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	Tehnologii Software Avansate pentru Comunicaţii

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Securitatea informaţiei şi a reţelelor de comunicaţii			
2.2 Titularul activităţilor de curs				S.l./Lect. Dr. Radu Lupu			
2.3 Titularul activităţilor de seminar / laborator				S.l./Lect. Dr. Radu Lupu			
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	3		2.10 Tipul de notare	Nota

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

3.1 Număr de ore pe săptămână	4	Din care: 3.2 curs	2	3.3 seminar/laborator	2
3.4 Total ore din planul de învăţământ	56	Din care: 3.5 curs	28	3.6 seminar/laborator	28
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					66
Tutorat					1
Examinări					2
Alte activităţi (dacă există):					0

3.7 Total ore studiu individual	69.00
3.8 Total ore pe semestru	125
3.9 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Parcurgerea şi/sau promovarea următoarelor discipline: • Programarea Calculatoarelor, • Structuri de Date şi Algoritmi, • Arhitecturi şi Protocoale pentru Comunicaţii, • Reţele şi Servicii, • Arhitecturi pentru Reţele şi Servicii, • Securitatea Reţelelor şi Servicilor
4.2 de rezultate ale învăţării	Acumularea următoarelor cunoştinţe: • aprofundarea principalelor aplicaţii ale sistemelor criptografice; • abilităţi de management al riscurilor de securitate în reţele Internet (identificarea ameninţărilor a atacurilor şi a vulnerabilităţilor de securitate); • capabilităţi de proiectare a arhitecturilor de securitate pentru servicii şi reţele de acces ptr. comunicaţii de date; • capacitatea de a implementa şi analiza principalele mecanisme şi servicii de securitate

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

5.1 Curs	Cursul se va desfăşura într-o sală dotată cu: • videoproiector şi computer, • access online, inclusiv la serviciul MS Teams şi Moodle, • tablă de scris tradiţională sau virtuală (en. whiteboard)
5.2 Seminar/ Laborator/Proiect	Laboratorul se va desfăşura într-o sală cu dotare specifică, care trebuie să includă: sisteme de calcul PC cu sistem de operare Windows+WSL2 sau Linux(Debian), emulator de reţea, servicii de reţea, tehnologii de securitate cu sursa-deschisă, unelte software cu sursa-deschisă ptr. generare şi analiza de trafic de reţea

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.)*

Această disciplină îşi propune să ofere o pregatire studenţilor la nivel începător şi mediu care va include cunoaşterea principalelor noţiuni generale, principii, modele, arhitecturi şi mecanisme de securitate, dar şi formarea unor abilităţi pentru a rezolva probleme practice de securitate.

Disciplina abordează ca tematică specifică implementarea unui proces simplu pentru managementul securităţii aplicaţiilor software pentru comunicaţii. Dezvoltarea capacităţilor de identificare a problemelor de securitate tipice software-ului pentru comunicatii (presupune identificarea principalelor tipuri de atac şi a consecinţelor aferente) şi de selectare a celor mai eficiente soluţii de securizare preventive/reactive. Analiza şi evaluarea riscurilor de securitate şi intimizare pentru cele mai reprezentative servicii şi contexte de reţea Internet.

Abilitatea de a identifica şi opera cu cerinţele de configurare şi de funcţionare ale mecanismelor de securitate pornind de la un set de cerinţe de securitate specifice celor mai comune aplicaţii software pentru comunicatii şi ale utilizatorilor. Cunoaşterea celor mai comune configuraţii de sisteme de securitate de reţea şi a protocoalelor generice pentru securizarea comunicaţiilor şi pentru controlul accesului.

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	Demonstrează că deţine cunoştinţe de bază şi deţine aptitudini de aplicare a cunoştinţelor în domeniul securităţii informaţiei în domeniul serviciilor pentru comunicaţii peste Internet. Capacitatea de a identifica principalele ameninţări de securitate şi evaluarea riscurilor de securitate asociate celor mai comune sisteme de comuncaţii Internet. Aplică în practică cunoştinţele acumulate pentru operarea corectă a măsurilor de securitate IT evitând cele mai comune vulnerabilităţi specifice fazelor de management al sistemelor şi serviciilor pentru comunicaţii Internet. Definirea şi implementarea unor infrastructuri PKI simple pentru managementul cheilor publice. Aplică metode şi instrumente consacrate şi/sau standardizate pentru implementarea unui proces simplu pentru managementul riscurilor de securitate ale unui scenariu dat. Capacitatea de a specifica principalele cerinţe de securitate ale serviciilor pentru comunicaţii şi de analiză pentru a determina cele mai eficiente măsuri de securitate care pot garanta nivelul de securitate cerut de un anumit sistem pentru comunicaţii. Abilitatea de analiză şi clasificare a sistemelor de securitate Internet. Proiectarea unor arhitecturi şi configuraţii simple de securitate pentru prevenirea/detecţia vulnerabilităţilor de securitate. Argumentează şi analizează coerent şi corect contextul de aplicare a cunoştinţelor de bază ale domeniului, în evaluarea modului de de funcţionare a protocoalelor şi mecanismelor de securitate. Comunicare orala şi în scris în limba romană şi engleză: utilizează vocabularul ştiinţific specific domeniului (jargonul), în vederea comunicării eficace şi fără echivoc, în scris şi oral. Abilităţi de utilizare a mediului de comunicare Internet (ex. Google, servicii de arhivare de documente) şi capacitatea de analiză şi selectare a surselor bibliografice relevante online.
Transversale (generale)	Lucrează în echipă şi comunică eficient, coordonându-şi eforturile cu ceilalţi pentru rezolvarea de situaţii problemă de complexitate medie. Autonomie şi gândire critică: abilitatea de a gândi în termeni ştiinţifici, de a căuta şi analiza date în mod independent, precum şi de a desprinde şi prezenta concluzii / identifica soluţii. Capacitate de analiză şi sinteză: prezintă în mod sintetic cunoştinţele dobândite, ca urmare a unui proces de analiză sistematică. Respectă principiile de etică academică: în activitatea de documentare citează corect sursele bibliografice utilizate. Gestionarea socio-emoţională adecvată a unor situaţii din viaţa reală/academică/profesională, demonstrând stăpânire de sine şi obiectivitate în luarea deciziilor sau în situaţii de stres.

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.* • Enumeră cele mai importante etape ale procesului de management al riscurilor de securitate pornind de la un scenariu de comunicare Internet. De asemenea, pentru fiecare categorie de măsuri de securitate poate numi corect principalele tehnologii aferente. Enumeră corect obiectivele atacurilor de securitate. • Defineşte noţiuni specifice domeniului (ameninţare, vulnerabilitati, atac, risc de securitate, nivel de securitate, obiective de securitate, cerinţe de securitate). • Descrie/clasifică simple arhitecturi de securitate, sisteme de securitate, procesele specifice managementului cheilor publice (PKI) şi structuri arbore pentru analiza atacurilor de reţea. • Evidenţiază relaţii între noţiunile specifice domeniului (enumerate mai sus)
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).* • Selectează şi grupează informaţii relevante pe baza unui scenariu predefinit în vederea analizei riscurilor de securitate pentru specificarea cerinţelor de securitate şi a măsurilor de securitate. • Utilizează argumentat principii specifice în vederea proiectării arhitecturilor de securitate şi în implementarea măsurilor de securitate pe baza unui set de cerinţe de securitate. • Lucrează productiv în echipă. • Rezolvă probleme practice propuse în cadrul lucrărilor de laborator/seminar. • Interpretează adecvat relaţii de cauzalitate (bunuri de valoare pentru organizaţie - ameniţări-resurse IT – vulnerabilităţi - atacuri - riscuri de securitate - cerinţe de securitate). • Analizează şi compară diverse clase de vulnerabilităţi, atacuri, mecanisme şi servicii de securitate. • Identifică soluţii arhitecturale şi servicii de securitate necesare pentru tratarea riscurilor de securitate. • Formulează concluzii la problemele soluţionate. • Argumentează soluţiile identificate/modurile de rezolvare.

Responsabilitate şi autonomie	*Capacitatea cursantului de a aplica în mod autonom şi responsabil cunoştinţele şi aptitudinile sale.* • Selectează surse bibliografice potrivite (inclusiv in limba engleza) şi le analizează. • Respectă principiile de etică academică, citând corect sursele bibliografice utilizate. • Manifestă colaborare cu ceilalţi colegi şi cadre didactice pentru depăşirea unor probleme în desfăşurarea activităţilor didactice • Demonstrează autonomie în organizarea situaţiei/contextului de învăţare sau a situaţiei problemă de rezolvat.

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.)*

Procesul de predare se va desfăşura folosind metode expozitive (prelegerea, expunerea), cât şi conversative-interactive, bazate pe învăţare prin descoperire directă şi indirectă a realităţii (experimentul, demonstraţia, modelarea), dar şi prin problematizare şi acţiune (exerciţiul, activităţile practice şi rezolvarea de probleme).

În activitatea de predare vor fi utilizate prelegeri, în baza unor prezentări Power Point sau diferite filmuleţe care vor fi puse la dispoziţia studenţilor. Fiecare curs va debuta cu recapitularea principalelor noţiuni deja studiate. Predarea se bazează pe folosirea videoproiectorului acoperind funcţia de comunicare şi demonstrativă. Materialele de curs sunt sub formă de note şi prezentări de curs care sunt disponibile în format electronic.

Prezentările utilizează imagini şi scheme, astfel încât informaţiile prezentate să fie uşor de înţeles şi asimilat.

Studenţii simulează, implementează, testează şi evaluează independent probleme prin utilizarea continuă a calculatorului şi a mediului software. De asemenea, se va exersa abilitatea de lucru în echipă pentru rezolvarea diferitelor sarcini de învăţare.

10. Conţinuturi

CURS		
Capitolul	**Conţinutul**	**Nr. ore**
1	Noţiuni de management al securităţii informaţiei (INFOSEC). Ameninţări, vulnerabilităţi şi atacuri în Internet. Agenţi de atac. Tratarea riscurilor de securitate si masuri de securitate.	6
2	Sisteme şi tehnici de securitate pentru reţeaua Internet. Sistemul firewall (caracteristici, elemente funcţionale, configuraţii, probleme şi soluţii). Sistemul pentru detecţia şi prevenirea intruziunilor-IDPS (arhitectura generică, caracteristici, performanţe, mecanisme pentru detecţie). Tehnici, mecanisme şi sisteme anti-(D)DoS. Tehnici şi sisteme anti-SPAM (mecanisme necriptografice şi criptografice, metoda Bayesiana).	8
3	Servicii generice de securitate pentru reţelele TCP/IP. Tehnologiile IPSec şi TLS. Protocoale si mecanisme criptografice aferente	4
4	Modele de arhitecturi şi principii de securitate pentru reţeaua Internet. Modelul punct-la-punct. Modelul pentru controlul accesului. Tehnici pentru specificarea politicilor de autorizare. Arhitectura IEEE 802.1x, AAA şi Single Sign-On	4

5	Securitatea reţelelor de acces radio WLAN, GSM şi 5G. Mecanisme de autentificare a entităţilor, asigurarea confidenţialităţii şi integrităţii datelor şi garantarea caracterului privat. Sistemele criptografice WEP, TKIP/WPA, CCMP/WPA2, WPA3	6
	Total:	28

Bibliografie:

1. R.Lupu, „Securitatea Informaţiei şi a Reţelelor de Comunicaţii”, Note de curs, Moodle@UNSTPB, iunie 2025, https://curs.upb.ro/2024/course/index.php?categoryid=1740
2. R.Shirey, „Internet Security Glossary, Version 2”, IETF, RFC 4949, http//www.ietf.org/rfc/rfc4949.txt, August 2007
3. A.Menezes, P. Van Oorschot, S.Vanstone, „Handbook of Applied Cryptography”, Ed. CRC Press 1996, ISBN 08493-8523-7
4. W.Stallings, L.Brown, „Computer Security.Principles and Practice”, Ed.Prentice Hall, ISBN 0-13-600424-5, 2008
5. J.Mirkovic, S.Dietrich, D.Dittrich, P.Reiher, „Internet Denial of Service: Attack and Defense Mechanisms”, Ed. Prentice Hall, ISBN 0-13-147573-8, 2004
6. A.B.Johnston, D.M.Piscitello, „Understanding Voice over IP Security”, Ed. Artech House, ISBN-13 978-1630812010, 2006
7. A. DeKok, „Network Access Identifier”, IETF, RFC 7542, 2015
8. C.Kaufman, P.Hoffman, et al., „Internet Key Exchange Protocol Version 2 (IKEv2)”, IETF, RFC 7296
9. E.Rescorla, „The Transport Layer Security (TLS) Protocol. Version 1.3”, IETF RFC 8446, 2018
10. D.Simon, B.Aboba et al., „The EAP-TLS Authentication Protocol”, IETF, RFC 5216
11. J.Edney, W.Arbaugh, „Real 802.11 Security: WiFi Protected Access and 802.11i”, Ed. Addison-Wesley Professional, ISBN-13 978-0321136206, 2003
12. 3GPP, “5G:Security architecture and procedures for 5G System”, ETSI TS 33.501 version 15.2.0 Release 15, October 2018

LABORATOR

Nr. crt.	Conţinutul	Nr. ore
1	Netfilter: firewall linux pentru securizarea reţelelor TCP/IP. Servicii N(P)AT şi „port forwarding”, „port knocking”	4
2	Snort: detecţia intruziunilor de reţea	4
3	Servicii de securitate IPSec	4
4	Managementul cheilor publice. Infrastructura PKI: generarea şi validarea certificatelor PK	6
5	Managementul cheilor publice. Infrastructura PKI: utilizarea certificatelor PK (scheme practice de criptare şi scheme de semnare digitala bazate pe PK)	4
6	Managementul cheilor publice. Infrastructura PKI: revocarea certificatelor PK	4
7	Colocviu final	2
	Total:	28

Bibliografie:

1. R.Lupu, „Securitatea Informației și a Rețelelor de Comunicații”, Note de curs, Moodle@UNSTPB, iunie 2025, https://curs.upb.ro/2024/course/index.php?categoryid=1740
2. Microsoft, “Microsoft Security Development Lifecycle(SDL)”, pagina web https://www.microsoft.com/en-us/securityengineering/sdl/threatmodeling
3. Mitre, „CVE”, pagina web https://cve.mitre.org/index.html
4. First, „Common Vunerability Scoring System SIG”, pagina web https://www.first.org/cvss
5. B.Schneier, „Academic: Attack Trees- Schneier on Security”, pagina web https://www.schneier.com/academic/archives/1999/12/attack_trees.html
6. NIST, „NIST Risk Management Framework (RMF)”, pagina web https://csrc.nist.gov/projects/risk-management/about-rmf
7. R.Lupu, VNET: Emulatorul de retea IPv4, https://github.com/rlupu/vnet

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 diferenţială a tehnicilor şi metodelor teoretice	Un examen scris de verificare, planficat în perioada de sesiune de examene. Subiectele acoperă întreaga materie, de la problemele generale ale domeniului managementului securității informației (amenințări, atacuri, obiective, cerințe și principii) până la arhitecturi, mecanisme și servicii de securitate pentru servicii și infrastructuri Internet.	50%

11.5 Seminar/laborator/proiect	- capabilităţile studenţilor de configurare, operare şi implementare a mecanismelor şi sistemelor de securitate oferite de sistemul Linux	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. Însuşirea cunoştinţelor fundamentale în domeniul securităţii informaţiei este demonstrată pe baza rezolvării unui set de teme; unele soluţii pot presupune realizarea unui program în limbajul C/Python.	30%
	- abilităţile de manipulare a elementelor fundamentale ale domeniului securităţii informaţiei; - aptitudinile de tratare a riscurilor de securitate pe baza unor studii de caz	Idem	20%
11.6 Condiţii de promovare			
• Obţinerea a 50% din punctajul total. • Participarea la activitatea de laborator este obligatorie. • Susţinerea examenului final nu este condiţionată de punctajul obţinut la laborator, dar examinarea poate acoperi concepte studiate în cadrul activităţii de a laborator			

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 dezvoltă abilităţi de a oferi soluţii unor probleme şi de a propune idei de îmbunătăţire a situaţiei existenţei în domeniul Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale, ramura industrială Retele si software de telecomunicatii.

În dezvoltarea conţinutului disciplinei s-au avut în vedere cunoştinţe descrise de literatura de specialitate si cercetările proprii publicate şi prezentate. Cursul are un conţinut similar cursurilor desfăşurate de universitatea POLITEHNICA din Bucuresti.

Se are în vedere dezvoltarea abilităţilor absolventului de a gestiona situaţii practice cu care se poate confrunta în viaţa reală în scopul creşterii contribuţiei acestuia la îmbunătăţirea mediului socio-economic.

Data completării Titular de curs Titular(i) de aplicaţii

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

21.09.2026	S.l./Lect. Dr. Radu Lupu	S.l./Lect. Dr. Radu Lupu

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