



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituția de învățământ superior	Universitatea Națională de Știință și Tehnologie Politehnica București
1.2 Facultatea	Electronică, Telecomunicații și Tehnologia Informației
1.3 Departamentul	Telecomunicații
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
1.5 Ciclu de studii	Masterat
1.6 Specializarea	Managementul Serviciilor și Rețelelor

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)	Managementul securității rețelelor și serviciilor						
2.2 Titularul activităților de curs	S.I./Lect. Dr. Laurentiu BOICESCU						
2.3 Titularul activităților de seminar / laborator	S.I./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 activităților 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 învățământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie și notițe Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					54
Tutorat					0
Examinări					4
Alte activități (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. Precondiții (acolo unde este cazul)

4.1 de curriculum	Programarea calculatoarelor Arhitecturi si protocoale de comunicatii Rețele de comunicatii Arhitecturi pentru rețele si servicii
4.2 de rezultate ale învățării	Cunoștințe în domeniul rețelelor de comunicații

5. Condiții necesare pentru desfășurarea optimă a activităților didactice (acolo unde este cazul)



5.1 Curs	Conform regulamentului studiilor universitare în UPB. Cursul se va desfășura într-o sală dotată cu videoproiector și computer.
5.2 Seminar/ Laborator/Proiect	Laboratorul se va desfășura 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 mașini virtuale (VirtualBox)

6. Obiectiv general *(Se referă la intențiile profesorilor pentru studenți, la ceea ce studenții vor fi învățați în timpul cursului. Oferă o orientare cu privire la locul cursului în cadrul domeniului științific abordat, precum și 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 învățământ al specializării studiate etc.)*

Disciplina are ca obiectiv dobândirea cunoștințelor de bază privind managementul securității informației și a rețelelor de comunicații, precum și principalele vulnerabilități, atacuri și mecanisme de protecție, precum și a abilității de a analiza nivelul de securitate al unei rețele și de a proiecta sisteme de protecție a informației, sistemelor de calcul și rețelelor de comunicații.

Se urmăresc: completarea pregătirii studenților în domeniul tehnologiilor software (și hardware) avansate pentru protecția informației și rețelelor de comunicații, dobândirea cunoștințelor necesare testării și evaluării securității rețelelor, dobândirea cunoștințelor necesare proiectării sistemelor avansate, multistrat, de protecție a rețelelor de comunicații.

7. Competențe *(Capacitatea dovedită de a utiliza cunoștințe, aptitudini și abilități personale, sociale și/sau metodologice în situații de muncă sau de studiu și pentru dezvoltarea profesională și personală. Reflectă cerințele angajatorilor.)*

Specifice	Operarea cu fundamente științifice, ingineresti și ale managementului securității informației Aplicarea cunoștințelor și conceptelor de bază, în scopul managementului securizării rețelelor de comunicații Utilizarea limbajelor de programare și a instrumentelor software specializate, cu orientare către managementul securității informației și rețelelor de comunicații
Transversale (generale)	Analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluții consacrate, asigurând astfel îndeplinirea sarcinilor profesionale Adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare tipărite, software specializat și resurse electronice în limba română și, cel puțin, într-o limbă de circulație internațională.

8. Rezultatele învățării *(Sunt enunțuri sintetice referitoare la ceea ce un student va fi capabil să facă sau să demonstreze la finalizarea unui curs. Rezultatele învățării reflectă realizările studentului și mai puțin intențiile profesorului. Rezultatele învățării informează studenții despre ceea ce se așteaptă de la ei din punct de vedere al performanței, pentru a obține notele și creditele dorite. Sunt definite în termeni concreți, folosind verbe similare exemplelor de mai jos și indică ceea ce se va urmări prin evaluare. Rezultatele învățării vor fi astfel redactate încât să fie evidențiată clar relația față de competențele definite la punctul 7.)*



Cunoștințe	<i>Rezultatul asimilării de informații prin învățare. Cunoștințele reprezintă ansamblul de fapte, principii, teorii și practici legate de un anumit domeniu de muncă sau de studiu. Pot fi teoretice și/sau faptice.</i> principalele mecanisme hardware și software utilizate în cadrul domeniului (sisteme de control al accesului, de detecție și prevenție a intruziunilor, de testare și evaluare a securității rețelelor, etc.) principalele mecanisme de asigurare a confidențialității informației (criptografie simetrică/asimetrică, infrastructura cu chei publice, etc.) modele arhitecturale utilizate în securitatea rețelelor și serviciilor
Aptitudini	<i>Capacitatea de a aplica cunoștințe și de a utiliza know-how pentru a duce la îndeplinire sarcini și a rezolva probleme. Aptitudinile sunt descrise ca fiind cognitive (implicând utilizarea gândirii logice, intuitive și creative) sau practice (implicând dexteritate manuală și utilizarea de metode, materiale, unelte și instrumente).</i> Utilizează argumentat principii specifice în vederea securizării rețelelor și serviciilor. Lucrează în echipă. Elaborează un text științific. Verifică experimental soluții identificate. Rezolvă aplicații practice. Analizează și compară tehnologii și biblioteci pentru securitatea rețelelor și serviciilor. Identifică soluții și elaborează planuri de rezolvare/proiecte. Argumentează soluțiile identificate/modurile de rezolvare.
Responsabilitate și autonomie	<i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale. Respectă principiile de etică academică, citând corect sursele bibliografice utilizate.</i> Demonstrează receptivitate pentru contexte noi de învățare. Manifestă colaborare cu ceilalți colegi și cadre didactice în desfășurarea activităților didactice Demonstrează autonomie în organizarea situației/contextului de învățare sau a situației problemă de rezolvat Conștientizează valoarea contribuției sale în domeniul ingineriei la identificarea de soluții viabile/sustenabile care să rezolve probleme din viața socială și economică (responsabilitate socială). Analizează și valorifică oportunități de afaceri/de dezvoltare antreprenorială în domeniul de specialitate. Demonstrează abilități de management al situațiilor din viața 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 studenților la stabilirea propriului parcurs de învățare, cum se identifică eventualele rămăneri în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)

Pornindu-se de la analiza caracteristicilor de învățare ale studenților și de la nevoile lor specifice, procesul de predare va explora metode de predare atât expositive (prelegerea, expunerea), cât și conservative-interactive, bazate pe modele de învățare prin descoperire facilitate de explorarea directă și indirectă a realității (experimentul, demonstrația, modelarea), dar și pe metode bazate pe acțiune, precum exercițiul, activitățile practice și rezolvarea de probleme.

În activitatea de predare vor fi utilizate prelegeri, în baza unor prezentări Power Point care vor fi puse la dispoziția studenților. Fiecare curs va debuta cu recapitularea capitolelor deja parcurse, cu accent asupra noțiunilor parcurse la ultimul curs. Primele cursuri vor recapitula noțiunile de programare orientată pe obiecte studiate în semestrele precedente.

Prezentările utilizează imagini și scheme, astfel încât informațiile prezentate să fie ușor de înțeles și asimilat. Această disciplină oferă informații și activități practice menite să-i sprijine pe studenți în eforturile de



învățare și de dezvoltare a unor relații optime de colaborare și comunicare într-un climat favorabil învățării prin descoperire.

Se va încuraja abilitatea de lucru în echipă pentru rezolvarea diferitelor sarcini de învățare.

10. Conținuturi

CURS		
Capitolul	Conținutul	Nr. ore
1	Noțiuni generale de securitate a informației și rețelelor de comunicații Noțiuni introductive Securitatea informației Mecanismele de securitate	2
2	Vulnerabilități și atacuri asupra serviciilor și rețelelor de comunicații Vulnerabilitățile principalelor sisteme de operare și tehnologiilor de comunicații Atacuri asupra sistemelor și protocoalelor de comunicații. Atacuri “Zero-Day”. Identificarea vulnerabilităților calculatoarelor și rețelelor de calculatoare. Baze de date de vulnerabilități	4
3	Securitatea informației. Criptografie. Noțiuni generale de criptografie Vulnerabilități și atacuri asupra sistemelor criptografice Clase de sisteme criptografice Criptografie simetrică și asimetrică Certificate criptografice Semnătura digitală Infrastructura cu chei publice	8
4	Tehnologii hardware și software de protecție a sistemelor de calcul și serviciilor software. Principiile securizării sistemelor de calcul. Principiul protecției stratificate. Sisteme hardware și 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 securității rețelelor de telecomunicații Principiul protecției stratificate în rețele de comunicații. Zone demilitarizate. Sisteme IDS/IPS și firewall; modalități de amprentare a traficului date în rețea și identificare a atacurilor Studiul și deturnarea atacurilor prin sisteme Honeypot Sisteme de management al securității rețelelor de comunicații; managementul informației și evenimentelor de securitate	6
6	Mecanisme de Autentificare, Autorizare și jurnalizare a Accesului (AAA) Principiile sistemelor AAA Sisteme AAA consacrate. Protocolul și serverul Radius Securitatea rețelelor 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-Pietroșanu, I. Bica, I. Priescu, “**Semnături electronice și securitate informatică**”, 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.	Conținutul	Nr. ore
1	Managementul cheilor publice Familiarizare cu sistemul de operare Linux Managementul cheilor publice Infrastructura PKI Aplicații practice ale certificatelor criptografice. HTTPs	4
2	Detecția atacurilor în cadrul rețelelor TCP/IP Mecanisme de filtrare a traficului. Sisteme firewall Sisteme de detecție și prevenție a intruziunilor Managementul informației și evenimentelor de securitate	4
3	Managementul vulnerabilităților Mecanisme de testare a securității rețelelor de telecomunicații. Identificarea vulnerabilităților și amenințărilor asupra rețelelor de telecomunicații	4
4	Colocviu final de laborator	2
Total:		

Bibliografie:

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



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



11. Evaluare

Tip activitate	11.1 Criterii de evaluare	11.2 Metode de evaluare	11.3 Pondere din nota finală
11.4 Curs	- cunoașterea noțiunilor teoretice fundamentale; - cunoașterea modului de aplicare a teoriei la probleme specifice; - analiza tehnicilor și metodelor teoretice.	Verificare în timpul semestrului la date fixate la începutul semestrului. Verificare finală în timpul sesiunii.	40%
11.5 Seminar/laborator/proiect	- dezvoltarea aptitudinilor de configurare, operare și implementare a mecanismelor și sistemelor de management al securității	Colocviu final de laborator, cuprinzând o componentă teoretică și o componentă practică, prin verificarea modului de rezolvare (implementare, testare, funcționare) de către student a unei probleme practice.	30%
	Teme de casă: - capacitatea de analiză și sinteză a temei abordate - capacitatea de implementare a aplicației practice, conform cerințelor - capacitatea de prezentare și argumentare soluției practice implementate	Susținerea finală a proiectului realizat	30%
11.6 Condiții de promovare			
Obținerea a 50% din punctajul total. Obținerea a 50% din punctajul aferent activității pe parcursul semestrului.			

12. Coroborarea conținutului disciplinei cu așteptările reprezentanților angajatorilor și asociațiilor profesionale reprezentative din domeniul aferent programului, precum și cu stadiul actual al cunoașterii în domeniul științific abordat și practicile în instituții de învățământ superior din Spațiul European al Învățământului Superior (SEİS)

Prin activitățile desfășurate, studenții dobândesc abilitatea de a oferi soluții unor probleme și de a propune idei de îmbunătățire a situației existente în domeniul securității rețelilor și serviciilor de telecomunicații.

În dezvoltarea conținutului disciplinei s-au avut în vedere cunoștințe, aspecte teoretice și practice, precum și fenomene descrise de literatura de specialitate, cercetările proprii publicate și experiența titularilor disciplinei.

Prin activitatea de disciplină se are în vedere dezvoltarea abilităților absolventului de a proiecta și implementa noi mecanisme pentru securitate, precum și de a analiza și depana mecanismele existente, inclusiv în vederea îmbunătățirii acestora. În acest fel, absolvenții cursului pot contribui la îmbunătățirea mediului economic, în domeniul securității rețelilor și serviciilor de telecomunicații.



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



Data completării

Titular de curs

Titular(i) de aplicații

25.09.2025

S.I./Lect. Dr. Laurentiu
BOICESCU

S.I./Lect. Dr. Laurentiu
BOICESCU

Data avizării în departament

Director de departament

26.09.2025

Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul
Facultății

Decan

26.09.2025

Prof. Dr. Mihnea Udrea