Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti
Facultatea de Electronică, Telecomunicaţii şi
Tehnologia Informaţiei

FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti**
1.2 Facultatea	**Electronică, Telecomunicaţii şi Tehnologia Informaţiei**
1.3 Departamentul	**Telecomunicaţii**
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
1.5 Ciclul de studii	Masterat
1.6 Specializarea	Managementul Serviciilor şi Reţelelor

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Managementul securităţii reţelelor şi serviciilor			
2.2 Titularul activităţilor de curs				S.l./Lect. Dr. Laurentiu BOICESCU			
2.3 Titularul activităţilor de seminar / laborator				S.l./Lect. Dr. Laurentiu BOICESCU			
2.4 Anul de studiu	1	2.5 Semestrul	2	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		S	2.9 Codul disciplinei	5		2.10 Tipul de notare	Nota

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

3.1 Număr de ore pe săptămână	3	Din care: 3.2 curs	2	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuţia fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notiţe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii şi eseuri					54
Tutorat					0
Examinări					4
Alte activităţi (dacă există):					0

3.7 Total ore studiu individual	58.00
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Programarea calculatoarelor Arhitecturi si protocoale de comunicatii Retele de comunicatii Arhitecturi pentru retele si servicii
4.2 de rezultate ale învăţării	Cunoştinţe în domeniul reţelelor de comunicaţii

5. Condiţii necesare pentru desfăşurarea optimă a activităţilor didactice (acolo unde este cazul)

5.1 Curs	Conform regulamentului studiilor universitare în UPB. Cursul se va desfăşura într-o sală dotată cu videoproiector şi computer.
5.2 Seminar/ Laborator/Proiect	Laboratorul se va desfăşura într-o sală cu dotare specifică, care trebuie să includă: videoproiector, sisteme de calcul cu mediu de dezvoltare NetBeans IDE, Server web (Apache Tomcat), Server de baze de date (MySQL), hipervizor pentru masini virtuale (VirtualBox)

6. Obiectiv general *(Se referă la intenţiile profesorilor pentru studenţi, la ceea ce studenţii vor fi învăţaţi în timpul cursului. Oferă o orientare cu privire la locul cursului în cadrul domeniului ştiinţific abordat, precum şi la rolul pe care acesta îl are în cadrul specializării studiate. Vor fi descrise de o manieră generală tematicile abordate, justificarea includerii cursului în planul de învăţământ al specializării studiate etc.)*

Disciplina are ca obiectiv dobândirea cunoştinţelor de bază privind managementul securităţii informaţiei şi a reţelelor de comunicaţii, precum şi principalele vulnerabilităţi, atacuri şi mecanisme de protecţie, precum şi a abilităţii de a analiza nivelul de securitate al unei reţele şi de a proiecta sisteme de protecţie a informaţiei, sistemelor de calcul şi reţelelor de comunicaţii.
Se urmăresc: completarea pregătirii studenţilor în domeniul tehnologiilor software (şi hardware) avansate pentru protecţia informaţiei si reţelelor de comunicaţii, dobândirea cunoştinţelor necesare testării şi evaluării securităţii reţelelor, dobândirea cunoştinţelor necesare proiectării sistemelor avansate, multistrat, de protecţie a reţelelor de comunicaţii.

7. Competenţe *(Capacitatea dovedită de a utiliza cunoştinţe, aptitudini şi abilităţi personale, sociale şi/sau metodologice în situaţii de muncă sau de studiu şi pentru dezvoltarea profesională şi personală. Reflectă cerinţele angajatorilor.)*

Specifice	Operarea cu fundamente ştiinţifice, inginereşti şi ale managementului securităţii informaţiei Aplicarea cunoştinţelor şi conceptelor de bază, în scopul managementului securizării reţelelor de comunicaţii Utilizarea limbajelor de programare şi a instrumentelor software specializate, cu orientare către managementul securităţii informaţiei şi reţelelor de comunicaţii
Transversale (generale)	Analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluţii consacrate, asigurând astfel îndeplinirea sarcinilor profesionale Adaptarea la noile tehnologii, dezvoltarea profesională şi personală, prin formare continuă folosind surse de documentare tipărite, software specializat şi resurse electronice în limba română şi, cel puţin, într-o limbă de circulaţie internaţională.

8. Rezultatele învăţării *(Sunt enunţuri sintetice referitoare la ceea ce un student va fi capabil să facă sau să demonstreze la finalizarea unui curs. Rezultatele învăţării reflectă realizările studentului şi mai puţin intenţiile profesorului. Rezultatele învăţării informează studenţii despre ceea ce se aşteaptă de la ei din punct de vedere al performanţei, pentru a obţine notele şi creditele dorite. Sunt definite în termeni concreţi, folosind verbe similare exemplelor de mai jos şi indică ceea ce se va urmări prin evaluare. Rezultatele învăţării vor fi astfel redactate încât să fie evidenţiată clar relaţia faţă de competenţele definite la punctul 7.)*

Cunoştinţe	*Rezultatul asimilării de informaţii prin învăţare. Cunoştinţele reprezintă ansamblul de fapte, principii, teorii şi practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice şi/sau faptice.* **principalele** mecanisme hardware şi software utilizate în cadrul domeniului (sisteme de control al accesului, de detecţie şi prevenţie a intruziunilor, de testare şi evaluare a securităţii reţelelor, etc.) **principalele mecanisme de asigurare a confidenţialităţii informaţiei (criptografie simetrică/asimetrică, infrastructura cu chei publice, etc.)** **modele arhitecturale utilizate** în securitatea reţelelor şi serviciilor
Aptitudini	*Capacitatea de a aplica cunoştinţe şi de a utiliza know-how pentru a duce la îndeplinire sarcini şi a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive şi creative) sau practice (implicând dexteritate manuală şi utilizarea de metode, materiale, unelte şi instrumente).* Utilizează argumentat principii specifice în vederea securizării reţelelor şi serviciilor. Lucrează în echipă. Elaborează un text ştiinţific. Verifică experimental soluţii identificate. Rezolvă aplicaţii practice. Analizează şi compară tehnologii şi biblioteci pentru securitatea reţelelor şi serviciilor. Identifică soluţii şi elaborează planuri de rezolvare/proiecte. Argumentează soluţiile identificate/modurile de rezolvare.
Responsabilitate şi autonomie	*Capacitatea cursantului de a aplica în mod autonom şi responsabil cunoştinţele şi aptitudinile sale.* Respectă principiile de etică academică, citând corect sursele bibliografice utilizate. Demonstrează receptivitate pentru contexte noi de învăţare. Manifestă colaborare cu ceilalţi colegi şi cadre didactice în desfăşurarea activităţilor didactice Demonstrează autonomie în organizarea situaţiei/contextului de învăţare sau a situaţiei problemă de rezolvat Conştientizează valoarea contribuţiei sale în domeniul ingineriei la identificarea de soluţii viabile/sustenabile care să rezolve probleme din viaţa socială şi economică (responsabilitate socială). Analizează şi valorifică oportunităţi de afaceri/de dezvoltare antreprenorială în domeniul de specialitate. Demonstrează abilităţi de management al situaţiilor din viaţa reală (gestionarea timpului, colaborare, conflict).

9. Metode de predare *(Se vor avea în vedere metode care să asigure predarea centrată pe student. Se va descrie modul în care se asigură participarea studenţilor la stabilirea propriului parcurs de învăţare, cum se identifică eventualele rămâneri în urmă şi ce măsuri remediale se adoptă în astfel de cazuri.)*

Pornindu-se de la analiza caracteristicilor de învăţare ale studenţilor şi de la nevoile lor specifice, procesul de predare va explora metode de predare atât expozitive (prelegerea, expunerea), cât şi conversative-interactive, bazate pe modele de învăţare prin descoperire facilitate de explorarea directa şi indirectă a realităţii (experimentul, demonstraţia, modelarea), dar şi pe metode bazate pe acţiune, precum exerciţiul, activităţile practice şi rezolvarea de probleme.
În activitatea de predare vor fi utilizate prelegeri, în baza unor prezentări Power Point care vor fi puse la dispoziţia studenţilor. Fiecare curs va debuta cu recapitularea capitolelor deja parcurse, cu accent asupra noţiunilor parcurse la ultimul curs. Primele cursuri vor recapitula noţiunile de programare orientată pe obiecte studiate în semestrele precedente.
Prezentările utilizează imagini şi scheme, astfel încât informaţiile prezentate să fie uşor de înţeles şi asimilat.
Acestă disciplină oferă informaţii şi activităţi practice menite să-i sprijine pe studenţi în eforturile de

învăţare şi de dezvoltare a unor relaţii optime de colaborare şi comunicare într-un climat favorabil învăţării prin descoperire.
Se va încuraja abilitatea de lucru în echipă pentru rezolvarea diferitelor sarcini de învăţare.

10. Conţinuturi

CURS		
Capitolul	**Conţinutul**	**Nr. ore**
1	Noţiuni generale de securitate a informaţiei şi reţelelor de comunicaţii Noţiuni introductive Securitatea informaţiei Mecanismele de securitate	2
2	Vulnerabilităţi şi atacuri asupra serviciilor şi reţelelor de comunicaţii Vulnerabilităţile principalelor sisteme de operare si tehnologiilor de comunicaţii Atacuri asupra sistemelor şi protocoalelor de comunicaţii. Atacuri “Zero-Day”. Identificarea vulnerabilităţilor calculatoarelor şi reţelelor de calculatoare. Baze de date de vulnerabilităţi	4
3	Securitatea informaţiei. Criptografie. Noţiuni generale de criptografie Vulnerabilităţi şi atacuri asupra sistemelor criptografice Clase de sisteme criptografice Criptografie simetrică şi asimetrică Certificate criptografice Semnătura digitală Infrastructura cu chei publice	8
4	Tehnologii hardware şi software de protecţie a sistemelor de calcul şi serviciilor software. Principiile securizării sistemelor de calcul. Principiul protecţiei stratificate. Sisteme hardware şi software de autentificare. Sisteme biometrice. Tehnologii avansate. Coprocesoare de securitate. TPM (Trusted Platform Module) Securitatea sistemului de operare Linux Securitatea serviciilor web	6
5	Managementul securităţii reţelelor de telecomunicaţii Principiul protecţiei stratificate în reţele de comunicaţii. Zone demilitarizate. Sisteme IDS/IPS şi firewall; modalităţi de amprentare a traficului date în reţea şi identificare a atacurilor Studiul şi deturnarea atacurilor prin sisteme Honeypot Sisteme de management al securităţii reţelelor de comunicaţii; managementul informaţiei şi evenimentelor de securitate	6
6	Mecanisme de Autentificare, Autorizare si jurnalizare a Accesului (AAA) Principiile sistemelor AAA Sisteme AAA consacrate. Protocolul şi serverul Radius Securitatea reţelelor fără fir (WLAN 802.11)	2
	Total:	28

Bibliografie:

Note de curs, disponibile pe platforma Moodle

"**Information security management handbook**", 6th edition, Auerbach publications, 2007, ISBN: 978-0-8493-7495-1

"**Computer and Information Security Handbook**", Morgan Kaufmann Publishers, 2009, ISBN: 978-0-12-374354-1

"**Hardware based computer security techniques to defeat hackers**", John Wiley and Sons, 2008, ISBN: 978-0-470-19339-6

W. Stallings, L. Brown, "**Computer Security: Principles and Practice (2nd Edition)**", Prentice Hall, 2008, ISBN: 978-0-13-277506-9

A. J. Menezes, P. C. van Oorschot; S. A. Vanstone, "**Handbook of Applied Cryptography**", CRC Press, 1996, ISBN: 0-8493-8523-7

B. Schneier, "**Applied Cryptography: Protocols, Algorithms and Source Code in C**" (20th Anniversary Edition), Wiley, 2015, ISBN: 978-1-119-09672-6

W. Stallings, "**Cryptography and Network Security**" (4th Edition), Prentice Hall, 2005, 978-0-13-187316-2

D. Littlejohn Shinder, M. Cross, "**Scene of the Cybercrime**" 2nd edition, Syngress Publishing, Elsevier, 2008, ISBN: 978-1-59749-276-8

V. Patriciu, M. Ene-Pietroşanu, I. Bica, I. Priescu, "**Semnaturi electronice si securitate informatica**", Bic All, 2006, ISBN: 973-571-564-3

K. Scarfone, W. Jansen, M. Tracy , "Recommendations of the National Institute of Standards and Technology", National Institute of Standards and Technology, 2008, http://csrc.nist.gov/publications/nistpubs/800-123/SP800-123.pdf

G. Stoneburner, A. Goguen, A. Feringa, "Risk Management Guide for Information Technology Systems", NIST SP 800-30, July 2002, http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

ISECOM, „Open Source Security Testing Methodology Manual (OSSTMM)", www.isecom.org/mirror/OSSTMM.3.pdf

LABORATOR

Nr. crt.	Conţinutul	Nr. ore
1	Managementul cheilor publice Familiarizare cu sistemul de operare Linux Managementul cheilor publice Infrastructura PKI Aplicaţii practice ale certificatelor criptografice. HTTPs	4
2	Detecţia atacurilor in cadrul reţelelor TCP/IP Mecanisme de filtrare a traficului. Sisteme firewall Sisteme de detecţie şi prevenţie a intruziunilor Managementul informaţiei şi evenimentelor de securitate	4
3	Managementul vulnerabilităţilor Mecanisme de testare a securităţii reţelelor de telecomunicaţii. Identificarea vulnerabilităţilor şi ameninţărilor asupra reţelelor de telecomunicaţii	4
4	Colocviu final de laborator	2
	Total:	

Bibliografie:

A se vedea referintele de mai sus.
Platforme de laborator, disponibile pe platforma Moodle

11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	- cunoaşterea noţiunilor teoretice fundamentale; - cunoaşterea modului de aplicare a teoriei la probleme specifice; - analiza tehnicilor şi metodelor teoretice.	Verificare în timpul semestrului la date fixate la începutul semestrului. Verificare finala in timpul sesiunii.	40%
11.5 Seminar/laborator/proiect	- dezvoltarea aptitudinilor de configurare, operare si implementare a mecanismelor si sistemelor de management al securităţii	Colocviu final de laborator, cuprinzând o componentă teoretică şi o componentă practică, prin verificarea modului de rezolvare (implementare, testare, funcţionare) de către student a unei probleme practice.	30%
	Teme de casă: - capacitatea de analiză şi sinteză a temei abordate - capacitatea de implementare a aplicaţiei practice, conform cerinţelor - capacitatea de prezentare şi argumentare soluţiei practice implementate	Susţinerea finală a proiectului realizat	30%
11.6 Condiţii de promovare			
Obţinerea a 50% din punctajul total. Obţinerea a 50% din punctajul aferent activităţii pe parcursul semestrului.			

12. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor angajatorilor şi asociaţiilor profesionale reprezentative din domeniul aferent programului, precum şi cu stadiul actual al cunoaşterii în domeniul ştiinţific abordat şi practicile în instituţii de învăţământ superior din Spaţiul European al Învăţământului Superior (SEÎS)

Prin activităţile desfăşurate, studenţii dobândesc abilitatea de a oferi soluţii unor probleme şi de a propune idei de îmbunătăţire a situaţiei existente în domeniul securităţii reţelelor şi serviciilor de telecomunicaţii.
În dezvoltarea conţinutului disciplinei s-au avut în vedere cunoştinţe, aspecte teoretice şi practice, precum şi fenomene descrise de literatura de specialitate, cercetările proprii publicate şi experienţa titularilor disciplinei.
Prin activitatea de disciplină se are în vedere dezvoltarea abilităţilor absolventului de a proiecta şi implementa noi mecanisme pentru securitate, precum şi de a analiza şi depana mecanismele existente, inclusiv în vederea îmbunătăţirii acestora. În acest fel, absolvenţii cursului pot contribui la îmbunătăţirea mediului economic, în domeniul securităţii retelelor si serviciilor de telecomunicaţii.

Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti

Facultatea de Electronică, Telecomunicaţii şi

Tehnologia Informaţiei

Data completării	Titular de curs	Titular(i) de aplicaţii
21.09.2026	S.l./Lect. Dr. Laurentiu BOICESCU	S.l./Lect. Dr. Laurentiu BOICESCU

Data avizării în departament	Director de departament
22.09.2026	Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul Facultăţii	Decan
22.09.2026	Prof. Dr. Mihnea Udrea