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	Comunicații Wireless Avansate

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Managementul incidentelor de securitate și audit The Management and Audit of Security Incidents			
2.2 Titularul activităților de curs				Conf.dr.ing. Constantin Viorel Marian			
2.3 Titularul activităților de seminar / laborator				Conf.dr.ing. Constantin Viorel Marian			
2.4 Anul de studiu	1	2.5 Semestrul	I	2.6. Tipul de evaluare	V	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei		DA	2.9 Codul disciplinei	UPB.04.M1.O.21-13		2.10 Tipul de notare	Nota

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

3.1 Număr de ore pe săptămână	2	Din care: 3.2 curs	1.00	3.3 seminar/laborator	1
3.4 Total ore din planul de învățământ	28.00	Din care: 3.5 curs	14	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					14
Tutorat					2
Examinări					4
Alte activități (dacă există):					2

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

4. Precondiții (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 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 cunoașterea și înțelegerea 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. 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	· La sfârșitul cursului, studenții vor fi capabili: o Să identifice nevoile de protecție și o Să conceapă o procedură operațională (de securitate informatică) o Să identifice si sa pună in balanța avantajele și dezavantaje, în termen de securitate, ale unei proceduri operaționale. o Să expună si să implementeze strategii si principii fundamentale de luptă împotriva criminalității cibernetice. o Să dezvolte o soluție / procedură pentru o anumită problemă de securitate. · În plus, fiecare student va dezvolta mai multe abilități practice: o Activarea securității informatice la calculatoare. o Elaborarea de proceduri practice pentru a rezolva anumite probleme specifice legate de securitatea informatică. · Proiectele scot in evidentă auto-învățarea și mai ales capacitățile de lucru în echipă (prin lucrul împreuna la temele de tip proiect). · Cursul are in vedere dobândirea cunoștințelor necesare personalului din organizațiile din domeniul IT&C pentru a aplica si implementa proiecte de specialitate. · De asemenea studenții își vor îmbunătăți cunoștințele și abilitățile 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; • Abilități de utilizare a calculatorului, a tehnologiei informației și a aparaturii specifice; • Capacitate de asumare a responsabilității; • Capacitate de documentare, cercetare și elaborare de studii de specialitate; • Capacitate de formare continuă, de dezvoltare personală și profesională pe toată durata activității.

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.)*

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

- Explicație
- Problematizare
- Demonstrație
- Conversație
- Studii de caz

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

10. Conținuturi

CURS		
Capitolul	**Conținutul**	**Nr. ore**
1	1. Contextul organizațional privind incidentele de securitate. Conducerea organizației/întreprinderii in raport cu securitatea informaționala. Procedura audit securitate IT: • interviuri cu departamentul tehnic al companiei; • observarea modului de lucru al angajaților; • analiza configurațiilor hardware/software ale echipamentelor; • conceptul si designul unei politici de securitate IT&C; • implementarea celor mai potrivite soluții de securitate a rețelelor; • sisteme de acces protejat, local sau la distanta; • soluții firewall si VPN; • detectarea intruziunilor (IDS) si evaluarea vulnerabilității; • securitatea conținutului (soluții antivirus, filtrare web si e-mail); • soluții de autentificare; • soluții de criptare si semnături digitale; • soluții de management al securității; • elaborarea unui raport complet privind infrastructura IT si a securității existente. 2. Evaluarea riscurilor / planificarea procesului de tratare a riscurilor 3. Resursele necesare pentru implementare 4. Implementare si control procese funcționale 5. Evaluarea eficacitate si performanta aplicării masurilor de securitatea informației 6. Monitorizare si îmbunătățire continuă 7. Standardizarea ITIL (IT Infrastructure Library) și IT Service Management • Strategia de service • Proiectarea • Tranziția • Operare • Îmbunătățirea continuă	14
	Total:	14

Bibliografie:

. C. V. Marian, "Support for course and lab" , "Suport de curs si laborator", Moodle UPB, https://curs.upb.ro/
. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems (replacing Sistemul de management al securității informației ISO/IEC 27001:2013)
. MIHAI Ioan-Cosmin, "Securitatea sistemului informatic", ISBN 978-973-627-369-8, Editura Dunărea de Jos (2007)
. L Brotherston, A Berlin. "Defensive Security Handbook: Best Practices for Securing Infrastructure", O'Reilly Media Ed, 2017.
. S Bosworth, M E Kabay, E Whyne. "Computer Security Handbook, 6th Edition (vol 1, vol 2)", Wiley Ed, 2014.
. C. V. Marian, „Operating systems and web applications fundamentals”, Editura Politehnica Press, București, 2021, ISBN 978-606-515-989-1
. C. V. Marian, „Apprendre l'administration des systèmes d'exploitation par des exemples (Linux)”, Editura Politehnica Press, București, 2022, ISBN 978-606-9608-19-7
. C. V. Marian, „Applications pour les administrateurs de systèmes et les serveurs Linux”, Editura Politehnica Press, București, 2023, ISBN 978-606-9608-67-8
. M. T. Goodrich, R. Tamassia. "Introduction to Computer Security". Person Ed., International Edition. 2010.
0. 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.
1. W. Stallings. "Computer Security: Principles and Practice". Prentice Hall Ed. 2011.
2. W. Stallings. "Cryptography and Network Security: Principles and Practice". Pearson Ed., International Edition. 2010.
3. G. Avoine, P. Junod, P. Oechslin. "Computer System Security". EPFL Press. 2007.

LABORATOR

Nr. crt.	Conținutul	Nr. ore
1	1. Formularea obiectivelor si cerințelor de securitate a organizațiilor ; Asigurarea ca riscurile de securitate sunt gestionate in mod eficient din punct de vedere al costului; 2. Asigurarea unei conformități cu legislația si diverse reglementari; Implementarea si gestionarea proceselor existente de management al securității informației; 3. Definirea de noi procese de management a securității informației; Identificarea si clarificarea proceselor existente de management a securității informației; 4. Utilizarea lui de către conducerea organizațiilor pentru a determina starea activităților de management a securității informației; 5. Utilizarea de către auditorii interni si externi ai organizațiilor pentru a determina gradul de conformitate cu politicile, directivele si standardele adoptate de către organizație; Furnizarea de informații relevante despre politicile de securitate a informației, directivele, standardele si procedurile către partenerii comerciali si alte organizații cu care organizația interacționează, din motive operaționale sau comerciale; 6. Punerea in aplicare a strategiei activând securitatea informației; Furnizarea de informații relevante despre securitatea informației clienților organizației. 7. Colocviu final	14
	Total:	14

Bibliografie:

- C. V. Marian, "Support for course and lab" , "Suport de curs si laborator", Moodle UPB, https://curs.upb.ro/
- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems (replacing Sistemul de management al securității informației ISO/IEC 27001:2013)
- L Brotherston, A Berlin. "Defensive Security Handbook: Best Practices for Securing Infrastructure", O'Reilly Media Ed, 2017.
- W. Stallings. "Computer Security: Principles and Practice". Prentice Hall Ed. 2011.
- Paul Cobbaut. Linux Security http://linux-training.be/index.php?nav=security
- C. V. Marian, Operating systems and web applications fundamentals, Editura Politehnica Press, București, 2021, ISBN 978-606-515-989-1
- C. V. Marian, Apprendre l'administration des systèmes d'exploitation par des exemples (Linux), Editura Politehnica Press, București, 2022, ISBN 978-606-9608-19-7
- C. V. Marian, Applications pour les administrateurs de systèmes et les serveurs Linux, Editura Politehnica Press, București, 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	- cunoașterea noțiunilor teoretice fundamentale privind securitatea tehnica si procedurala a calculatoarelor; - cunoașterea modului de aplicare a procedurilor in cazul problemelor specifice; - analiza diferențială a tehnicilor și metodelor teoretice de audit; - capacitatea de analiză a literaturii de specialitate prin studiu individual și extragerea informațiilor cheie privind eliminarea vulnerabilităților de securitate	Examen scris în sesiunea de examene corespunzătoare semestrului; subiectele acoperă întreaga materie, realizând o sinteză între parcurgerea teoretică comparativă a materiei și aplicații.	50%
11.5 Seminar/laborator/proiect	configurarea echipamentelor conform noțiunilor de curs și a tehnicilor prezentate	Colocviu final cu susținere de proiect/laborator. Sunt evaluate atât înțelegerea aspectelor teoretice, cât și abilitatea de a implementa și testa o problemă practică.	50%
11.6 Condiții de promovare			

- cunoaşterea, înţelegerea şi utilizarea corectă a procedurilor si a conceptelor fundamentale din cadrul domeniului securităţii calculatoarelor personale; - înţelegerea principalelor tipuri de atacuri informatice şi capacitatea de a proiecta si organiza procedural un sistem de securizare funcţional; - realizarea obligaţiilor caracteristice activităţii 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)

Cursul şi aplicaţiile de proiect / laborator oferă studenţilor baza de cunoştinţe necesară înţelegerii principalelor probleme de securitate legate de calculatoarele personale şi modalităţi specifice de abordare. Concret, disciplina oferă atât cunoştinţele necesare proiectării şi validării unor politici de securitate adecvate protecţiei calculatoarelor personale, cât şi capacitatea de aplicare a tehnicilor de analiză şi detecţie a unor atacuri informatice şi de eliminare sau diminuare a efectului acestor atacuri asupra sistemelor de calcul personale.

Programa disciplinei răspunde concret cerinţelor actuale de dezvoltare şi evoluţie a economiei europene şi a serviciilor din domeniul ICT. În contextul progresului tehnologic actual al sistemelor şi 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 generaţie. Programa se referă atât la măsurile tehnice ce se impun protecţiei informatice, cât şi la cele care vizează comportamentul angajaţilor în relaţia acestora cu tehnica de calcul din dotare.

Disciplina asigură absolvenţilor competente adecvate cu necesităţile calificărilor actuale şi o pregătire ştiinţifică şi tehnică moderne, de calitate şi competitive, care să le permită angajarea rapidă după absolvire, fiind perfect încadrată în politica Universităţii 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. Posibilii angajatori vizează atât mediul academic (profil didactic şi de cercetare) cât şi mediul industrial de cercetare-dezvoltare precum organizaţii/firme de orice dimensiune, de la cele mici create de studenţi/masteranzi, până la cele multinaţionale, care utilizează calculatoare personale (conectate sau nu în reţea) şi sunt interesate în managementul securităţii acestora

Data completării	Titular de curs	Titular(i) de aplicaţii
10.09.2024	Conf.dr.ing. Constantin Viorel Marian	Conf.dr.ing. Constantin Viorel Marian

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

Universitatea Națională de Știință și Tehnologie Politehnica București

Facultatea de Electronică, Telecomunicații și

Tehnologia Informației

Data aprobării în Consiliul Facultății

25.10.2024

Decan

Prof. Dr. Mihnea Udrea