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, Telecomunicaţii şi Tehnologii Informaţionale
1.5 Ciclul de studii	Masterat
1.6 Specializarea	Telecomunicații

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)			Elemente de securitate cibernetica				
2.2 Titularul activităților de curs			Prof. Dr. Ing. Octavian Fratu				
2.3 Titularul activităților de seminar / laborator			Prof. Dr. Ing. Octavian Fratu				
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		DS	2.9 Codul disciplinei	UPB.04.M2.O.18-10		2.10 Tipul de notare	Nota

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

3.1 Număr de ore pe săptămână	2.5	Din care: 3.2 curs	1.50	3.3 seminar/laborator	1
3.4 Total ore din planul de învățământ	35.00	Din care: 3.5 curs	21	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					61
Tutorat					0
Examinări					4
Alte activități (dacă există):					0

3.7 Total ore studiu individual	65.00
3.8 Total ore pe semestru	100
3.9 Numărul de credite	4

4. Precondiții (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 învățării	Acumularea următoarelor cunoștințe generale: – concepte fundamentale de programarea calculatoarelor și sisteme de operare.

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

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.)*

Scopul principal al acestei discipline este de a asigura studenților o înțelegere cuprinzătoare a principiilor și provocărilor asociate cu securitatea calculatoarelor personale și a dispozitivelor mobile. Includerea acestei discipline în curriculum este justificată de relevanța tot mai mare a securității cibernetice în era digitală, unde înțelegerea complexității securității dispozitivelor personale și mobile este esențială pentru protecția datelor individuale și ale diverselor organizații.
Cursul își propune să ofere studenților o perspectivă largă asupra subiectelor cheie legate de securitatea computerelor și a dispozitivelor mobile, incluzând concepte generale de securitate, vulnerabilități, detecția și prevenirea atacurilor cibernetice, conturi de utilizatori și parole, precum și soluții de securitate pentru întreținerea calculatoarelor personale. La finalul cursului, studenții vor avea o bază solidă în gestionarea securității calculatoarelor personale, atât staționare cât și portabile, vor înțelege procesul de management al securității și vor fi capabili să dezvolte o politică de securitate.
Cursul abordează, de asemenea teme precum vectorii atacurilor cibernetice, incluzând viruși, viermi și alți agenți rău intenționați, împreună cu metodele pentru detectarea, eliminarea și căile de penetrare ale acestor atacuri, cum ar fi serviciile de e-mail, serviciile web, rețelele de calculatoare și interfețele calculatorului personal. În plus, cursul discută și analizează resurse avansate de securitate, metode de stocare a datelor în calculatoarele personale utilizând diverse sisteme de operare, proceduri și utilități pentru identificarea și recuperarea informațiilor șterse sau distruse, și tehnici pentru extragerea și interpretarea datelor în scopuri de expertiză criminalistică.
– Laboratorul se axează pe securitatea rețelelor în care se află calculatorul personal sau dispozitivul mobil, oferind o introducere în metodele de exploatare a rețelelor, analiza traficului și securitatea endpoint-urilor (dispozitive fizice care se conectează și fac schimb de informații cu o rețea de calculatoare).
– Proiectul oferă posibilitatea ca studenții să folosească diverse mașini virtuale pentru a descoperi vulnerabilitățile din cadrul unei rețele.

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 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 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.* • Definește corect noțiunile de bază ale domeniului securității calculatorului. • Descrie în mod corespunzător conceptele fundamentale legate de vulnerabilitățile ce pot apărea în funcționarea calculatorului personal sau a dispozitivelor mobile. • Evidențiază modalitățile de testare și evaluare a securității pentru un calculator personal. • Înțelege diferențele între diferitele tipuri de vulnerabilități cibernetice. • Definește și utilizează elementele de bază legate analiza și prelucrarea datelor stocate de • calculatorul personal pentru identificarea vulnerabilităților. • Este capabil să utilizeze corect principalele modalități de analiză a securității calculatorului personal și a terminalelor mobile. • Înțelege conceptele de bază legate de analiza securității calculatorului personal.
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 într-un context dat, putând astfel să descrie corespunzător diverse aspecte teoretice sau practice ale domeniului securității cibernetice. • Utilizează argumentat conceptele specifice domeniului securității cibernetice, în vederea abordării corecte a unor probleme. • Verifică experimental soluțiile identificate pentru rezolvarea practică a găsirii de vulnerabilități cibernetice și propunerea de contramăsuri eficiente. • Formulează concluzii corecte asupra rezultatelor experimentele realizate. • Argumentează modul de rezolvare și soluțiile utilizate pentru rezolvarea unor probleme.
Responsabilitate și autonomie	*Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.* • Selectează și grupează informații relevante într-un context dat, putând astfel să descrie corespunzător diverse aspecte teoretice sau practice ale domeniului securității cibernetice. • Utilizează argumentat conceptele specifice domeniului securității cibernetice, în vederea abordării corecte a unor probleme. • Verifică experimental soluțiile identificate pentru rezolvarea practică a găsirii de vulnerabilități cibernetice și propunerea de contramăsuri eficiente. • Formulează concluzii corecte asupra rezultatelor experimentele realizate. • Argumentează modul de rezolvare și soluțiile 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 studenților la stabilirea propriului parcurs de învățare, cum se identifică eventualele rămâneri în urmă și ce măsuri remediale se adoptă în astfel de cazuri.)*

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

Fiecare curs debutează cu recapitularea succintă a capitolelor anterioare, cu accent asupra noțiunilor parcurse la ultimul curs. Prezentările utilizează numeroase imagini și scheme, astfel încât informațiile prezentate să fie cât mai ușor de înțeles și asimilat. Materialele complete de curs sunt disponibile în format electronic pe platforma Moodle a facultății.
Predarea cunoștințelor în cadrul orelor de laborator se bazează pe comunicarea orală și explicarea detaliată a metodelor utilizate și a rezultatelor obținute, într-o manieră permanent interactivă. Studenții implementează și evaluează independent aceleași probleme prin utilizarea calculatorului, a mediului software și a echipamentelor hardware (atunci când este cazul). Aplicațiile realizate îi ajută pe studenți în dezvoltarea unor relații optime de comunicare într-un climat favorabil învățării prin descoperire. Materialele de laborator sunt disponibile studenților sub formă electronică pe platforma Moodle a facultății.
Predarea cunoștințelor în cadrul orelor de proiect se realizează prin discuții detaliate, oferirea de specificații cu privire la scopul final al proiectului și a contextului necesar (programe specifice), precum și indicații pentru a descoperi soluții la problemele cerute. Materialele de proiect sunt disponibile studenților sub formă electronică pe platforma Moodle a facultății.

10. Conținuturi

CURS		
Capitolul	**Conținutul**	**Nr. ore**
1	Principii și probleme de securitate ale calculatoarelor personale, portabile și a terminalelor mobile 1.1. Concepte generale privind securitatea calculatoarelor personale, portabile și a terminalelor mobile 1.2. Vulnerabilități. Modalități de detecție și de prevenire a atacurilor informatice 1.3. Conturi de utilizator și parole 1.4. Soluții de securitate pentru întreținerea calculatorului personal, portabil și a terminalului mobil	4
2	Managementul securității calculatoarelor personale fixe sau portabile și a terminalelor mobile 2.1. Procesul de management al securității 2.2. Politica de securitate	2
3	Vectori ai atacurilor informatice 3.1. Viruși, viermi și alți agenți distructivi 3.2. Proceduri de detecție și eliminare a vectorilor atacurilor informatice 3.3. Căi de penetrare a vectorilor atacurilor informatice: serviciul de e-mail, serviciul web, rețeaua de calculatoare, interfețele calculatorului personal, a celui portabil și a terminalului mobil 3.4. Spyware și Adware 3.5. Securitatea perimetrului de lucru al calculatorului personal. Filtre. Firewall	6
4	Întreținerea calculatorului personal, a celui portabil și a terminalului mobil 4.1. Proceduri standard de întreținere a calculatorului personal, a celui portabil și a terminalului mobil 4.2. Proceduri specifice sistemelor Windows 4.3. Proceduri specifice sistemelor Linux 4.4. Proceduri specific 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:

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	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 și a terminalelor mobile – Platforme de laborator, disponibile în format electronic pe platforma Moodle a facultății de ETTI: https://curs.upb.ro/2023/course/view.php?id=13822
2. R. Crăciunescu, Securitatea calculatorului personal si a terminalelor mobile – Teme, documentație, materiale diverse pentru proiect, disponibil în format electronic pe platforma Moodle a facultății 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	Cunoașterea noțiunilor teoretice fundamentale legate de securitatea calculatorului personal. Cunoașterea modului de aplicare a teoriei la rezolvarea unor probleme specifice domeniului.	Examen scris în sesiunea de examene.	50
11.5 Seminar/laborator/proiect	Înțelegerea tehnicilor fundamentale de analiză și prelucrare a vulnerabilităților calculatorului personal sau a rețelei în care aceste se află. Cunoașterea modului de simulare și de implementare practică (pe calculator) a metodelor studiate, cu ajutorul unor programe specifice.	Fișă de laborator la fiecare lucrare de laborator	50
11.6 Condiții de promovare			
Obținerea a 50% din punctajul total. – Realizarea obligațiilor caracteristice activității de laborator/proiect (participarea la lucrările planificate).			

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 (SEÎS)

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 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
01.10.2024	Prof. Dr. Ing. Octavian Fratu	Prof. Dr. Ing. Octavian Fratu

Data avizării în departament	Director de departament
27.10.2024	Conf. Dr. Serban Georgica Obreja

Data aprobării în Consiliul Facultăţii	Decan
01.11.2024	Prof. Dr. Mihnea Udrea