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 Information and Computer Networks Security			
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	II	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		DA	2.9 Codul disciplinei	UPB.04.M2.O.09-08		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	2.00	3.3 seminar/laborator	2
3.4 Total ore din planul de învăţământ	56.00	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 și/sau promovarea următoarelor discipline: • Programarea Calculatoarelor, • Structuri de Date și Algoritmi, • Arhitecturi și Protocoale pentru Comunicații, • Rețele și Servicii, • Arhitecturi pentru Rețele și Servicii, • Securitatea Rețelelor și Servicilor
4.2 de rezultate ale învățării	Acumularea următoarelor cunoștințe: • aprofundarea principalelor aplicații ale sistemelor criptografice; • abilități de management al riscurilor de securitate în rețele Internet (identificarea amenințărilor a atacurilor și a vulnerabilităților de securitate); • capabilități de proiectare a arhitecturilor de securitate pentru servicii și rețele de acces ptr. comunicații de date; • capacitatea de a implementa și analiza principalele mecanisme și servicii de securitate

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

5.1 Curs	Cursul se va desfășura într-o sală dotată cu: • videoproiector și computer, • access online, inclusiv la serviciul MS Teams și Moodle, • tablă de scris tradițională sau virtuală (en. whiteboard)
5.2 Seminar/ Laborator/Proiect	Laboratorul se va desfășura 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 rețea, servicii de rețea, tehnologii de securitate cu sursa-deschisă, unelte software cu sursa-deschisă ptr. generare și analiza de trafic de rețea

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.)*

Această disciplină își propune să ofere o pregatire studenților la nivel începător și mediu care va include cunoașterea principalelor noțiuni generale, principii, modele, arhitecturi și mecanisme de securitate, dar și formarea unor abilități pentru a rezolva probleme practice de securitate.

Disciplina abordează ca tematică specifică implementarea unui proces simplu pentru managementul securității aplicațiilor software pentru comunicații. Dezvoltarea capacităților de identificare a problemelor de securitate tipice software-ului pentru comunicatii (presupune identificarea principalelor tipuri de atac și a consecințelor aferente) și de selectare a celor mai eficiente soluții de securizare preventive/reactive. Analiza și evaluarea riscurilor de securitate și intimizare pentru cele mai reprezentative servicii și contexte de rețea Internet.

Abilitatea de a identifica și opera cu cerințele de configurare și de funcționare ale mecanismelor de securitate pornind de la un set de cerințe de securitate specifice celor mai comune aplicații software pentru comunicatii și ale utilizatorilor. Cunoașterea celor mai comune configurații de sisteme de securitate de rețea și a protocoalelor generice pentru securizarea comunicațiilor și pentru controlul accesului.

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	Demonstrează că deține cunoștințe de bază și deține aptitudini de aplicare a cunoștințelor în domeniul securității informației în domeniul serviciilor pentru comunicații peste Internet. Capacitatea de a identifica principalele amenințări de securitate și evaluarea riscurilor de securitate asociate celor mai comune sisteme de comuncații Internet. Aplică în practică cunoștințele acumulate pentru operarea corectă a măsurilor de securitate IT evitând cele mai comune vulnerabilități specifice fazelor de management al sistemelor și serviciilor pentru comunicații Internet. Definirea și implementarea unor infrastructuri PKI simple pentru managementul cheilor publice. Aplică metode și instrumente consacrate și/sau standardizate pentru implementarea unui proces simplu pentru managementul riscurilor de securitate ale unui scenariu dat. Capacitatea de a specifica principalele cerințe de securitate ale serviciilor pentru comunicații și de analiză pentru a determina cele mai eficiente măsuri de securitate care pot garanta nivelul de securitate cerut de un anumit sistem pentru comunicații. Abilitatea de analiză și clasificare a sistemelor de securitate Internet. Proiectarea unor arhitecturi și configurații simple de securitate pentru prevenirea/detecția vulnerabilităților de securitate. Argumentează și analizează coerent și corect contextul de aplicare a cunoștințelor de bază ale domeniului, în evaluarea modului de de funcționare a protocoalelor și mecanismelor de securitate. Comunicare orala și în scris în limba romană și engleză: utilizează vocabularul științific specific domeniului (jargonul), în vederea comunicării eficace și fără echivoc, în scris și oral. Abilități de utilizare a mediului de comunicare Internet (ex. Google, servicii de arhivare de documente) și capacitatea de analiză și selectare a surselor bibliografice relevante online.
Transversale (generale)	Lucrează în echipă și comunică eficient, coordonându-și eforturile cu ceilalți pentru rezolvarea de situații problemă de complexitate medie. Autonomie și gândire critică: abilitatea de a gândi în termeni științifici, de a căuta și analiza date în mod independent, precum și de a desprinde și prezenta concluzii / identifica soluții. Capacitate de analiză și sinteză: prezintă în mod sintetic cunoștințele dobândite, ca urmare a unui proces de analiză sistematică. Respectă principiile de etică academică: în activitatea de documentare citează corect sursele bibliografice utilizate. Pune în practică elemente de inteligență emoțională în gestionarea socio-emoțională adecvată a unor situații din viața reală/academică/profesională, demonstrând stăpânire de sine și obiectivitate în luarea deciziilor sau în situații de stres.

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	*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.* • 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. • Definește noțiuni specifice domeniului (amenințare, vulnerabilitati, atac, risc de securitate, nivel de securitate, obiective de securitate, cerințe de securitate). • Descrie/clasifică simple arhitecturi de securitate, sisteme de securitate, procesele specifice managementului cheilor publice (PKI) și structuri arbore pentru analiza atacurilor de rețea. • Evidențiază relații între noțiunile specifice domeniului (enumerate mai sus)
Aptitudini	*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).* • Selectează și grupează informații relevante pe baza unui scenariu predefinit în vederea analizei riscurilor de securitate pentru specificarea cerințelor de securitate și a măsurilor de securitate. • Utilizează argumentat principii specifice în vederea proiectării arhitecturilor de securitate și în implementarea măsurilor de securitate pe baza unui set de cerințe de securitate. • Lucrează productiv în echipă. • Rezolvă probleme practice propuse în cadrul lucrărilor de laborator/seminar. • Interpretează adecvat relații de cauzalitate (bunuri de valoare pentru organizație - amenințări-resurse IT – vulnerabilități - atacuri - riscuri de securitate - cerințe de securitate). • Analizează și compară diverse clase de vulnerabilități, atacuri, mecanisme și servicii de securitate. • Identifică soluții arhitecturale și servicii de securitate necesare pentru tratarea riscurilor de securitate. • Formulează concluzii la problemele soluționate. • Argumentează soluțiile identificate/modurile de rezolvare.

Responsabilitate și autonomie	*Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.* • Selectează surse bibliografice potrivite (inclusiv in limba engleza) și le analizează. • Respectă principiile de etică academică, citând corect sursele bibliografice utilizate. • Manifestă colaborare cu ceilalți colegi și cadre didactice pentru depășirea unor probleme în desfășurarea activităților didactice • Demonstrează autonomie în organizarea situației/contextului de învățare sau a situației 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 studenților la stabilirea propriului parcurs de învățare, cum se identifică eventualele rămâneri în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)*

Procesul de predare se va desfășura folosind metode expozitive (prelegerea, expunerea), cât și conversative-interactive, bazate pe învățare prin descoperire directă și indirectă a realității (experimentul, demonstrația, modelarea), dar și prin problematizare și acțiune (exercițiul, activitățile practice și rezolvarea de probleme).

În activitatea de predare vor fi utilizate prelegeri, în baza unor prezentări Power Point sau diferite filmulețe care vor fi puse la dispoziția studenților. Fiecare curs va debuta cu recapitularea principalelor noțiuni deja studiate. Predarea se bazează pe folosirea videoproiectorului acoperind funcția de comunicare și demonstrativă. Materialele de curs sunt sub formă de note și prezentări de curs care sunt disponibile în format electronic.

Prezentările utilizează imagini și scheme, astfel încât informațiile prezentate să fie ușor de înțeles și asimilat.

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

10. Conținuturi

CURS		
Capitolul	**Conținutul**	**Nr. ore**
1	Noțiuni de management al securității informației (INFOSEC). Amenințări, vulnerabilități și atacuri în Internet. Agenți de atac. Tratarea riscurilor de securitate	6
2	Sisteme și tehnici de securitate pentru rețeaua Internet. Sistemul firewall (caracteristici, elemente funcționale, configurații, probleme și soluții). Sistemul pentru detecția și prevenirea intruziunilor-IDPS (arhitectura generică, caracteristici, performanțe, mecanisme pentru detecție). Tehnici, mecanisme și sisteme anti-(D)DoS. Tehnici și sisteme anti-SPAM (mecanisme necriptografice și criptografice, metoda Bayesiana).	8
3	Servicii generice de securitate pentru rețelele TCP/IP. Tehnologiile IPSec și TLS. Servicii și mecanisme criptografice aferente	4
4	Modele de arhitecturi și principii de securitate pentru rețeaua Internet. Modelul punct-la-punct. Modelul pentru controlul accesului. Tehnici pentru specificarea politicilor de autorizare. Arhitectura IEEE 802.1x și AAA	4
5	Securitatea rețelelor de acces radio WLAN, GSM și 5G. Mecanisme de autentificare a entităților, asigurarea confidențialității și integrității datelor și garantarea caracterului privat. Sistemele criptografice WEP, TKIP/WPA, CCMP/WPA2, WPA3	6

	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. 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.	**Conținutul**	**Nr. ore**
1	Netfilter: firewall linux pentru securizarea rețelelor TCP/IP. Servicii N(P)AT și „port forwarding”, „port knocking”	4
2	Snort: detecția intruziunilor de rețea	4
3	Servicii de securitate IPSec	4
4	Managementul cheilor publice. Infrastructura PKI: generarea și validarea certificatelor PK	4
5	Managementul cheilor publice. Infrastructura PKI: utilizarea certificatelor PK (scheme practice de criptare și scheme de semnare digitala bazate pe PK)	4
6	Managementul cheilor publice. Infrastructura PKI: revocarea certificatelor PK	4
7	Metode pentru detecția atacurilor (Bayes, Markov, CUSUM, Entropie)	2
8	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-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.	60%

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.	25%
	- abilităţile de manipulare a elementelor fundamentale ale domeniului securităţii informaţiei; - aptitudinile de tratare a riscurilor de securitate pe baza unor studii de caz	Idem	15%
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 Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației

09.09.2022 S.l./Lect. Dr. Radu Lupu S.l./Lect. Dr. Radu Lupu

Data avizării în departament Director de departament

27.10.2024 Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul Facultății Decan

25.10.2024 Prof. Dr. Mihnea Udrea