UNIVERSITATEA „VASILE ALECSANDRI” din BACĂU
Facultatea de Inginerie
Calea Mărăşeşti, Nr. 157, Bacău, 600115, Tel./Fax +40 234 580170
http://inginerie.ub.ro; e-mail: decaning@ub.ro

FIŞA DISCIPLINEI
(licenţă)

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea „Vasile Alecsandri” din Bacău
1.2. Facultatea	Facultatea de Inginerie
1.3. Departamentul	Departamentul de Energetică și Știința Calculatoarelor
1.4. Domeniul de studii	Calculatoare și Tehnologia Informației
1.5. Ciclul de studii	Licenţă
1.6. Programul de studii/calificarea	Tehnologia Informației
1.7. Forma de învăţământ	Învățământ cu frecvenţă

2. Date despre disciplină

2.1. Denumirea disciplinei	**Criptografie si Securitate Informațională**				
2.2. Titularul activităţilor de curs	Ș.l.dr.ing. Pruteanu Eusebiu				
2.3. Titularul activităţilor de seminar	Drd. Ing. Ungureanu Andrei Gabriel				
2.4. Anl de studiu	**2021-2022**	2.5. Semestrul	**6**	2.6. Tipul de evaluare	**C**
2.7. Regimul disciplinei	Categoria formativă a disciplinei DF - fundamentală, DD - în domeniu, DS - de specialitate, DC - complementară				**DS**
	Categoria de opţionalitate a disciplinei: DI - obligatorie (impusă), DO - opţională (la alegere), DL - facultativă (liber aleasă)				**DO**

3. Timpul total estimat (ore alocate activităţilor didactice)

3.1. Număr de ore pe săptămână	**3**	3.2. Curs	**2**	3.3. Seminar/Laborator/Proiect	**0/1/0**
3.4. Totalul de ore pe semestru din planul de învăţământ	**42**	3.5. Curs	**28**	3.6. Seminar/Laborator/Proiect	**14**

Distribuţia fondului de timp pe semestru:	ore
Studiul după manual, suport de curs, bibliografie şi notiţe	**10**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	**10**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	**10**
Tutoriat	**1**
Examinări	**2**
Alte activităţi (precizaţi):	

3.7. Total ore studiu individual	**33**
3.8. Total ore pe semestru	**75**
3.9. Numărul de credite	**3**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Noţiuni de bază în reţelistică
4.2. de competenţe	• Tehnologii Internet,-JAVA; Rețele de Calculatoare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Sala cu proiector, platforma http://cadredidactice.ub.ro, Platforma Teams, http://pruteanue.ub.ro,
5.2. de desfăşurare a seminarului/laboratorului/proiectului	• Laboratorul se desfăşoară într-o sală cu proiector si cu echipamente dedicate de reţelistică legate la internet. Teste pe platforma on-line alocate cursului, http://examene.pe.ub.ro, etc.

6. Competenţe specifice acumulate

6.1. Competenţe profesionale	C3.1. Identificarea unor clase de probleme şi metode de rezolvare caracteristice sistemelor informatice. Expunerea unor concepte fundamentale asupra securitatii informatice C4.3. Elaborarea specificaţiilor şi proiectarea unor sisteme informatice folosind metode şi instrumente specifice C5.3. Utilizarea unor principii şi metode de bază pentru asigurarea securităţii, siguranţei şi uşurinţei în exploatare a sistemelor hardware, software şi de comunicaţii. Utilizarea potentialului stiintific dobandit in activitatea practica cu specific informatic
Competenţe transversale	

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1. Obiectivul general al disciplinei	Asimilarea cunostintelor de baza din domeniul securitatii informatiilor si dezvoltarea abilitatilor de a analiza critic, a înțelege, a conceptele fundamentale si de a proiecta aplicații de securitatea informației (in anumite limite: domeniul este foarte vast si cursul de fata nu discuta decat o zona limitată a domeniului, in concordanta cu abordarea in multe universitati de prestigiu din lume).
7.2. Obiectivele specifice (vizează competențele asigurate de programul de studiu);	***Ob. de cunoaștere (OC):*** (1) Înțelegerea, cunoasterea si utilizarea adecvata a conceptului de criptografie și securitatea informatiei, a primitivelor și metodelor criptografice și a metodelor steganografice de baza(functionarea), avantajele si dezavantajele acestora. (3) Însușirea abilității de a analiza cerințele, riscurile si vulnerabilitatile unor sisteme informatice din punct de vedere al securitatii informatiei. (4) Intelegerea si capacitatea de analiza si proiectare a sistemelor de gestiune a securitatii informatiei in context organizational. ***Ob. de abilitare (Oab)/ Instrumental-aplicative:*** (1) Abilitatea de evaluare a vulnerabilităților, riscurilor și configurarea, monitorizarea, depanarea și implementarea măsurilor de securitate adecvate (2) Abilitatea de a proiecta, implementa și evalua un sitem se securitate (3) capacitate sporita de învatare intuitiva, bazata pe analogii, exemple diverse si similitudini; (4) capacitate sporita de învatare intuitiva, bazata pe analogii, similitudini și exemple diverse; ***Ob. de atitudinale (OAt):*** (1) punerea în aplicare a politicilor de securitate pentru a atenua riscurile. (2) Manifestarea unor atitudini pozitive si responsabile fata de domeniul stiintific si tehnic; (3) Valorificare optima si creativa a propriului potential în activitatile stiintifice si tehnice; (4) Implicarea în promovarea si dezvoltarea inovatiilor stiintifice si tehnice; (5) Participarea la propria dezvoltare profesionala si stiintifica.

8. Conţinuturi

	Curs	Nr. ore	Metode de predare	Observaţii
01.	Introducerea în cadrul general al protecţiei şi securitatea informației și în ***teoria controlului accesului***. Sisteme de gestiune a securitatii informatiei – concepte fundamentale și etape de proiectare	2	Prelegeri, discuţii asupra problemelor prezentate, Folosirea metodelor multimedia de predare si acces la Internet. Studentii sunt invitati sa colaboreze la proiectele de cercetare. Ore de consultatii in timpul	Facultativ: Securizarea comunicaţiilor pentru a asigura confidenţialitatea datelor. Punerea în aplicare celor trei AAA pe routere folosind bazele de date ale routerelor locale şi a celor bazate pe server ACS sau ISE. Explicarea ameninţărilor de securitate în cadrul infrastructurilor reţelelor moderne şi atenuarea acesetora. Implementarea
02	Controlul accesului: ***modele discretionare; modele mandatate; modelul bazat pe roluri.*** Politici, standarde, norme şi proceduri de securitate. Standardul de securitate a ISO 27001.	2		
03	Elemente de criptografie si criptanaliză. Tehnologii & sisteme criptografice (computationale). Criptografia clasica – cifruri simetrice de substitutie, de transpozitie, cifruri produs.	2		
04	***Criptografia cu chei simetrice*** *de tip stream si generatoare de numere aleatoare; Criptografia cu chei simetrice de tip bloc si modurile de operare a cifrurilor bloc; Criptografia cu chei asimetrice – cifruri asimetrice* ***Managementul cheilor***. Asigurarea securităţii SI publice şi private. - *Semnaturi digitale/*electronice si infrastructuri de securitate Cei 3 A: ”Authentication, Authorization and Accounting”	2		
05	***Functii de hashing.*** Ascunderea informatiei - steganografie si marcare digitala. Rolul numerelor aleatoare in securitatea informatiei			
06	***Extensii de securitate pentru DNS*** (DNSsec)	2		
07	***Extensii de securitate pentru IP***. Securitatea comerțului electronic și a sistemelor electronice de plati	2		
08	Protocolul SSL&TLS Expunere si demonstratii. Protocoalele S/MIME si PGP	2		
09	Smart carduri si sisteme biometrice Analiza și Managementul securitatii informatiilor și a riscurilor în Sistemele Informatice	2		
10	Securitatea in web, a bazelor de date, a codului sursa in programare, astemelor embeded și a sistemelor distribuite. Ingineria/Reingineria	2		

	sistemelor de securitate informatica		semestrului si inaintea examenului	securităţii în reţelele private virtuale. Testarea securităţii reţelelor şi crearea politicilor de securitate.
11	Implementarea sistemelor de prevenţie a intruziunilor (IDS). Securizarea LAN. Studiu de caz	2		
12	Implementarea VPN "Virtual Private Networks" Monitorizarea în mod sigur a reţelelor de comunicaţii şi de calculatoare. Studiu de caz	2		
13	Directii noi: securitatea calculului in cloud	2		
14	Standarde si reglementari. Auditarea si certificarea, aspecte juridice, legislatia privind protecţia şi securitatea sistemelor informatice. Criminalitatea informatica, colectarea si investigarea probelor.	2		

Bibliografie

[1] Cursuri si laboratoare: http://examene.pe.ub.ro/ ; http://cadredidactice.ub.ro/pruteanue/
[2] Cryptography: Theory and Practice, Douglas R. Stinson; CRC Press, ISBN 0-8493-8521-0.
[3] Information Warfare and Security, Dorothy E. Denning; ACM Press & Addison Wesley, ISBN 0-201-43303-6.
[4] Handbook of Applied Cryptography, Alfred J. Menezes, Paul C. van Oorschot and Scott A. Oprea, D. – Protecţia şi securitatea sistemelor informationale, Polirom, Iaşi, 2019
[5] Patriciu, V. – Securitatea şi protecţia informaţiilor în reţele de calculatoare, Ed. Didactică şi Pedagogică, Bucureşti,
[6] Criptografie si securitatea informatiei. Aplicatii. David Nacccache Emil Simion, Matrix Rom 2020 978-973-755-675-2
[7] Provocări si strategii de securitate cibernetică Ioan-Cosmin Mihai, Gabriel Petrică, Costel Ciuchi, Lauren?iu Giurea Editura Sitech 2015 978-606-11-4951-3
[8] Securitatea informatiilor. Ed.a II-a,Ioan-Cosmin Mihai, Gabriel Petrică Editura Sitech 2014 978-606-11-4364-1
[9] *Procedures for Detecting Cybercrime Activities on Websites Ioan-Cosmin Mihai Ed. Sitech 2017 978-606-11-6119-5*

Bibliografie minimală

[1] Popa Sorin Eugen – "Securitatea sistemelor informatice" – note de curs şi aplicaţii, Ed. Alma Mater Bacău, 2016;
[2] Cursuri si laboratoare: http://examene.pe.ub.ro/ ; http://cadredidactice.ub.ro/pruteanue/ Indrumar de Laborator
[3] HOWARD, M., LIPNER, S., The Security Development Lifecycle: SDL: A Process for Developing Demonstrably More Secure Software, Microsoft Press, 2018.
[4] SMITH, G.E., Control and Security of E-Commerce, John Wiley & Sons, New York, 2019.

Aplicaţii (Seminar / laborator / proiect)	**Nr. ore**	**Metode de predare**	**Observaţii**
[1] Introducere in teoria controlului accesului: modele discretionare; modele mandatate; modelul bazat pe roluri	2	Oral şi cu mijloace multimedia / platforme online • Stil de predare interactiv, • rezolvare de probleme • Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari • teste de evaluare si discutarea soluțiilor • Ex. implementare • teme de casă / miniproiecte	N/A
[2] Elemente de criptografie. Criptarea ca metoda de securitate a informatiilor. Algoritmi criptografici. Managementul cheilor. Steganografia ca metoda de securitate a iinformatiilor. Algoritmi criptografici clasici Algoritmi steganografici	2		N/A
[3] Firewall. Wireshark. Blockchain.Bitcoins	2		
[4] Hash Algoritmi MD5, SHA – asigurarea integrității unui mesaj. Certificate SSL JAVA. IDEA-International Data Encryption Algorithm	2		
[5] Extensii de securitate pentru DNS (DNSsec). Extensii de securitate pentru IP. Securitatea siteWeb, captcha, rewrite module .htacces. Expresii regulate.	2		
[6] Protocoale de securitate, HTTPS, SSL (Secure Socket Layer) &TLS; Protocoalele S/MIME si PGP	2		
[7] Sec retelei prin V.P.N., Open VPN, tunelare. (B) Directii noi: securitatea calculului in cloud. Prezentarea si discutarea proiectelor asignate	2		

Bibliografie minimală

La fel ca la curs

Bibliografie suplimentară

[1] Cursuri si laboratoare: http://examene.pe.ub.ro/ ; http://cadredidactice.ub.ro/pruteanue/
[2] OPREA, D., Protectia şi securitatea informaţiilor, POLIROM, 2018.
[3] SLADE, R., Dictionary of Information Security, Syngress Publishing, 2016.
[4] WALKER, A., Absolute Beginner's Guide To: Security, Spam, Spyware & Viruses, QUE, 2019.
[5] WEBER R., Information Systems Control and Audit, Prentice Hall, New Jersey, 2020

Resurse Internet
www.squid-cache.org http://www.wingate.com/download.php; http://www.youngzsoft.net/ccproxy/ www.digimarc-id.com www.aris-techni.fr/ www.infowar.com, www.itpapers.com, www computer.org, www.information week.com, www.intelligenterprise.com, www.technologyevaluation.com, www.verisign.com, www.infoworld.com http://infosecuritymag.techtarget.com, www.scmagazine.com; www.issa.org, http://secinf.net

Analiza sistemelor de gestiune a securitatii informatiei in context organizational – studii de caz (analiza vulnerabilitatilor, metode de gestiune a riscurilor, etc.). Prezentarea aplicaţiei ce trebuie realizată (Implementarea algoritmului): "Reverse Chiper"; algoritmul lui Cezar; ADFGVX; PlayFair; Vigenere; "Homophonic"; Implementarea criptării/decriptării: RSA, Enigma,DES. Implementarea Triple DES clasic, algoritmului MD5; algoritmului SHA-1, AES.

9. Coroborarea conţinuturilor disciplinei cu aşteptările reprezentanţilor comunităţii epistemice, asociaţiilor profesionale şi angajatori reprezentativi din domeniul aferent programului

Se asigură competenţe conform prevederilor RNCIS. Se realizeaza prin discutii periodice cu reprezentantii angajatorilor si prin abordarea tehnologiilor de actualitate utilizate in cadrul companiilor IT.

- Conținutul cursului și al laboratorului, prin problematica tratată, pune la dispoziția studentului cunoștințe conforme cu așteptările reprezentanților comunității epistemice și angajatorilor reprezentativi din domeniul calculatoarelor și tehnologiei informației. Tematica abordată și cursuri asemanatoare din comunitatea academica si industr se regăsește la universități de renume, cum ar fi:

Compatibilitate națională:

- Universitatea "Alexandru Ioan Cuza" din Iași, Facultatea de Informatică, " Securitatea Informatiei" https://profs.info.uaic.ro/~webdata/planuri/2019/licenta/ro/CS3102.pdf
- Universitatea de Vest din Timișoara, Matematică și Informatică, " Criptografie și Securitatea Informației" https://www.info.uvt.ro/others/fise_disciplina/securitate_cibernetica/CriptografieSiSecuritateaInformatiei_sc.pdf
- Universitatea „Ștefan cel Mare" Suceava, Facultatea Inginerie Electrică şi Ştiinţa Calculatoarelor, "Criptografie Și Securitate Informaţionala", https://fiesc.usv.ro/wp-content/uploads/sites/17/2021/01/17.USV_.FIESC_.C.DS_.08.17-CSI-CERLINCA-M.pdf

Compatibilitate internațională:

- CS255: Introduction to Cryptography, http://crypto.stanford.edu/~dabo/cs255/
- Cryptography and Cryptanalysis, http://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-875-cryptography-andcryptanalysis-spring-2005/
- Cryptographer and Entrepreneur, http://saweis.net/crypto.html
- Applied Cryptography, http://courses.engr.illinois.edu/cs598man/fa2009/
- CSE 107 Introduction to Modern Cryptography, http://cseweb.ucsd.edu/users/mihir/cse107/
- CSE 207 Modern Cryptography, http://cseweb.ucsd.edu/~mihir/cse207/
- practical cryptographic systems. http://spar.isi.jhu.edu/~mgreen/650.445/650.445__Main.html
- CS 276 Cryptography, http://www.cs.berkeley.edu/~daw/teaching/cs276-s06/

10. Evaluare

Tip activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Abilitatea de a conceptualiza, sintetiza si analiza problemele specifice domeniului CSI prin cunoasterea și expunerea clară a conceptelor teoretice si a rezultatelor din domeniu cu aplicare în practică..	metoda de ***evaluare sumativa*** (prin ex– Test grila (TG) de cunoştinţe teoretice	**70%**
10.5. Seminar/laborator /proiect	Calitatea judecăţilor formate, gândirea logică, flexibilitatea – capacitatea de a utiliza diferite tehnici de criptare și tehnologii de securitate. Prezența activă la laborator, răspunsuri la întrebări, portofoliu, prezentarea unor referate/miniproiect elaborate pe parcursul semestrului sau proiectarea, dezvoltarea și realizarea unei aplicații din domeniu, cu îndeplinirea obiectivelor asumate	***Evaluare formativa*** pe parcursul lab. (**AL**). ***Evaluare sumativa*** – prin probă practică. Proiect (**PL**)–Test final	**10%AL+ 20%PL**

10.6. Standard minim de performanţă

Cunoasterea conceptelor de baza din domeniu:

- media finală la examen se calculează numai în situația în care nota obtinută la proba teoretică şi nota obţinută la proba practică (conform baremurilor specificate) sunt de minim 5.
- activitate minimă in timpul laboratorului - prezența minima la 6/(12) şedinţe de laborator. Media laboratoarelor - minim 5, iar studentul care nu promoveaza aceasta activitate nu se poate prezenta la examen in sesiunea normala.
- cel putin o interventie la aplicatiile care se fac in timpul laboratoarelor;

- sa dovedeasca insusirea minima a materiei parcurse (notiuni de baza) și că noţiunile prezentate nu sunt însuşite mecanic. Insuşirea principalelor noţiuni, principii, teorii, abordări din domeniul
- predarea proiectului cotat cu minim 5 (indeplinirea cerințelor minimale).
- Examen/Colocviu final practic, insotit de intrebari teoretice si sustinerea miniproiectului - nota minima: 5 (deci este necesar ca fiecare din cele 3 note să fie cel puţin 4.5).

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
18.09.2020	Șef lucrări dr. ing. Pruteanu Eusebiu	Drd. Ing. Ungureanu Andrei Gabriel

Data avizării în departament	Semnătura directorului de departament
23.09.2021	Prof. univ. dr. ing. George CULEA

Data aprobării în Consiliul Facultăţii	Semnătura decanului
27.09.2021	Conf. univ dr. ing. Mirela PANAINTE-LEHĂDUȘ