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 Wireless Avansate

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Managementul incidentelor de securitate şi audit The Management and Audit of Security Incidents			
2.2 Titularul activităţilor de curs				Conf. Dr. Constantin Viorel Marian			
2.3 Titularul activităţilor de seminar / laborator				Conf. Dr. Constantin Viorel Marian			
2.4 Anul de studiu	1	2.5 Semestrul	1	2.6. Tipul de evaluare	V	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		S	2.9 Codul disciplinei	6		2.10 Tipul de notare	Nota

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

3.1 Număr de ore pe săptămână	2	Din care: 3.2 curs	1	3.3 seminar/laborator	1
3.4 Total ore din planul de învăţământ	28	Din care: 3.5 curs	14	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					20
Tutorat					0
Examinări					2
Alte activităţi (dacă există):					0

3.7 Total ore studiu individual	22.00
3.8 Total ore pe semestru	50
3.9 Numărul de credite	2

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Să aibă competenţe obţinute ca urmare a parcurgerii cursului / cursurilor de informatică. • Este obligatoriu ca studenţii să aibă cunoştinţe pentru a folosi sistemul de operare Linux. • Fiecare student trebuie să aibă cunoştinţe despre sistemele de operare / mediile de lucru Unix (Free BSD, OpenBSD) si cunoştinţe de bază de a configura sistemul de operare Windows). • Fiecare student trebuie să aibă cunoştinţe de bază de reţea de calculatoare. • În plus, fiecare student trebuie să aibă cunoştinţe de bază de programare. Parcurgerea şi/sau promovarea următoarelor programe este benefică: • Sisteme de Operare Linux • Baze de date • Aplicaţii web
4.2 de rezultate ale învăţării	Acumularea următoarelor cunoştinţe: • Fiecare student trebuie sa aibă abilitaţi de a utiliza un calculator personal si un server. • Studenţii trebuie sa ştie sa utilizeze calculatoare interconectate in reţea. • Utilizarea cunoştinţelor de configurarea a calculatoarelor si a reţelelor de calculatoare • Folosirea cunoştinţelor de configurare a sistemelor de operare Unix / Linux / Windows

5. Condiţii necesare pentru desfăşurarea optimă a activităţilor didactice (acolo unde este cazul)

5.1 Curs	Videoproiector Note de curs Bibliografia recomandată
5.2 Seminar/ Laborator/Proiect	Calculatoare cu minim 2 maşini virtuale Linux, firewall; Prezenţa si activitatea obligatorie la laboratoare (conform regulamentului studiilor universitare de masterat în UPB).

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.)*

Obiectivul acestui curs este de a oferi o primă viziune asupra securităţii procedurale si informatice din interiorul unei întreprinderi dar şi de a creşte gradul de conştientizare al studenţilor asupra securităţii informatice. La sfârşitul cursului, studenţii vor înţelege câteva din conceptele de bază ale managementului întreprinderilor in general, al managementului operaţional procedural aplicate conceptelor de securitate informatică.
De asemenea cursul îşi propune să discute principiile de bază şi principalele tehnologii utilizate în securizarea calculatoarelor personale, managementul securităţii calculatoarelor personale, servicii de securitate pentru protejarea calculatoarelor personale: definiţii, tehnici şi mecanisme utilizate.

Aplicaţiile au ca obiectiv aplicarea conceptelor prezentate la curs, recunoaşterea particularităţilor contextului de aplicare a procedurilor si tehnologiilor de securitate informatice şi selectarea soluţiei optime. Se urmăresc proiectarea, configurarea, operarea si auditarea principalelor tehnologii legate de securitatea calculatoarelor personale şi de securizarea sistemelor de operare.
De asemenea cunoaşterea şi înţelegerea tipurilor actuale de atacuri informatice, a măsurilor tehnice de prevenire sau înlăturare a acestora, a procedurilor necesare de a fi aplicate si in final auditarea unui sistem complex.

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	La sfârşitul cursului, studenţii vor fi capabili: • Să identifice nevoile de protecţie şi • Să conceapă o procedură operaţională (de securitate informatică) • Să identifice si sa pună in balanţa avantajele şi dezavantaje, în termen de securitate, ale unei proceduri operaţionale. • Să expună si să implementeze strategii si principii fundamentale de luptă împotriva criminalităţii cibernetice. • Să dezvolte o soluţie / procedură pentru o anumită problemă de securitate. În plus, fiecare student va dezvolta mai multe abilităţi practice: • Activarea securităţii informatice la calculatoare. • Elaborarea de proceduri practice pentru a rezolva anumite probleme specifice legate de securitatea informatică. Proiectele scot in evidentă auto-învăţarea şi mai ales capacităţile de lucru în echipă (prin lucrul împreuna la temele de tip proiect). Cursul are in vedere dobândirea cunoştinţelor necesare personalului din organizaţiile din domeniul IT&C pentru a aplica si implementa proiecte de specialitate. De asemenea studenţii îşi vor îmbunătăţi cunoştinţele şi abilităţile lor în limba engleză/franceză (o parte a predării si a bibliografiei, câteva materiale suplimentare sunt in limba engleză/franceză).
Transversale (generale)	• Abilitatea de a lucra în echipă; • Abilitate de comunicare; • Abilităţi de utilizare a calculatorului, a tehnologiei informaţiei şi a aparaturii specifice; • Capacitate de asumare a responsabilităţii; • Capacitate de documentare, cercetare şi elaborare de studii de specialitate; • Capacitate de formare continuă, de dezvoltare personală şi profesională pe toată durata activităţii.

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.* • Capacitatea de a analiza riscurile de securitate şi a determina specificaţiile echipamentelor si sistemelor electronice si de comunicaţie securizate; • Identificarea vulnerabilităţilor si riscurilor de securitate la nivelul protocoalelor si reţelelor de telecomunicaţii (inclusiv virtualizare si cloud) si utilizarea de protocoale de securitate; • Conceperea, proiectarea si implementarea planurilor de securitate la nivelul organizaţiei/infrastructurii critice; • Capacitatea de a proiecta si implementa aplicaţii, sisteme si protocoale criptografice, folosind dispozitive FPGA, sisteme on-chip, software etc • Capacitatea de a proiecta si implementa sisteme hardware (calculatoare, terminale mobile) si software (baze de date, aplicaţii software) securizate • Capacitatea de a evalua si audita securitatea sistemelor de control industrial si a infrastructurilor critice, de a aplica standarde de securitate si auditare; • Capacitatea de a înţelege si propune soluţii de securitate avansata bazata pe machine learning, inteligentei artificiale si masive de date (big data); • Capacitatea de a analiza si propune soluţii de securizare si exploatare a conţinutului multimedia; • Îndeplinirea sarcinilor profesionale cu identificarea exactă a obiectivelor de realizat, a unor factori potenţiali de risc, a resurselor disponibile, a aspectelor economico-financiare, condiţiilor de finalizare a acestora, etapelor de lucru, timpului de lucru, şi termenelor de realizare aferente; • Executarea responsabilă a unor sarcini de lucru în echipă pluridisciplinară cu asumarea de roluri pe diferite paliere ierarhice.
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).* • Abilitatea de a lucra în echipă; • Abilitate de comunicare; • Abilităţi de utilizare a calculatorului, a tehnologiei informaţiei şi a aparaturii specifice; • Capacitate de asumare a responsabilităţii; • Capacitate de documentare, cercetare şi elaborare de studii de specialitate; • Capacitate de formare continuă, de dezvoltare personală şi profesională pe toată durata activităţii.
Responsabilitate şi autonomie	*Capacitatea cursantului de a aplica în mod autonom şi responsabil cunoştinţele şi aptitudinile sale.* • Abilitatea de a lucra în echipă; • Abilitate de comunicare;

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.)*

- Prelegere

- Explicaţie
- Problematizare
- Demonstraţie
- Conversaţie
- Studii de caz

Cursurile sunt predate într-o manieră interactivă, fiind încurajată participarea activă a studenţilor. Sunt folosite mijloace şi tehnici multimedia (videoproiector). Materialele de curs (notele şi prezentările de curs) sunt disponibile studenţilor în format electronic.

10. Conţinuturi

CURS		
Capitolul	**Conţinutul**	**Nr. ore**
1	1. Contextul organizaţional privind incidentele de securitate. Conducerea organizaţiei/întreprinderii in raport cu securitatea informaţionala. Procedura audit securitate IT: • interviuri cu departamentul tehnic al companiei; • observarea modului de lucru al angajaţilor; • analiza configuraţiilor hardware/software ale echipamentelor; • conceptul si designul unei politici de securitate IT&C; • implementarea celor mai potrivite soluţii de securitate a reţelelor; • sisteme de acces protejat, local sau la distanta; • soluţii firewall si VPN; • detectarea intruziunilor (IDS) si evaluarea vulnerabilităţii; • securitatea conţinutului (soluţii antivirus, filtrare web si e-mail); • soluţii de autentificare; • soluţii de criptare si semnături digitale; • soluţii de management al securităţii; • elaborarea unui raport complet privind infrastructura IT si a securităţii existente. 2. Evaluarea riscurilor / planificarea procesului de tratare a riscurilor 3. Resursele necesare pentru implementare 4. Implementare si control procese funcţionale 5. Evaluarea eficacitate si performanta aplicării masurilor de securitatea informaţiei 6. Monitorizare si îmbunătăţire continuă 7. Standardizarea ITIL (IT Infrastructure Library) şi IT Service Management • Strategia de service • Proiectarea • Tranziţia • Operare • Îmbunătăţirea continuă	14
	Total:	14

Bibliografie:

1. C. V. Marian, "Support for course and lab" , "Suport de curs si laborator", Moodle UPB, https://curs.upb.ro/
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems (replacing Sistemul de management al securităţii informaţiei ISO/IEC 27001:2013)
3. MIHAI Ioan-Cosmin, "Securitatea sistemului informatic", ISBN 978-973-627-369-8, Editura Dunărea de Jos (2007)
4. L Brotherston, A Berlin. "Defensive Security Handbook: Best Practices for Securing Infrastructure", O'Reilly Media Ed, 2017.
5. S Bosworth, M E Kabay, E Whyne. "Computer Security Handbook, 6th Edition (vol 1, vol 2)", Wiley Ed, 2014.
6. C. V. Marian, „Operating systems and web applications fundamentals”, Editura Politehnica Press, Bucureşti, 2021, ISBN 978-606-515-989-1
7. C. V. Marian, „Apprendre l'administration des systèmes d'exploitation par des exemples (Linux)”, Editura Politehnica Press, Bucureşti, 2022, ISBN 978-606-9608-19-7
8. C. V. Marian, „Applications pour les administrateurs de systèmes et les serveurs Linux”, Editura Politehnica Press, Bucureşti, 2023, ISBN 978-606-9608-67-8
9. M. T. Goodrich, R. Tamassia. "Introduction to Computer Security". Person Ed., International Edition. 2010.
10. Wm. A. Conklin, G. G. White, C. Cothren, D. Williams, R. L. Davis. "Principles of Computer Security. Security+ and Beyond". Mc Graw Hill Higher Education Ed. 2004.
11. W. Stallings. "Computer Security: Principles and Practice". Prentice Hall Ed. 2011.
12. W. Stallings. "Cryptography and Network Security: Principles and Practice". Pearson Ed., International Edition. 2010.
13. G. Avoine, P. Junod, P. Oechslin. "Computer System Security". EPFL Press. 2007.

LABORATOR

Nr. crt.	Conţinutul	Nr. ore
1	1. Formularea obiectivelor si cerinţelor de securitate a organizaţiilor ; Asigurarea ca riscurile de securitate sunt gestionate in mod eficient din punct de vedere al costului; 2. Asigurarea unei conformităţi cu legislaţia si diverse reglementari; Implementarea si gestionarea proceselor existente de management al securităţii informaţiei; 3. Definirea de noi procese de management a securităţii informaţiei; Identificarea si clarificarea proceselor existente de management a securităţii informaţiei; 4. Utilizarea lui de către conducerea organizaţiilor pentru a determina starea activităţilor de management a securităţii informaţiei; 5. Utilizarea de către auditorii interni si externi ai organizaţiilor pentru a determina gradul de conformitate cu politicile, directivele si standardele adoptate de către organizaţie; Furnizarea de informaţii relevante despre politicile de securitate a informaţiei, directivele, standardele si procedurile către partenerii comerciali si alte organizaţii cu care organizaţia interacţionează, din motive operaţionale sau comerciale; 6. Punerea in aplicare a strategiei activând securitatea informaţiei; Furnizarea de informaţii relevante despre securitatea informaţiei clienţilor organizaţiei. 7. Colocviu final	14

	Total:	14

Bibliografie:

1. C. V. Marian, "Support for course and lab" , "Suport de curs si laborator", Moodle UPB, https://curs.upb.ro/
2. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems (replacing Sistemul de management al securităţii informaţiei ISO/IEC 27001:2013)
3. L Brotherston, A Berlin. "Defensive Security Handbook: Best Practices for Securing Infrastructure", O'Reilly Media Ed, 2017.
4. W. Stallings. "Computer Security: Principles and Practice". Prentice Hall Ed. 2011.
5. Paul Cobbaut. Linux Security http://linux-training.be/index.php?nav=security
6. C. V. Marian, Operating systems and web applications fundamentals, Editura Politehnica Press, Bucureşti, 2021, ISBN 978-606-515-989-1
7. C. V. Marian, Apprendre l'administration des systèmes d'exploitation par des exemples (Linux), Editura Politehnica Press, Bucureşti, 2022, ISBN 978-606-9608-19-7
8. C. V. Marian, Applications pour les administrateurs de systèmes et les serveurs Linux, Editura Politehnica Press, Bucureşti, 2023, ISBN 978-606-9608-67-8

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 privind securitatea tehnica si procedurala a calculatoarelor; - cunoaşterea modului de aplicare a procedurilor in cazul problemelor specifice; - analiza diferenţială a tehnicilor şi metodelor teoretice de audit; - capacitatea de analiză a literaturii de specialitate prin studiu individual şi extragerea informaţiilor cheie privind eliminarea vulnerabilităţilor de securitate	Examen scris în sesiunea de examene corespunzătoare semestrului sau verificare; subiectele acoperă întreaga materie, realizând o sinteză între parcurgerea teoretică comparativă a materiei şi aplicaţii.	20%
11.5 Seminar/laborator/proiect	Configurarea echipamentelor conform noţiunilor de curs şi a tehnicilor prezentate	Colocviu final cu susţinere de proiect/laborator. Sunt evaluate atât înţelegerea aspectelor teoretice, cât şi abilitatea de a implementa şi testa o problemă practică.	80%
11.6 Condiţii de promovare			

- cunoașterea, înțelegerea și utilizarea corectă a procedurilor si a conceptelor fundamentale din cadrul domeniului securității calculatoarelor personale;
- înțelegerea principalelor tipuri de atacuri informatice și capacitatea de a proiecta si organiza procedural un sistem de securizare funcțional;
- realizarea obligațiilor caracteristice activității de proiect / laborator (participarea la lucrările planificate);
- obtinerea a minum jumatate din punctajul de la curs si jumatate din punctajul de la 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)

Industria are o cerere importantă de ingineri calificaţi, cu specializări legate de securitate informatică şi cu un fundament solid în electronică, sisteme şi tehnologia informaţiei, astfel încât să se poată menţine ritmul de dezvoltare de noi produse hardware şi aplicaţii software.

Programa cursului răspunde concret acestor cerinţe actuale de dezvoltare şi evoluţie, subscrise economiei europene a serviciilor din domeniul de telecomunicaţii avansate. În contextul progresului tehnologic actual al dispozitivelor electronice, domeniile de activitate vizate sunt practic nelimitate.

Se asigură astfel absolvenţilor competenţe adecvate cu necesităţile calificărilor actuale si o pregătire ştiinţifică şi tehnică moderne, de calitate şi competitive,care să le permită angajarea rapidă după absolvire, fiind perfect încadrat în politica Universităţii Nationale de Stiinte si Tehnologie Politehnica din Bucureşti, atât din punctul de vedere al conţinutului şi structurii, cât şi din punctul de vedere al aptitudinilor şi deschiderii internaţionale oferite studenţilor.

Cursul și aplicațiile de proiect / laborator oferă studenților baza de cunoștințe necesară înțelegerii principalelor probleme de securitate legate de calculatoarele personale și modalități specifice de abordare. Concret, disciplina oferă atât cunoștințele necesare proiectării și validării unor politici de securitate adecvate protecției calculatoarelor personale, cât și capacitatea de aplicare a tehnicilor de analiză și detecție a unor atacuri informatice și de eliminare sau diminuare a efectului acestor atacuri asupra sistemelor de calcul personale.

Programa disciplinei răspunde concret cerințelor actuale de dezvoltare și evoluție a economiei europene și a serviciilor din domeniul ICT. În contextul progresului tehnologic actual al sistemelor și dispozitivelor electronice de calcul, domeniile de activitate vizate sunt practic nelimitate, de la utilizarea sistemelor de calcul de mari dimensiuni până la folosirea unor terminale portabile de ultimă generație. Programa se referă atât la măsurile tehnice ce se impun protecției informatice, cât și la cele care vizează comportamentul angajaților în relația acestora cu tehnica de calcul din dotare.

Disciplina asigură absolvenților competente adecvate cu necesitățile calificărilor actuale și o pregătire științifică și tehnică moderne, de calitate și competitive, care să le permită angajarea rapidă după absolvire, fiind perfect încadrată în politica Universității POLITEHNICA din 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 industrial de cercetare-dezvoltare precum organizații/firme de orice dimensiune, de la cele mici create de studenți/masteranzi, până la cele multinaționale, care utilizează calculatoare personale (conectate sau nu în rețea) și sunt interesate în managementul securității acestora

Data completării | Titular de curs | Titular(i) de aplicații

Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației

21.09.2026	Conf. Dr. Constantin Viorel Marian	Conf. Dr. Constantin Viorel Marian

Data avizării în departament	Director de departament
22.09.2026	Conf. Dr. Serban Georgica Obreja



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

