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	**Dispozitive, Circuite şi Arhitecturi Electronice**
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
1.5 Ciclul de studii	Masterat
1.6 Specializarea	Tehnologii Multimedia în Aplicaţii de Biometrie şi Securitatea Informaţiei

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Securitatea calculatorului personal şi a terminalelor mobile Personal Computer and Mobile Terminal Security			
2.2 Titularul activităţilor de curs				Prof. dr. ing. Octavian FRATU			
2.3 Titularul activităţilor de seminar / laborator				Prof. dr. ing. Răzvan-Eusebiu CRĂCIUNESCU			
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	2		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	Parcurgerea următoarelor discipline: – Programarea calculatoarelor şi limbaje de programare (1 şi 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) 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 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 deţine cunoştinţe de bază privind conceptele teoretice şi metodele de securitate a calculatorului personal şi a terminalelor mobile. – Aplică în practică cunoştinţele teoretice dobândite şi utilizează maşini virtuale pentru a simula diverse tipuri de vulnerabilităţi şi contramăsuri. – Aplică metode şi instrumente standardizate, specifice domeniului securităţii cibernetice, pentru realizarea procesului de evaluare si planificare a procesului de management al securităţii calculatoarelor personale fixe sau portabile, în funcţie de problemele de rezolvat şi identifică soluţii. – Argumentează şi analizează coerent şi corect contextul de aplicare a cunoştinţelor de bază ale domeniului securităţii cibernetice, utilizând concepte cheie ale disciplinei şi metodologia specifică. – Comunicare orală şi în scris în limba română: utilizează vocabularul ştiinţific specific domeniului studiat, în vederea comunicării eficiente şi corecte, în scris şi oral. – Comunicare orală şi în scris într-o limba străină (engleză): demonstrează înţelegerea şi aplicarea corectă a vocabularului aferent domeniului studiat, într-o limbă străină.
Transversale (generale)	– Comunică eficient, în special în timpul orelor de aplicaţii, 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, de a identifica soluţii, precum şi de a desprinde şi prezenta concluzii. – 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. – Pune în practică elemente de inteligenţă emoţională în gestionarea socio-emoţională adecvată a unor situaţii din viaţa academică, 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.* – 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 surse bibliografice potrivite şi le analizează. – 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 contextului de învăţare şi a problemelor de rezolvat. – Conştientizează valoarea contribuţiei sale în domeniul ingineriei la identificarea de soluţii viabile care să rezolve probleme din viaţa socială şi economică. – Analizează oportunităţi de afaceri sau de dezvoltare antreprenorială, pornind de la cunoştinţele dobândite în domeniul securităţii cibernetice. – Demonstrează abilităţi de management ale situaţiilor din viaţa reală (de exemplu gestionarea corectă a timpului de învăţare).

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.

10. Conţinuturi

CURS		
Capitolul	**Conţinutul**	**Nr. ore**

1	Principii şi probleme de securitate ale calculatoarelor personale, portabile şi a terminalelor mobile 1.1. Concepte generale privind securitatea calculatoarelor personale, portabile şi a terminalelor mobile 1.2. Vulnerabilităţi. Modalităţi de detecţie şi de prevenire a atacurilor informatice 1.3. Conturi de utilizator şi parole 1.4. Soluţii de securitate pentru întreţinerea calculatorului personal, portabil şi a terminalului mobil	4
2	Managementul securităţii calculatoarelor personale fixe sau portabile şi a terminalelor mobile 2.1. Procesul de management al securităţii 2.2. Politica de securitate	2
3	Vectori ai atacurilor informatice 3.1. Viruşi, viermi şi alţi agenţi distructivi 3.2. Proceduri de detecţie şi eliminare a vectorilor atacurilor informatice 3.3. Căi de penetrare a vectorilor atacurilor informatice: serviciul de e-mail, serviciul web, reţeaua de calculatoare, interfeţele calculatorului personal, a celui portabil şi a terminalului mobil 3.4. Spyware şi Adware 3.5. Securitatea perimetrului de lucru al calculatorului personal. Filtre. Firewall	6
4	Întreţinerea calculatorului personal, a celui portabil şi a terminalului mobil 4.1. Proceduri standard de întreţinere a calculatorului personal, a celui portabil şi a terminalului mobil 4.2. Proceduri specifice sistemelor Windows 4.3. Proceduri specifice sistemelor Linux 4.4. Proceduri specifice sistemelor Android sau iOS	6
5	Resurse avansate de securitate 5.1. Modalităţi de stocare a datelor in calculatoarele personale, portabile şi terminalele mobile folosind diferite sisteme de operare 5.2. Proceduri şi utilitare pentru identificarea şi refacerea informaţiilor şterse sau distruse 5.3. Extragerea şi interpretarea datelor informatice pentru expertize criminalistice	6
6	Tendinţe privind evoluţia atacurilor cibernetice şi a măsurilor de securitate cibernetică 6.1 Analiza comportamentală a calculatorului personal, portabil şi a terminalului mobil, precum şi a fluxurilor de date destinate sau generate de acestea 6.2. Utilizarea inteligenţei artificiale pentru detectarea anomaliilor comportamentale asociate calculatorului personal, portabil şi terminalului mobil	4
	Total:	28

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/
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	Protecţia muncii. Introducere în exploatarea reţelelor – Se descrie modul în care computerele interacţionează şi comunică între ele. Se introduc conceptele de bază ale reţelelor de calculatoare, urmate de metodologia şi instrumentele necesare pentru a ataca diverse servicii de reţea.	4
2	Securitatea reţelelor şi analiza traficului – Se discută conceptele de bază ale securităţii reţelelor şi ale analizei traficului pentru a identifica şi a investiga anomaliile de reţea.	4
3	Securitatea endpoint-urilor – Se analizează metode de monitorizare a activităţii calculatorului personal.	2
4	Gestionarea informaţiilor şi evenimentelor de securitate – Se analizează funcţionarea unui sistem de tip SIEM şi de asemenea crearea de interogări simple şi avansate pentru a căuta răspunsuri specifice din jurnalele acestui sistem.	4
	Total:	14

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/
2. T. Bradley, H. Carvey, *Essential Computer Security*, Syngress Publishing Inc., Rockland, USA, 2006, ISBN 1- 59749-114-4.
3. 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 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.	50%
11.6 Condiţii de promovare			
– 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 și al atacurilor cibernetice tot mai sofisticate, există o cerere crescută pe piața muncii pentru competențe avansate în securitatea informațiilor. Angajatorii și asociațiile profesionale subliniază necesitatea ca absolvenții să aibă o înțelegere solidă a securității rețelelor, managementului vulnerabilităților, criptografiei și legislației în domeniu. Prin acoperirea unui spectru larg de subiecte, de la principiile de bază la gestionarea avansată a securității, disciplina răspunde acestor nevoi. De asemenea, actualizarea conținutului cursului cu cele mai recente cercetări și tehnologii din domeniu este un aspect fundamental pentru pregătirea studenților în abordarea provocărilor dinamice ale securității informatice. Alinierea cu standardele Spațiului European al Învățământului Superior (SEÎS) contribuie la asigurarea calității educației și recunoașterea competențelor pe plan internațional, pregătind studenții pentru piața globală a muncii și provocările securității cibernetice.
Se asigură astfel absolvenților programului de masterat competențe adecvate cu necesitățile calificărilor actuale și o pregătire științifică și tehnică modernă, de calitate și competitivă, care să le permită angajarea rapidă după absolvire, disciplina fiind perfect încadrată în politica Universității Naționale de Știință și Tehnologie POLITEHNICA București, atât din punctul de vedere al conținutului și structurii, cât și din punctul de vedere al aptitudinilor și deschiderii internaționale oferite studenților. Posibilii angajatori vizează atât mediul academic (profil didactic și de cercetare), cât și mediul de cercetare-dezvoltare din instituțiile de stat și private care utilizează rețele de calculatoare, calculatoare personale și diverse terminale mobile și sunt interesate în managementul securității acestora, sau oferă servicii avansate de securitate locale și / sau la nivel de rețea.

Data completării	Titular de curs	Titular(i) de aplicații
21.09.2026	Prof. dr. ing. Octavian FRATU	Prof. dr. ing. Răzvan-Eusebiu CRĂCIUNESCU

Data avizării în departament	Director de departament
22.09.2026	Prof. Dr. Claudius Dan



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

