



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, Telecomunicații și Tehnologii Informaționale
1.5 Ciclu de studii	Masterat
1.6 Specializarea	Comunicații Wireless Avansate

2. Date despre disciplină

2.1 Denumirea disciplinei (ro)		Managementul incidentelor de securitate și audit					
(en)		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					14
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					
Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					
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	<ul style="list-style-type: none">Să aibă competențe obținute ca urmare a parcurgerii cursului / cursurilor de informatică.Este obligatoriu ca studenții să aibă cunoștințe pentru a folosi sistemul de operare Linux.Fiecare student trebuie să aibă cunoștințe despre sistemele de operare / mediile de lucru Unix (Free BSD, OpenBSD) și cunoștințe de bază de a configura sistemul de operare Windows).Fiecare student trebuie să aibă cunoștințe de bază de rețea de calculatoare.În plus, fiecare student trebuie să aibă cunoștințe de bază de programare. Parcurgerea și/sau promovarea următoarelor programe este benefică: <ul style="list-style-type: none">Sisteme de Operare LinuxBaze de dateAplicații web
4.2 de rezultate ale învățării	<ul style="list-style-type: none">Acumularea următoarelor cunoștințe:Fiecare student trebuie să aibă abilitați de a utiliza un calculator personal și un server.Studenții trebuie să știe să utilizeze calculatoare interconectate în rețea.Utilizarea cunoștințelor de configurarea a calculatoarelor și a rețelelor de calculatoareFolosirea cunoștințelor de configurare a sistemelor de operare Unix / Linux / Windows

5. Condiții necesare pentru desfășurarea optimă a activităților didactice (acolo unde este cazul)

5.1 Curs	<ul style="list-style-type: none">VideoproiectorNote de cursBibliografia recomandată
5.2 Seminar/ Laborator/Proiect	<ul style="list-style-type: none">Calculatoare cu minim 2 mașini virtuale Linux, firewall;Prezența obligatorie la laboratoare (conform regulamentului studiilor universitare de masterat în UPB).

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.)

· Obiectivul acestui curs este de a oferi o primă viziune asupra securității procedurale și informatice din interiorul unei întreprinderi dar și de a crește gradul de conștientizare al studenților asupra securității informatice. La sfârșitul cursului, studenții vor înțelege câteva din conceptele de bază ale managementului întreprinderilor în general, al managementului operațional procedural aplicat conceptelor de securitate informatică.

De asemenea cursul își propune să discute principiile de bază și principalele tehnologii utilizate în securizarea calculatoarelor personale, managementul securității calculatoarelor personale, servicii de securitate pentru protejarea calculatoarelor personale: definiții, tehnici și mecanisme utilizate.

· Aplicațiile au ca obiectiv aplicarea conceptelor prezentate la curs, recunoașterea particularităților contextului de aplicare a procedurilor și tehnologiilor de securitate informatice și selectarea soluției optime. Se urmăresc proiectarea, configurarea, operarea și auditarea principalelor tehnologii legate de securitatea calculatoarelor personale și 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 și în 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	<ul style="list-style-type: none">· La sfârșitul cursului, studenții vor fi capabili:<ul style="list-style-type: none">o Să identifice nevoile de protecție șio Să conceapă o procedură operațională (de securitate informatică)o Să identifice și să pună în balanța avantajele și dezavantaje, în termen de securitate, ale unei proceduri operaționale.o Să expună și să implementeze strategii și 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:<ul style="list-style-type: none">o Activarea securității informatice la calculatoare.o Elaborarea de proceduri practice pentru a rezolva anumite probleme specifice legate de securitatea informatică.· Proiectele scot în evidență auto-învățarea și mai ales capacitățile de lucru în echipă (prin lucrul împreună la temele de tip proiect).· Cursul are în vedere dobândirea cunoștințelor necesare personalului din organizațiile din domeniul IT&C pentru a aplica și implementa proiecte de specialitate.<ul style="list-style-type: none">· De asemenea studenții își vor îmbunătăți cunoștințele și abilitățile lor în limba engleză/franceză (o parte a predării și a bibliografiei, câteva materiale suplimentare sunt în limba engleză/franceză).
Transversale (generale)	<ul style="list-style-type: none">• 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 exemplurilor 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	<p><i>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.</i></p> <ul style="list-style-type: none">• Capacitatea de a analiza riscurile de securitate și a determina specificațiile echipamentelor și sistemelor electronice și de comunicație securizate;• Identificarea vulnerabilităților și riscurilor de securitate la nivelul protocoalelor și rețelelor de telecomunicații (inclusiv virtualizare și cloud) și utilizarea de protocoale de securitate;• Conceperea, proiectarea și implementarea planurilor de securitate la nivelul organizației/infrastructurii critice;• Capacitatea de a proiecta și implementa aplicații, sisteme și protocoale criptografice, folosind dispozitive FPGA, sisteme on-chip, software etc• Capacitatea de a proiecta și implementa sisteme hardware (calculatoare, terminale mobile) și software (baze de date, aplicații software) securizate• Capacitatea de a evalua și audita securitatea sistemelor de control industrial și a infrastructurilor critice, de a aplica standarde de securitate și auditare;• Capacitatea de a înțelege și propune soluții de securitate avansată bazată pe machine learning, inteligenței artificiale și masive de date (big data);• Capacitatea de a analiza și propune soluții de securizare și exploatare a conținutului multimedia;• Îndeplinirea sarcinilor profesionale cu identificarea exactă a obiectivelor de realizat, a unor factori potențiali de risc, a resurselor disponibile, a aspectelor economico-financiare, condițiilor de finalizare a acestora, etapelor de lucru, timpului de lucru, și termenelor de realizare aferente;• Executarea responsabilă a unor sarcini de lucru în echipă pluridisciplinară cu asumarea de roluri pe diferite paliere ierarhice.
Aptitudini	<p><i>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).</i></p> <ul style="list-style-type: none">• 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.
Responsabilitate și autonomie	<p><i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.</i></p> <ul style="list-style-type: none">• 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 studenților la stabilirea propriului parcurs de învățare, cum se identifică eventualele rămăneri în urmă și 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	<p>1. Contextul organizațional privind incidentele de securitate. Conducerea organizației/întreprinderii în raport cu securitatea informațională.</p> <p>Procedura audit securitate IT:</p> <ul style="list-style-type: none">• interviuri cu departamentul tehnic al companiei;• observarea modului de lucru al angajaților;• analiza configurațiilor hardware/software ale echipamentelor;• conceptul și designul unei politici de securitate IT&C;• implementarea celor mai potrivite soluții de securitate a rețelelor;• sisteme de acces protejat, local sau la distanță;• soluții firewall și VPN;• detectarea intruziunilor (IDS) și evaluarea vulnerabilității;• securitatea conținutului (soluții antivirus, filtrare web și e-mail);• soluții de autentificare;• soluții de criptare și semnături digitale;• soluții de management al securității;• elaborarea unui raport complet privind infrastructura IT și a securității existente. <p>2. Evaluarea riscurilor / planificarea procesului de tratare a riscurilor</p> <p>3. Resursele necesare pentru implementare</p> <p>4. Implementare și control procese funcționale</p> <p>5. Evaluarea eficacitate și performanța aplicării măsurilor de securitatea informației</p> <p>6. Monitorizare și îmbunătățire continuă</p> <p>7. Standardizarea ITIL (IT Infrastructure Library) și IT Service Management</p> <ul style="list-style-type: none">• 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.
- 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.
- W. Stallings. "Computer Security: Principles and Practice". Prentice Hall Ed. 2011.
- W. Stallings. "Cryptography and Network Security: Principles and Practice". Pearson Ed., International Edition. 2010.
- 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	<ul style="list-style-type: none">- cunoașterea noțiunilor teoretice fundamentale privind securitatea tehnica si procedurata 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			



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

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 (SEIS)

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. Programă 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. Posibili 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

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

Decan

25.10.2024

Prof. Dr. Mihnea Udrea