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 în reţelele de calculatoare Security in Computer Networks			
2.2 Titularul activităţilor de curs				Dr. ing. Dragoş DRĂGHICESCU			
2.3 Titularul activităţilor de seminar / laborator				Dr. ing. Dragoş DRĂGHICESCU			
2.4 Anul de studiu	2	2.5 Semestrul	I	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		DA	2.9 Codul disciplinei	UPB.04.M3.O.20-32		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					65
Tutorat					0
Examinări					4
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 următoarelor discipline: – Programarea calculatoarelor – Securitatea calculatorului personal şi a terminalelor mobile

4.2 de rezultate ale învățării	Acumularea următoarelor cunoștințe generale: – concepte fundamentale de programarea calculatoarelor și sisteme de operare; – concepte de bază privind securizarea și autentificarea informației digitale din calculatoarele personale.

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 și echipamente de rețea. – 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.)*

Disciplina are ca obiectiv principal dobândirea unor cunoștințe teoretice și practice în domeniul securității cibernetice, domeniul cu cea mai rapidă creștere din industria tehnologiei informației și calculatoarelor (TIC).
– În cadrul cursului, studenții vor dobândi cunoștințele esențiale, necesare proiectării și exploatării în siguranță a unor sisteme informatice, precum și pentru a proteja din punct de vedere procedural informațiile digitale din cadrul unor instituții sau companii. De asemenea, cursul va permite studenților să acumuleze expertiză în investigarea incidentelor legate de securitatea cibernetică în cadrul rețelele de calculatoare sau dispozitivelor IoT și în aplicarea standardelor, modelelor și celor mai bune practici pentru a rezolva sau pre-întâmpina problemele de securitate ale rețelelor de calculatoare. Cursul conține și noțiuni de bază legate de elaborarea politicilor de securitate, necesare prevenției riscurilor și amenințărilor asupra infrastructurilor digitale.
– Laboratorul acoperă următoarele subiecte: administrarea Linux și securitatea sistemului de operare; lucrul cu utilitare de rețea și automatizarea acestora prin intermediul script-urilor Bash; exersarea cunoștințelor generale de rețelistică (principii generale de securitate, studiul și utilizarea protocoalelor de tip IPsec etc.); principii de scriere a codului sigur (aplicate la limbajele Python și C); exploatarea vulnerabilităților aplicațiilor; principii ale integrității datelor, confidențialitate și autenticitate.

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 în domeniul securității cibernetice. – Aplică în practică cunoștințele teoretice dobândite în vederea proiectării și exploatării în siguranță a sistemelor informatice. – Aplică metode și instrumente standardizate, specifice domeniului securității cibernetice, pentru realizarea procesului de evaluare a unei situații de risc informatic, în funcție de problemele de rezolvat și identifică soluții. – Argumentează și analizează coerent și corect contextul de aplicare a instrumentelor hardware și software necesare, 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 citează corect 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 cibernetice: configurarea și managementul rețelelor, tipurile de atac asupra rețelelor de calculatoare, protecția sistemelor informatice, securitatea aplicațiilor Web și a cloud-ului etc. – Descrie în mod corespunzător conceptele fundamentale legate de evitarea incidentelor și apărarea sistemelor informatice. – Evidențiază și analizează vulnerabilitățile rețelelor de calculatoare. – Înțelege securitatea fizică și a mediului de lucru (conceptele de autentificare și identificare, drepturile de acces ale utilizatorilor). – Definește și utilizează elementele de bune practici în configurarea, protecția și administrarea sistemelor informatice. – Este capabil să realizeze corect mentenanța și actualizarea sistemelor IT. – Înțelege conceptele de bază legate de reziliența sistemelor informatice.

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 reţelelor de calculatoare, în vederea abordării corecte a problemelor ce trebuie rezolvate. – Verifică experimental soluţiile identificate pentru detectarea şi prevenirea incidentelor de securitate în reţelele de calculatoare. – Formulează concluzii corecte asupra rezultatelor experimentelor 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 figuri 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 de reţea (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	"Introducere" – Concepte generale. Principalii vectori de atac asupra infrastructurilor informatice: vectori de atac asupra rețelelor de calculatoare; vectori de atac asupra dispozitivelor mobile și IoT	2
2	"Guvernanța sistemelor informatice" – Analiza riscurilor de securitate a sistemelor informatice. Politica de securitate a sistemului informatic. Auditul de securitate al sistemului informatic. Cartografierea ecosistemului și gestionarea activelor digitale	2
3	"Protecția sistemelor informatice" – Securitatea fizică și a mediului de lucru: drepturile de acces ale utilizatorilor; autentificare și identificare. Concepte de bune practici în configurarea, protecția și administrarea sistemelor informatice: configurarea inițială a sistemelor și conceptul Zero-Trust; segregarea sistemelor; filtrarea traficului; mentenanța și actualizarea continuă a sistemelor IT; izolarea sistemelor critice de tip industrial / IoT	6
4	"Evitarea incidentelor și apărarea sistemelor informatice" – Detectarea și înregistrarea (jurnalizarea) evenimentelor de securitate. Sistemele de tip firewall și detecția intruziunilor. Corelarea și analiza jurnalelor. Răspunsul și acțiunile la raportarea unor incidente de securitate	6
5	"Reziliența sistemelor informatice" – Introducere în noțiunile de disponibilitate ridicată și reziliență a sistemelor informatice. Sisteme de disponibilitate-ridicată continuă. Sisteme de disponibilitate-ridicată active-pasive	4
6	"Managementul riscurilor sistemelor informatice" – Introducere. Standarde actuale	2
7	"Implementarea cerințelor minime de securitate" – Guvernanță: managementul securității informației; managementul ecosistemului. Protecție: managementul arhitecturii și administrării sistemelor; managementul identității și accesului utilizatorilor; managementul mentenanței. Managementul detecției și al incidentelor de securitate. Reziliență: managementul continuității afacerii; managementul crizelor și restaurarea sistemelor. Arhitecturi de securizare a rețelelor de sisteme informatice	6
	Total:	28

Bibliografie:

1. D. Drăghicescu, *Securitatea în rețelele de calculatoare*, suport de curs electronic pe platforma Moodle a facultății de ETTI: https://curs.upb.ro/
2. R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 3rd Edition, Wiley, 2020, ISBN: 978-1-119-64278-7.
3. R. Bejtlich, *The Practice of Network Security Monitoring: Understanding Incident Detection and Response*, No Starch Press, 2013, ISBN: 978-1593275099.
4. M. Chapple, D. Seidl, *CompTIA Security+ Study Guide: Exam SY0-601*, 8th Edition, Wiley (Series: Sybex Study Guide), 2021, ISBN: 978-1-119-73626-4.
5. M. Ciampa, *CompTIA Security+ Guide to Network Security Fundamentals*, 5th Edition, Cengage Learning, 2014, ISBN: 978-1305093911.
6. W. Stallings, *Network Security Essentials: Applications and Standards*, 4th Edition, Prentice Hall, Upper Saddle River, New Jersey, 2011, ISBN: 978-0-13-610805-4.
7. Al. Caranica, Al. Vulpe, M.-E. Pârvu, D. Drăghicescu, O. Fratu, "ToR-SIM, A Mobile Malware Analysis Platform", *Proc. of the 10th Int. Conf. on Speech Technology and Human-Computer Dialogue* (*SpeD*), Timișoara, pp. 1-6, Oct. 10-12, 2019, IEEE NY, ISBN: 978-1-7281-0984-8.

LABORATOR		
Nr. crt.	**Conținutul**	**Nr. ore**
1	Protecția muncii. Elemente de Linux pentru securitatea rețelelor: exerciții practice	4

2	Securitatea aplicațiilor Web și strategii de apărare cu Linux	4
3	Răspuns la incidente și monitorizarea rețelelor cu Linux	4
4	Securizarea cloud-ului: soluții și practici recomandate bazate pe Linux	4
5	Securizarea dispozitivelor conectate în Internetul lucrurilor (IoT)	4
6	Securitatea rețelelor VPN cu Linux	4
7	Colocviu final	4
	Total:	28

Bibliografie:

1. D. Drăghicescu, *Securitatea în rețelele de calculatoare – Platforme de laborator*, disponibile în format electronic pe platforma Moodle a facultății de ETTI: https://curs.upb.ro/
2. A. Hoffman, *Web Application Security: Exploitation and Countermeasures for Modern Web Applications*, O'Reilly Media, 2020.
3. R. Messier, M. Jang, *Security Strategies in Linux Platforms and Applications*, 3rd Edition, Jones & Bartlett Learning, 2022.
4. J. Doyle, J. Caroll, *Routing TCP/IP*, Vol. 1 (2nd Edition), Cisco Press, Indianapolis, USA, 2006, ISBN: 978-1587052026.

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 rețelelor de calculatoare. 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 asigurare a securității sistemelor informatice. Configurarea corectă a setărilor de rețea și implementarea practică a unor soluții de detectare și analiză a incidentelor de securitate într-o rețea de calculatoare.	Colocviu final de laborator (test pe calculator).	50%
11.6 Condiții de promovare			
– Obținerea a 50% din punctajul total. – Realizarea obligațiilor caracteristice activității de laborator (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)

Programa disciplinei oferă studenților suportul teoretic și practic necesar cunoașterii aspectelor fundamentale ale domeniului securității cibernetice, domeniul cu cea mai rapidă creștere din industria actuală a tehnologiei informației și calculatoarelor. Securitatea cibernetică implică protocoale, tehnologii, sisteme, instrumente și tehnici pentru a securiza și opri atacurile rău intenționate, atacuri ce pot duce la pierderea sau furtul de informație, uneori critică, din cadrul unor instituții sau companii.

Disciplina permite dobândirea cunoştinţelor esenţiale, necesare proiectării şi exploatării în siguranţă a sistemelor informatice, acumulării de expertiză în investigarea incidentelor legate de securitatea cibernetică în cadrul reţelelor de calculatoare sau dispozitivelor IoT, precum şi în elaborarea politicilor de securitate. Prin urmare, ea răspunde concret cerinţelor actuale de dezvoltare şi evoluţie a economiei europene a serviciilor din domeniul TIC, dar şi practicilor curente din cadrul celor mai avansate instituţii de învăţământ superior din Europa.
Se asigură astfel absolvenţilor 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 şi sunt interesate în managementul securităţii acestora, sau oferă servicii avansate de securitate locale şi la nivel de reţea.

Data completării	Titular de curs	Titular(i) de aplicaţii
	Dr. ing. Dragoş DRĂGHICESCU	Dr. ing. Dragoş DRĂGHICESCU

Data avizării în departament	Director de departament
31.10.2024	Prof. Dr. Claudius DAN

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