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	**Tehnologie Electronică şi Fiabilitate**
1.4 Domeniul de studii	Inginerie Electronică, Telecomunicaţii şi Tehnologii Informaţionale
1.5 Ciclul de studii	Masterat
1.6 Specializarea	Ingineria Calităţii şi Siguranţei în Funcţionare în Electronică şi Telecomunicaţii

2. Date despre disciplină

2.1 Denumirea disciplinei (ro) (en)				Modelarea stochastică şi statistică aplicată Stochastic modeling and applied statistics			
2.2 Titularul activităţilor de curs				Conf. Dr. Emil SIMION			
2.3 Titularul activităţilor 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 activităţilor 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 învăţământ	28.00	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					40
Tutorat					4
Examinări					3
Alte activităţi (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. Precondiţii (acolo unde este cazul)

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

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

5.1 Curs	Cursul se va desfăşura într-o sală dotată cu videoproiector şi computer.

5.2 Seminar/ Laborator/Proiect	Seminarul se va desfăşura într-o sală dotată cu videoproiector şi computer.

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.)*

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

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	Demonstrează că deţine cunoştinţe de bază/avansate în domeniul statisticii aplicate şi al criptografiei. Corelează cunoştinţele. Aplică în practică cunoştinţele. Aplică metode şi instrumente standardizate, specifice domeniului, pentru realizarea procesului de evaluare şi diagnoză a unei situaţii, în funcţie de problemele identificate/raportate, şi identifică soluţii. Argumentează şi analizează coerent şi corect contextul de aplicare a cunostinţelor de bază ale domeniului, utilizând concepte cheie ale disciplinei şi metodologia specifică. Comunicare orală şi în scris în limba română: utilizează vocabularul ştiinţific specific domeniului, în vederea comunicării eficace, în scris şi oral.
Transversale (generale)	Lucrează în echipă şi comunică eficient, coordonându-şi eforturile cu ceilalţi pentru rezolvarea de situaţii problemă de complexitate medie. Autonomie şi gândire critică: abilitatea de a gândi în termeni ştiinţifici, de a căuta şi analiza date în mod independent, precum şi de a desprinde şi prezenta concluzii / identifica soluţii. Capacitate de analiză şi sinteză: prezintă în mod sintetic cunoştinţele 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 inteligenţă emoţională în gestionarea socio-emoţională adecvată a unor situaţii din viaţa reală/academică/profesională, demonstrând stăpânire de sine şi obiectivitate în luarea deciziilor sau în situaţii de stres.

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.* Defineşte noţiuni specifice domeniului. Descrie/clasifică noţiuni/procese/fenomene/structuri. Evidenţiază consecinţe şi relaţii. Cunoaşte şi aplică metodologii şi instrumente specifice pentru crearea unei structuri logice şi fizice a bazelor de date (structuri de date logice, diagrame, metodologii de modelare, relaţii între entităţi).
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. Utilizează argumentat principii specifice în vederea analizei relaţiilor de dependenţă / independenţă, cauzalitate / asociere. Lucrează productiv în echipă. Elaborează un text ştiinţific. Rezolvă aplicaţii practice. Argumentează soluţiile identificate/modurile de rezolvare. Aplică scheme şi modele de validare şi analiză a algoritmilor si protocoalelor criptografice, realizează prelucrări / comparaţii / interpretări ale datelor. Dobândeşte, corectează sau îmbunătăţeşte cunoştinţele despre algoritmi si protocoale criptografice, utilizând metode şi tehnici ştiinţifice.

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 situaţiei/contextului de învăţare sau a situaţiei problemă de rezolvat Manifestă responsabilitate socială prin implicarea activă în viaţa socială studenţească/implicare în evenimentele din comunitatea academică Promovează/contribuie prin soluţii noi, aferente domeniului de specialitate pentru a îmbunătăţi calitatea vieţii sociale. Conştientizează valoarea contribuţiei sale în domeniul ingineriei la identificarea de soluţii viabile/sustenabile care să rezolve probleme din viaţa socială şi economică (responsabilitate socială). Aplică principii de etică/deontologie profesională în analiza impactului tehnologic al soluţiilor propuse în domeniul de specialitate asupra mediului înconjurător. Analizează şi valorifică oportunităţi de afaceri/de dezvoltare antreprenorială în domeniul de specialitate. Demonstrează abilităţi de management al situaţiilor din viaţa reală (gestionarea timpului colaborare vs. conflict). Identificarea oportunităţilor de formare continuă şi utilizarea eficientă, pentru propria dezvoltare, a surselor informaţionale şi a resurselor de comunicare şi formare profesională asistată (portaluri Internet, aplicaţii software de specialitate, baze de date, cursuri on-line etc.) atât în limba romana, cât şi într-o limbă de circulaţie internaţională. Capacitatea de a comunica cu structurile ierarhice superioare şi cu echipa aflată în subordine

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.)*

Pornindu-se de la analiza caracteristicilor de învăţare ale studenţilor şi de la nevoile lor specifice, procesul de predare va explora metode de predare atât expozitive (prelegerea, expunerea), cât şi conversative-interactive, bazate pe modele de învăţare prin descoperire facilitate de explorarea directă şi indirectă a realităţii (experimentul, demonstraţia, modelarea), dar şi pe metode bazate pe acţiune, precum exerciţiul, activităţile practice şi rezolvarea de probleme. În activitatea de predare vor fi utilizate prelegeri, în baza unor prezentări Power Point sau diferite filmuleţe care vor fi puse la dispoziţia studenţilor. Fiecare curs va debuta cu recapitularea capitolelor deja parcurse, cu accent asupra noţiunilor parcurse la ultimul curs. Prezentările utilizează imagini şi scheme, astfel încât informaţiile prezentate să fie uşor de înţeles şi asimilat. Această disciplină acoperă informaţii şi activităţi practice menite să-i sprijine pe studenţi în eforturile de învăţare şi de dezvoltare a unor relaţii optime de colaborare şi comunicare într-un climat favorabil învăţării prin descoperire.

10. Conţinuturi

CURS		
Capitolul	**Conţinutul**	**Nr. ore**
1	Teoria probabilităţilor. Scheme clasice de probabilitate. Distribuţii 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 şi 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 ş.a, Criptografie şi Securitatea Informaţiei. Aplicaţii, MATRIXROM, 2011.
3. B. Schneier, Applied Criptography, Second Edition, John Wiley & Sons, 1996.
4. E. Simion, V. Preda şi A. Popescu, Criptanaliza. Rezultate şi 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 cripotgrafici 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 ş.a, Criptografie şi Securitatea Informaţiei. Aplicaţii, MATRIXROM, 2011.
3. B. Schneier, Applied Criptography, Second Edition, John Wiley & Sons, 1996.
4. E. Simion, V. Preda şi A. Popescu, Criptanaliza. Rezultate şi 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.

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; - cunoaşterea modului de aplicare a teoriei la probleme specifice; - analiza diferenţială a tehnicilor şi metodelor teoretice.	Articol ştiinţific şi examen final	67%
11.5 Seminar/laborator/proiect	- cunoaşterea aplicării, pe exemple concrete, a elementelor teoretice exemplificate în cadrul cursului.	Notare în timpul semestrului	33%
11.6 Condiţii de promovare			
Obţinerea a 50% din punctajul total. Obţinerea a 50% din punctajul aferent activităţii pe parcursul semestrului.			

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)

Prin activităţile desfăşurate, studenţii dezvoltă abilităţi de a oferi soluţii unor probleme şi de a propune idei de îmbunătăţire a situaţiei existenţei în domeniul statisticii matematice.

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

Prin activităţile de la seminar se are în vedere dezvoltarea abilităţilor absolventului de a gestiona situaţii practice cu care se poate confrunta în viaţa reală în scopul creşterii contribuţiei acestuia la îmbunătăţirea mediului socio-economic.

Data completării	Titular de curs	Titular(i) de aplicaţii
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