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	Comunicaţii Mobile

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Securitatea sistemelor radio			
2.2 Titularul activităţilor de curs				Prof. Dr. Simona HALUNGA			
2.3 Titularul activităţilor de seminar / laborator				Prof. Dr. Simona HALUNGA			
2.4 Anul de studiu	2	2.5 Semestrul	1	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		DA	2.9 Codul disciplinei	UPB.04.M2.O.08-13		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	1.5	3.3 seminar/laborator	1.5
3.4 Total ore din planul de învăţământ	42	Din care: 3.5 curs	21	3.6 seminar/laborator	21
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					61
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	Parcurgerea următoarelor discipline: – Programarea calculatoarelor și limbaje de programare (1 și 2)
4.2 de rezultate ale învăţării	Acumularea următoarelor cunoştinţe generale: – concepte fundamentale de programarea calculatoarelor şi sisteme de operare.

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.
5.2 Seminar/ Laborator/Proiect	– Laboratorul se va desfăşura într-o sală cu dotare specifică, care trebuie să includă: videoproiector, computer, software specific (maşini virtuale, Kali Linux, Matlab) şi acces la Internet. – Prezenţa obligatorie la laboratoare (conform regulamentului studiilor universitare de masterat în UNSTPB).

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.)*

Scopul principal al acestei discipline este de a asigura studenţilor o înţelegere cuprinzătoare a principiilor şi provocărilor asociate cu securitatea calculatoarelor personale şi a dispozitivelor mobile. Includerea acestei discipline în curriculum este justificată de relevanţa tot mai mare a securităţii cibernetice în era digitală, unde înţelegerea complexităţii securităţii dispozitivelor personale şi mobile este esenţială pentru protecţia datelor individuale şi ale diverselor organizaţii.
Cursul îşi propune să ofere studenţilor o perspectivă largă asupra subiectelor cheie legate de securitatea computerelor şi a dispozitivelor mobile, incluzând concepte generale de securitate, vulnerabilităţi, detecţia şi prevenirea atacurilor cibernetice, conturi de utilizatori şi parole, precum şi soluţii de securitate pentru întreţinerea calculatoarelor personale. La finalul cursului, studenţii vor avea o bază solidă în gestionarea securităţii calculatoarelor personale, atât staţionare cât şi portabile, vor înţelege procesul de management al securităţii şi vor fi capabili să dezvolte o politică de securitate.
Cursul abordează, de asemenea teme precum vectorii atacurilor cibernetice, incluzând viruşi, viermi şi alţi agenţi rău intenţionaţi, împreună cu metodele pentru detectarea, eliminarea şi căile de penetrare ale acestor atacuri, cum ar fi serviciile de e-mail, serviciile web, reţelele de calculatoare wired si wireless şi interfeţele calculatorului personal. În plus, cursul discută şi analizează resurse avansate de securitate, metode de stocare a datelor în calculatoarele personale utilizând diverse sisteme de operare, proceduri şi utilităţi pentru identificarea şi recuperarea informaţiilor şterse sau distruse, şi tehnici pentru extragerea şi interpretarea datelor în scopuri de expertiză criminalistică.
– Laboratorul se axează pe securitatea reţelelor în care se află calculatorul personal sau dispozitivul mobil, oferind o introducere în metodele de exploatare a reţelelor, analiza traficului şi securitatea endpoint-urilor (dispozitive fizice care se conectează şi fac schimb de informaţii cu o reţea de calculatoare).

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 deține cunoștințe de bază privind conceptele teoretice și metodele de securitate a calculatorului personal și a terminalelor mobile. • Aplică în practică cunoștințele teoretice dobândite și utilizează mașini virtuale pentru a simula diverse tipuri de vulnerabilități și contramăsuri. • Aplică metode și instrumente standardizate, specifice domeniului securității cibernetice, pentru realizarea procesului de evaluare si planificare a procesului de management al securității calculatoarelor personale fixe sau portabile, în funcție de problemele de rezolvat și identifică soluții. • Argumentează și analizează coerent și corect contextul de aplicare a cunoștințelor de bază ale domeniului securității cibernetice, utilizând concepte cheie ale disciplinei și metodologia specifică. • Comunicare orală și în scris în limba română: utilizează vocabularul științific specific domeniului studiat, în vederea comunicării eficiente și corecte, în scris și oral. • Comunicare orală și în scris într-o limba străină (engleză): demonstrează înțelegerea și aplicarea corectă a vocabularului aferent domeniului studiat, într-o limbă străină.
Transversale (generale)	• Comunică eficient, în special în timpul orelor de aplicații, 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, de a identifica soluții, precum și de a desprinde și prezenta concluzii. • 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 citeazăncorect sursele bibliografice utilizate. • Pune în practică elemente de inteligență emoțională în gestionarea socio-emoțională adecvată a unor situații din viața academică, demonstrând stăpânire de sine și obiectivitate în luarea deciziilor sau în situații 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 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.)*

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.* • Defineşte corect noţiunile de bază ale domeniului securităţii calculatorului. • Descrie în mod corespunzător conceptele fundamentale legate de vulnerabilităţile ce pot apărea în funcţionarea calculatorului personal sau a dispozitivelor mobile. • Evidenţiază modalităţile de testare şi evaluare a securităţii pentru un calculator personal. • Înţelege diferenţele între diferitele tipuri de vulnerabilităţi cibernetice. • Defineşte şi utilizează elementele de bază legate analiza şi prelucrarea datelor stocate de • calculatorul personal pentru identificarea vulnerabilităţilor. • Este capabil să utilizeze corect principalele modalităţi de analiză a securităţii calculatorului personal şi a terminalelor mobile. • Înţelege conceptele de bază legate de analiza securităţii calculatorului personal.
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 într-un context dat, putând astfel să descrie corespunzător diverse aspecte teoretice sau practice ale domeniului securităţii cibernetice. • Utilizează argumentat conceptele specifice domeniului securităţii cibernetice, în vederea abordării corecte a unor probleme. • Verifică experimental soluţiile identificate pentru rezolvarea practică a găsirii de vulnerabilităţi cibernetice şi propunerea de contramăsuri eficiente. • Formulează concluzii corecte asupra rezultatelor experimentele realizate. • Argumentează modul de rezolvare şi soluţiile utilizate pentru rezolvarea unor probleme.
Responsabilitate şi autonomie	*Capacitatea cursantului de a aplica în mod autonom şi responsabil cunoştinţele şi aptitudinile sale.* • Selectează şi grupează informaţii relevante într-un context dat, putând astfel să descrie corespunzător diverse aspecte teoretice sau practice ale domeniului securităţii cibernetice. • Utilizează argumentat conceptele specifice domeniului securităţii cibernetice, în vederea abordării corecte a unor probleme. • Verifică experimental soluţiile identificate pentru rezolvarea practică a găsirii de vulnerabilităţi cibernetice şi propunerea de contramăsuri eficiente. • Formulează concluzii corecte asupra rezultatelor experimentele realizate. • Argumentează modul de rezolvare şi soluţiile utilizate pentru rezolvarea unor probleme.

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.)*

Cursurile sunt predate într-o manieră interactivă, fiind încurajată participarea activă a studenţilor. Sunt folosite atât metode clasice de predare (prelegerea şi expunerea), utilizând prezentări PowerPoint prin intermediul mijloacelor multimedia, cât şi interactive, bazate pe întrebări – răspunsuri şi feedback-ul studenţilor, adaptând permanent demersul pedagogic la posibilităţile de asimilare şi învăţare a studenţilor (prin repetarea suplimentară a anumitor noţiuni şi concepte, dacă acest lucru se dovedeşte necesar).

Fiecare curs debutează cu recapitularea succintă a capitolelor anterioare, cu accent asupra noţiunilor parcurse la ultimul curs. Prezentările utilizează numeroase imagini şi scheme, astfel încât informaţiile prezentate să fie cât mai uşor de înţeles şi asimilat. Materialele complete de curs sunt disponibile în format electronic pe platforma Moodle a facultăţii.
Predarea cunoştinţelor în cadrul orelor de laborator se bazează pe comunicarea orală şi explicarea detaliată a metodelor utilizate şi a rezultatelor obţinute, într-o manieră permanent interactivă. Studenţii implementează şi evaluează independent aceleaşi probleme prin utilizarea calculatorului, a mediului software şi a echipamentelor hardware (atunci când este cazul). Aplicaţiile realizate îi ajută pe studenţi în dezvoltarea unor relaţii optime de comunicare într-un climat favorabil învăţării prin descoperire. Materialele de laborator sunt disponibile studenţilor sub formă electronică pe platforma Moodle a facultăţii.
Predarea cunoştinţelor în cadrul orelor de proiect se realizează prin discuţii detaliate, oferirea de specificaţii cu privire la scopul final al proiectului şi a contextului necesar (programe specifice), precum şi indicaţii pentru a descoperi soluţii la problemele cerute. Materialele de proiect sunt disponibile studenţilor sub formă electronică pe platforma Moodle a facultăţii.

10. Conţinuturi

CURS		
Capitolul	**Conţinutul**	**Nr. ore**
1	Introducere. Scurta trecere în revistă a aspectelor legate de rețele de calculatoare. Arhitectura de securitate OSI. Mecanisme de Implementare	3
2	Algoritmi de criptare cu cheie publică. Tehnici de criptare bloc. Tehnici de criptare iterativă. Utilizarea algoritmilor de criptare	3
3	Algoritmi de criptare cu cheie privată. RSA. El Gamal. Gestiunea cheilor publice	3
4	Autentificarea mesajelor. Algoritmii Hash si Mac. Protocoale de autentificare şi semnătura digitală	3
5	Securitatea rețelelor. Kerberos. Securitatea în rețelele e-mail, IP, şi web	3
6	Securitatea retelelor mobile 2/3/4/5 G.	3
7	Securitatea retelelot WiFi	3
	Total:	21

Bibliografie:
Bibliografie:
1. O. Fratu, Securitatea calculatorului personal şi a terminalelor mobile, suport de curs electronic pe platforma Moodle a facultăţii de ETTI: https://curs.upb.ro/2023/course/view.php?id=13822
2. T. Bradley, H. Carvey, Essential Computer Security, Syngress Publishing Inc., Rockland, USA, 2006, ISBN 1- 59749-114-4.
3. K. Fung, Network Security Technologies, 2nd Edition, Auerbach Publications, Boca Raton, USA, 2005, ISBN 0-8493-3027-0.
4. A. Earle, Wireless Security Handbook, Auerbach Publications, Boca Raton, USA, 2006, ISBN 0-8493-3378-4.
5. W. Stallings, L. Brown, Computer Security. Principles and Practice, Prentice Hall, 2008.

LABORATOR		
Nr. crt.	**Conţinutul**	**Nr. ore**
1	Cifrul Cesar. Criptare. Decriptare. Tehnici de atac brute force	3
2	AES. Criptare. Decriptare	3

3	DES. Criptare. Decriptare. Folosirea in modalitatea CBC	3
4	RC4. Criptare. Decriptare	3
5	Semnatura digitala folosind algoritmii SHA	3
6	RSA. Criptare. Decriptare. Semnatura digitala - generare si verificare	3
7	Verificare finala laborator	3
	Total:	21

Bibliografie:

1. R. Crăciunescu, Securitatea calculatorului personal şi a terminalelor mobile – Platforme de laborator, disponibile în format electronic pe platforma Moodle a facultăţii de ETTI: https://curs.upb.ro/2023/course/view.php?id=13822
2. R. Crăciunescu, Securitatea calculatorului personal si a terminalelor mobile – Teme, documentaţie, materiale diverse pentru proiect, disponibil în format electronic pe platforma Moodle a facultăţii de ETTI: https://curs.upb.ro/2023/course/view.php?id=13822
3. T. Bradley, H. Carvey, Essential Computer Security, Syngress Publishing Inc., Rockland, USA, 2006, ISBN 1- 59749-114-4.
4. W. Stallings, L. Brown, Computer Security. Principles and Practice, Prentice Hall, 2008

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 legate de securitatea calculatorului personal. Cunoaşterea modului de aplicare a teoriei la rezolvarea unor probleme specifice domeniului.	Examen scris si oral în sesiunea de examene.	50
11.5 Seminar/laborator/proiect	Înţelegerea tehnicilor fundamentale de analiză şi prelucrare a vulnerabilităţilor calculatorului personal sau a reţelei în care aceste se află. Cunoaşterea modului de simulare şi de implementare practică (pe calculator) a metodelor studiate, cu ajutorul unor programe specifice.	Fişă de laborator la fiecare lucrare de laborator. Evaluare finala	50
11.6 Condiţii de promovare			
- Obţinerea a 50% din punctajul de la laborator. - Obţinerea a 50% din punctajul total. – Realizarea obligaţiilor caracteristice activităţii de laborator/proiect (participarea la lucrările planificate).			

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)

Universitatea Naţională de Ştiinţă şi Tehnologie Politehnica Bucureşti

Facultatea de Electronică, Telecomunicaţii şi

Tehnologia Informaţiei

În contextul digitalizării accelerate şi al atacurilor cibernetice tot mai sofisticate, există o cerere crescută pe piaţa muncii pentru competenţe avansate în securitatea informaţiilor. Angajatorii şi asociaţiile profesionale subliniază necesitatea ca absolvenţii să aibă o înţelegere solidă a securităţii reţelelor, managementului vulnerabilităţilor, criptografiei şi legislaţiei în domeniu. Prin acoperirea unui spectru larg de subiecte, de la principiile de bază la gestionarea avansată a securităţii, disciplina răspunde acestor nevoi. De asemenea, actualizarea conţinutului cursului cu cele mai recente cercetări şi tehnologii din domeniu este un aspect fundamental pentru pregătirea studenţilor în abordarea provocărilor dinamice ale securităţii informatice.

Alinierea cu standardele Spaţiului European al Învăţământului Superior (SEÎS) contribuie la asigurarea calităţii educaţiei şi recunoaşterea competenţelor pe plan internaţional, pregătind studenţii pentru piaţa globală a muncii şi provocările securităţii cibernetice.

Se asigură astfel absolvenţilor programului de masterat competenţe adecvate cu necesităţile calificărilor actuale şi o pregătire ştiinţifică şi tehnică modernă, de calitate şi competitivă, care să le permită angajarea rapidă după absolvire, disciplina fiind perfect încadrată în politica Universităţii Naţionale de Ştiinţă şi Tehnologie POLITEHNICA Bucureşti, atât din punctul de vedere al conţinutului şi structurii, cât şi din punctul de vedere al aptitudinilor şi deschiderii internaţionale oferite studenţilor. Posibilii angajatori vizează atât mediul academic (profil didactic şi de cercetare), cât şi mediul de cercetare-dezvoltare din instituţiile de stat şi private care utilizează reţele de calculatoare, calculatoare personale şi diverse terminale mobile şi sunt interesate în managementul securităţii acestora, sau oferă servicii avansate de securitate locale şi / sau la nivel de reţea.

Data completării	Titular de curs	Titular(i) de aplicaţii
21.09.2026	Prof. Dr. Simona HALUNGA	Prof. Dr. Simona HALUNGA

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