



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	Tehnologie Electronică și Fiabilitate
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicații și Tehnologii Informaționale
1.5 Ciclul de studii	Masterat
1.6 Specializarea	Ingineria Calității și Siguranței în Funcționare în Electronică și Telecomunicații

2. Date despre disciplină

2.1 Denumirea disciplinei (ro)		Modelarea stohastică și statistică aplicată					
(en)		Stochastic modeling and applied statistics					
2.2 Titularul activităților de curs		Conf. Dr. Emil SIMION					
2.3 Titularul activităților de seminar / laborator		Conf. Dr. Emil SIMION					
2.4 Anul de studiu	1	2.5 Semestrul	I	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Ob
2.8 Tipul disciplinei	DS	2.9 Codul disciplinei	UPB.04.M1.O.14-01	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					40
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					
Pregătire seminarii/ laboratoare/proiecte, teme, referate, portofolii și eseuri					
Tutorat					4
Examinări					3
Alte activități (dacă există):					0
3.7 Total ore studiu individual	47.00				
3.8 Total ore pe semestru	75				
3.9 Numărul de credite	3				

4. Precondiții (acolo unde este cazul)

4.1 de curriculum	Nu este cazul.
4.2 de rezultate ale învățării	Acumularea unor cunoștințe de bază din domeniile: statistică matematică, criptografie.

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	Seminarul se va desfășura într-o sală dotată cu videoproiector și computer.
-----------------------------------	---

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.*)

Aplicarea în mediul virtual a tehnicilor și metodelor probabiliste și statistice. Aplicarea, în situații tipice, a metodelor de proiectare a algoritmilor și protocoalelor criptografice (criptografia), precum și a metodelor de evaluare a acestora (criptanaliza).

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/avansate în domeniul statisticii aplicate și al criptografiei. Corelează cunoștințele. Aplică în practică cunoștințele. Aplică metode și instrumente standardizate, specifice domeniului, pentru realizarea procesului de evaluare și diagnoză a unei situații, în funcție de problemele identificate/raportate, și identifică soluții. Argumentează și analizează coerent și corect contextul de aplicare a cunoștințelor de bază ale domeniului, utilizând concepte cheie ale disciplinei și metodologia specifică. Comunicare orală și în scris în limba română: utilizează vocabularul științific specific domeniului, în vederea comunicării eficiente, în scris și oral.
Transversale (generale)	Lucrează în echipă și comunică eficient, 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, precum și de a desprinde și prezenta concluzii / identifica soluții. 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 reală/academică/profesională, 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 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> <p>Definește noțiuni specifice domeniului. Descrie/clasifică noțiuni/procese/fenomene/structuri. Evidențiază consecințe și relații. Cunoaște și aplică metodologii și instrumente specifice pentru crearea unei structuri logice și fizice a bazelor de date (structuri de date logice, diagrame, metodologii de modelare, relații între entități).</p>
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> <p>Selectează și grupează informații relevante într-un context dat. Utilizează argumentat principii specifice în vederea analizei relațiilor de dependență / independență, cauzalitate / asociere. Lucrează productiv în echipă. Elaborează un text științific. Rezolvă aplicații practice. Argumentează soluțiile identificate/modurile de rezolvare. Aplică scheme și modele de validare și analiză a algoritmilor și protocoalelor criptografice, realizează prelucrări / comparații / interpretări ale datelor. Dobândește, corectează sau îmbunătățește cunoștințele despre algoritmi și protocoale criptografice, utilizând metode și tehnici științifice.</p>



Responsabilitate și autonomie	<p><i>Capacitatea cursantului de a aplica în mod autonom și responsabil cunoștințele și aptitudinile sale.</i></p> <p>Selectează surse bibliografice potrivite și le analizează.</p> <p>Respectă principiile de etică academică, citând corect sursele bibliografice utilizate.</p> <p>Demonstrează receptivitate pentru contexte noi de învățare.</p> <p>Manifestă colaborare cu ceilalți colegi și cadre didactice în desfășurarea activităților didactice</p> <p>Demonstrează autonomie în organizarea situației/contextului de învățare sau a situației problemă de rezolvat</p> <p>Manifestă responsabilitate socială prin implicarea activă în viața socială studențească/implicare în evenimentele din comunitatea academică</p> <p>Promovează/contribuie prin soluții noi, aferente domeniului de specialitate pentru a îmbunătăți calitatea vieții sociale.</p> <p>Conștientizează valoarea contribuției sale în domeniul ingineriei la identificarea de soluții viabile/sustenabile care să rezolve probleme din viața socială și economică (responsabilitate socială).</p> <p>Aplică principii de etică/deontologie profesională în analiza impactului tehnologic al soluțiilor propuse în domeniul de specialitate asupra mediului înconjurător.</p> <p>Analizează și valorifică oportunități de afaceri/de dezvoltare antreprenorială în domeniul de specialitate.</p> <p>Demonstrează abilități de management al situațiilor din viața reală (gestionarea timpului colaborare vs. conflict).</p> <p>Identificarea oportunităților de formare continuă și utilizarea eficientă, pentru propria dezvoltare, a surselor informaționale și a resurselor de comunicare și formare profesională asistată (portaluri Internet, aplicații software de specialitate, baze de date, cursuri on-line etc.) atât în limba română, cât și într-o limbă de circulație internațională.</p> <p>Capacitatea de a comunica cu structurile ierarhice superioare și cu echipa aflată în subordine</p>
--------------------------------------	---

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.*)

Pornindu-se de la analiza caracteristicilor de învățare ale studenților și de la nevoile lor specifice, procesul de predare va explora metode de predare atât expositive (prelegerea, expunerea), cât și conservative-interactive, bazate pe modele de învățare prin descoperire facilitate de explorarea directă și indirectă a realității (experimentul, demonstrația, modelarea), dar și pe metode bazate pe acțiune, precum exercițiul, activitățile practice și rezolvarea de probleme. În activitatea de predare vor fi utilizate prelegeri, în baza unor prezentări Power Point sau diferite filmulețe care vor fi puse la dispoziția studenților. Fiecare curs va debuta cu recapitularea capitolelor deja parcurse, cu accent asupra noțiunilor parcurse la ultimul curs. Prezentările utilizează imagini și scheme, astfel încât informațiile prezentate să fie ușor de înțeles și asimilat. Această disciplină acoperă informații și activități practice menite să-i sprijine pe studenți în eforturile de învățare și de dezvoltare a unor relații optime de colaborare și comunicare într-un climat favorabil învățării prin descoperire.

10. Conținuturi

CURS		
Capitolul	Conținutul	Nr. ore
1	Teoria probabilităților. Scheme clasice de probabilitate. Distribuții de probabilitate. Teorema limită centrală.	1



2	Estimarea parametrilor. Estimare punctuală. Metoda momentelor și metoda verosimilității maxime.	2
3	Intervale de încredere. Teste statistice.	1
4	Teste statistice utilizate în evaluarea generatoarelor aleatoare și pseudoaleatoare.	2
5	Tehnici și metode criptografice. Algoritmi clasici de cifrare; Algoritmi simetrici de cifrare (AES, moduri de operare); Evaluarea de securitate.	2
6	Protocoale criptografice (identificare și autentificare, schimb de chei: Diffie-Hellman).	2
7	Evaluarea de securitate a infrastructurii de comunicații (algoritm, modul criptografic: ISO19790/FIPS 140-3, produse criptografice: ISO 15408/EUCC, sisteme: ISO27001, directiva NIS-2).	2
8	Studii de caz (analiza atacurilor ransomware, analize de securitate).	2
	Total:	14

Bibliografie:

1. A.J. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1999.
2. D. Naccache, E. Simion ș.a, Criptografie și Securitatea Informației. Aplicații, MATRIXROM, 2011.
3. B. Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, 1996.
4. E. Simion, V. Preda și A. Popescu, Criptanaliza. Rezultate și Tehnici Matematice, Ed. Univ. Buc., ISBN 973575975-6, 2004.
5. D. Stinton, Cryptography, Theory and Practice, Chapman & Hall/CRC, Third Edition, 2006.
6. W. Stalings, Cryptography and Network Security: Principles and Practice (6th Edition)- 6th Edition, 2013.
7. FIPS 140-2, Security Requirements for Cryptographic Modules, 2001.
8. National Institute of Standards and Technologies, SP 800-22, A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010.
9. Suport curs platforma Moodle UPB - <https://archive.curs.upb.ro/2022/course/view.php?id=10146>.

SEMINAR

Nr. crt.	Conținutul	Nr. ore
1	Aplicații ale teoremei limită centrală	2
2	Aplicații privind Estimarea parametrilor. Estimare punctuală. Metoda momentelor și metoda verosimilității maxime.	2
3	Intervale de încredere. Teste statistice.	2
4	Criptanaliza sistemelor clasice de cifrare. Criptanaliza și evaluarea de securitate a algoritmilor simetrici.	2
5	Evaluarea de securitate a algoritmilor criptografici asimetrici	2
6	Studii de caz privind atacurile ransomware	4
	Total:	14



Bibliografie:

1. A.J. Menezes, P. Oorschot, S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1999.
2. D. Naccache, E. Simion ș.a, Criptografie și Securitatea Informației. Aplicații, MATRIXROM, 2011.
3. B. Schneier, Applied Cryptography, Second Edition, John Wiley & Sons, 1996.
4. E. Simion, V. Preda și A. Popescu, Criptanaliza. Rezultate și Tehnici Matematice, Ed. Univ. Buc., ISBN 973575975-6, 2004.
5. D. Stinton, Cryptography, Theory and Practice, Chapman & Hall/CRC, Third Edition, 2006.
6. W. Stallings, Cryptography and Network Security: Principles and Practice (6th Edition)- 6th Edition, 2013.
7. FIPS 140-2, Security Requirements for Cryptographic Modules, 2001.
8. National Institute of Standards and Technologies, SP 800-22, A statistical test suite for random and pseudorandom number generators for cryptographic applications, 2010.
9. Suport curs platforma Moodle UPB - <https://archive.curs.upb.ro/2022/course/view.php?id=10146>.

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; - cunoașterea modului de aplicare a teoriei la probleme specifice; - analiza diferențială a tehnicilor și metodelor teoretice.	Articol științific și examen final	67%
11.5 Seminar/laborator/proiect	- cunoașterea aplicării, pe exemple concrete, a elementelor teoretice exemplificate în cadrul cursului.	Notare în timpul semestrului	33%
11.6 Condiții de promovare			
Obținerea a 50% din punctajul total. Obținerea a 50% din punctajul aferent activității pe parcursul semestrului.			

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 (SEİS)

Prin activitățile desfășurate, studenții dezvoltă abilități de a oferi soluții unor probleme și de a propune idei de îmbunătățire a situației existenței în domeniul statisticii matematice.

În dezvoltarea conținutului disciplinei s-au avut în vedere cunoștințe / aspecte / fenomene descrise de literatura de specialitate / cercetările proprii publicate / prezentate.

Prin activitățile de la seminar se are în vedere dezvoltarea abilităților absolventului de a gestiona situații practice cu care se poate confrunta în viața reală în scopul creșterii contribuției acestuia la îmbunătățirea mediului socio-economic.

Data completării

Titular de curs

Titular(i) de aplicații

11.10.2024

Conf. Dr. Emil SIMION

Conf. Dr. Emil SIMION



Universitatea Națională de Știință și Tehnologie Politehnica București
Facultatea de Electronică, Telecomunicații și
Tehnologia Informației



Data avizării în departament

Director de departament

Conf. dr. ing. Marian VLĂDESCU

Data aprobării în Consiliul Facultății

Decan

01.11.2024

Prof. Dr. Mihnea Udrea