCP și ARP
6. Implementarea ACL standard în mediul de simulare.	Exerciții aplicative, demonstrații practice	Configurarea și testarea listelor de control al accesului
7. Implementare ACL extins în mediul de simulare.	Exerciții aplicative, lucru individual	Filtrarea traficului în rețea utilizând ACL extinse
8. NAT și PAT	Demonstrații practice, exerciții aplicative	Configurarea mecanismelor de translație a adreselor în rețea
9. Nmap	Demonstrații practice, studii de caz	Utilizarea instrumentelor de scanare pentru identificarea vulnerabilităților
10. Metasploit	Demonstrații practice, exerciții aplicative	Analiza vulnerabilităților și testarea mecanismelor de securitate
11. SEToolkit	Demonstrații practice, studii de caz	Simularea atacurilor de tip inginerie socială
12. Exercițiu Practic de tip CTF (Capture the Flag)	Activitate practică, lucru în echipă, evaluare aplicativă	Aplicarea integrată a cunoștințelor dobândite în scenarii practice

Bibliografie

1. Laura Chappell – **Wireshark Network Analysis**
2. Wendell Odom – **CCENT/CCNA ICND1 100–105 Official Cert Guide**
3. Paul Browning – **101 Labs – Cisco CCNA**
4. Wendell Odom – **CCNA 200-301 Official Cert Guide, Volume 1 & 2**

8. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

Conținuturile disciplinei **Securitate Informatică** sunt corelate cu evoluțiile actuale din domeniul securității cibernetice și cu standardele academice și profesionale promovate de comunitatea științifică și de organizațiile internaționale din domeniul tehnologiei informației.

Materialul de curs și laborator este în conformitate cu programa universitară și se regăsește în planurile de învățământ al universităților din țară și străinătate, corelat cu nevoile mediului economic.

Prin activitățile desfășurate în cadrul cursurilor și laboratoarelor, studenții dobândesc competențe practice privind analiza vulnerabilităților, utilizarea instrumentelor de securitate și implementarea mecanismelor de protecție a sistemelor informatice. Aceste competențe sunt relevante pentru domenii precum administrarea rețelelor, securitatea sistemelor informatice, testarea securității aplicațiilor și analiza incidentelor de securitate. Disciplina contribuie la formarea competențelor necesare pentru integrarea absolvenților pe piața muncii în domeniul IT, răspunzând cerințelor angajatorilor care solicită specialiști capabili să identifice riscurile de securitate și să implementeze soluții eficiente pentru protejarea sistemelor și a datelor informatice.

9. Evaluare

Tip de activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
9.1. Curs	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs	Test online (grilă) sau lucrare scrisă (grilă), și/sau prezentarea unei teme de cercetare din domeniul cursului.	60%
9.2. Laborator	Abilitatea de rezolvare a unor probleme specifice domeniului, Prezență, (inter)activitate în timpul orelor de laborator	Prezentare proiect	40%

9.3. Standard minim de performanță

Pentru obținerea notei **minime de promovare (5)**, studentul trebuie să demonstreze:

- Înțelegerea conceptelor fundamentale și a noțiunilor utilizate în domeniul securității informatice, evidențiată prin participarea activă la discuțiile și activitățile desfășurate în cadrul cursurilor și laboratoarelor.
- Capacitatea de a aplica corect conceptele și metodele studiate în rezolvarea exercițiilor și a activităților practice realizate la laborator.
- Capacitatea de analiză critică, din perspectiva securității informatice, a unui studiu de caz prezentat sau analizat în cadrul cursului sau laboratorului.
- Utilizarea și explicarea corectă a termenilor specifici domeniului securității informațiilor.

Promovarea disciplinei presupune obținerea minimum 50% din punctajul total, conform criteriilor de evaluare stabilite în fișa disciplinei.

Pentru nota 7-8:

Studentul demonstrează o bună înțelegere a conceptelor și metodelor de securitate informatică și este capabil să aplice corect cunoștințele dobândite în analiza unor situații concrete. Poate identifica vulnerabilități, interpreta rezultatele obținute în cadrul activităților practice și propune soluții adecvate pentru îmbunătățirea securității sistemelor informatice.

Pentru nota 9-10:

Studentul demonstrează o înțelegere aprofundată a conceptelor și tehnologiilor de securitate informatică și capacitatea de a analiza critic și integra cunoștințele dobândite. Poate evalua complex situații de securitate, utiliza instrumente specifice pentru identificarea vulnerabilităților și propune soluții argumentate pentru protejarea sistemelor informatice.

Nota finală reflectă nivelul de cunoaștere a conceptelor teoretice, implicarea în activitățile practice și capacitatea de aplicare a cunoștințelor dobândite.

Notă:

1) Regimul disciplinei (conținut) - pentru nivelul de licență se alege una din variantele: DF (disciplină fundamentală) / DS (disciplină de specialitate) / DC (disciplină complementară)

2) Regimul disciplinei (obligativitate) - se alege una din variantele: DO=discipline obligatorii (impuse) / DOP=discipline opționale/ DFC (disciplină facultativă).

Data completării

15.02.2026

Titular de curs

Conf.univ.dr. Alin-Daniel MUNTEANU

Titular de laborator

Valenin MARIA

Data avizării în departament

20.02.2026

Director de departament

Conf.univ.dr. Victoria IORDAN