FIŞA DISCIPLINEI
ANUL UNIVERSITAR 2023 - 2024

1. DATE DESPRE PROGRAM

1.1 Instituţia de învăţământ superior	*UNIVERSITATEA DIN CRAIOVA*
1.2 Facultatea	*Facultatea de Automatică, Calculatoare şi Electronică*
1.3 Departamentul	*Departamentul de Automatică şi Electronică*
1.4 Domeniul de studii	*Ingineria sistemelor*
1.5 Ciclul de studii[1]	*Licenţă*
1.6 Programul de studii (denumire/cod)[2] /Calificarea	*Ingineria sistemelor multimedia /*

2. DATE DESPRE DISCIPLINĂ

2.1 Denumirea disciplinei				**Tehnici de securizare a informaţiei**					
2.2 Titularul activităţilor de curs				Prof. dr. ing. Dorin ŞENDRESCU					
2.3 Titularul activităţilor aplicative				Asist. drd. ing. Oana CIUCĂ					
2.4 Anul de studiu	4	2.5 Semestrul	8	2.6 Tipul disciplinei (conţinut)[3]	**DS**	2.7 Regimul disciplinei (obligativitate)[4]	**DO**	2.8 Tipul de evaluare	**E**

3. TIMPUL TOTAL ESTIMAT (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	3	din care: 3.2 curs	2	3.3 laborator	1
3.4 Total ore din planul de învăţământ	30	din care: 3.5 curs	20	3.6 laborator	10
3.7 Distribuţia fondului de timp					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					-
▪ Examinări					5
▪ Alte activităţi: consultaţii, cercuri studenţești					10

Total ore activităţi individuale	45
3.8 Total ore pe semestru[5]	75
3.9 Numărul de credite[6]	3

4. PRECONDIŢII (acolo unde este cazul)

4.1 de curriculum	Studentul trebuie să posede cunoştinţe de specialitate dobândite la următoarele discipline: Programarea calculatoarelor şi limbaje de programare, Algebră liniară, geometrie analitică şi diferenţială, Procesare de documente.
4.2 de competenţe	Nu sunt necesare.

5. CONDIŢII (acolo unde este cazul)

5.1. de desfăşurare a cursului	Predarea cursului se face folosind videoproiectorul. Pentru unele explicaţii şi răspunsuri la întrebari din sală se foloseşte tabla. Se asigură suport de curs în format electronic şi acces la documetaţii actualizate. Procesul de predare are următoarea structură: ▪ 80% prezentare teoretică, pe baza suportului de curs (slide-uri) ▪ 20% activitate interactivă (discuţii cu studenţii)
5.2. de desfăşurare a seminarului/ laboratorului/proiectului	Laboratorul utilizează o reţea de calculatoare. Sunt implementați algoritmii de securizare a informaţiei și configurate și testate soft-urile de protejare a calculatoarelor (antivirus și firewall).

6. COMPETENŢELE SPECIFICE ACUMULATE [7]

Competenţe profesionale	Prin cunoştinţele predate la curs, prin exemplele prezentate şi prin aplicaţiile practice efectuate în cadrul laboratorului, cursul „Tehnici de securizare și criptare" contribuie la formarea competenţelor profesionale: ▪ **C5:** Proiectarea şi administrarea reţelelor de calculatoare, a sistemelor de comunicaţie şi a sistemelor multimedia în condiţii de asigurare a calităţii şi securităţii sistemelor informatice.
Competenţe transversale	▪

7. OBIECTIVELE DISCIPLINEI (reieşind din grila competenţelor specifice acumulate)

7.1 Obiectivul general al disciplinei	Contribuie la formarea viitorilor ingineri din domeniul sistemelor multimedia, asigurându-le cunoştinţe în domeniul securizării informaţiei. Sunt abordate concepte de bază utilizate în proiectarea și realizarea sistemelor de securizare a datelor.
7.2 Obiectivele specifice	Introducere în teoria securizării informaţiei, tehnici de protecție a datelor: parole, criptare cu cheie simetrică și cu cheie publică, semnături digitale, configurare programe antivirus și firewall. Laboratorul are rolul de a fixa cunoștințele teoretice și de a permite înțelegerea mecanismelor de protecție a datelor prin aplicaţii practice.

8. CONŢINUTURI

8.1 Curs (unităţi de conţinut)	Nr. ore	Metode de predare
1. Generalităti 1.1. Probleme generale privind protecţia şi securitatea datelor. 1.2. Fixarea terminologiei; Tratarea specificităţii securităţii în context Internet.	2	Predarea cursului se face folosind videoproiectorul. - 80% prezentare teoretică, pe baza suportului de curs (slide-uri). - 20% activitate interactivă (discuţii cu studenţii) Materialele necesare vor fi puse la dispozitia studenţilor în format electronic şi în formă tipărită.
2. Concepte şi modele aritmetico-logice utilizate în tehnicile criptografice 2.1. Operaţii booleene; 2.2. Elemente de teoria numerelor; 2.3. Aritmetică modulară.	2	
3. Criptografie cu cheie secretă. Detalierea tehnicilor de criptografie simetrică. 3.1. DES (Data Encription Standard); 3.2. Algoritmi de substituţie; 3.3. Tehnica one-time-pad.	2	
4. Criptografie cu chei publice. 4.1. Descrierea metodei RSA (Rivest-Shamir-Aldeman) 4.2. Descrierea metodei ElGamal; 4.3. Descrierea metodei Rabin	2	
5. Funcţii de dispersie (hash) utilizate în criprografie 5.1. Descrierea metodei MD5 (Message Digest) 5.2. Descrierea metodei SHA (Secure Hash Alghorithm).	2	
6. Semnături digitale. 6.1. Domenii de utilizare; 6.2. Algoritmi de criptare utilizaţi în semnătura digitală.	2	
7. Protocoale de autentificare 7.1. Protocolul Diffie-Helman; 7.2. Notari electronici; 7.3. Sisteme de încredere 7.4. Protocolul şi sistemul Kerberos	2	
8. Securitate în cadrul protocolului TCP/IP. 8.1. Structura unui firewall. 8.2. Funcţiile unui firewall	2	

9. Protocoale la nivel de aplicaţie şi aplicaţii securizate. 9.1. Protocolul SSH; 9.2. Protocolul SFTP; 9.3. Protocolul HTTPS 9.4. Protocolul SSL.	2	
10. Viruşi informatici 10.1. Anatomie; 10.2. Clasificări; 10.3. Funcţionalităţi; 10.4. Protecţia antivirus	2	
Total	**20 ore**	

Bibliografie [8]

1. W Stallings, Cryptography and Network Security, second ed., Prentice-Hall, 1999
2. Cormen T. Leiserson C. Rivest R introducere în algoritmi. Computer press Agora, 1999.
3. Jursic A. Menezes A. Elliptic curves and Cryptography http://www.certicom.com/research/ weccrypt.html WhitePaper
4. Patriciu V. Criptografie şi securitatea reţelelor de calculatoare. Ed. Tehnică, 1994
5. *** Resurse Web plecând de la . (http://WilliamStallings.com/Security2e.html).
6. Ciprian Răcuciu, Aspecte privind secretizarea semnalelor video, A XXVI-a Sesiune de Comunicări Ştiinţifice cu Participare Internaţională, Ed. Academia Tehnică Militară, Bucureşti, 1995.
7. Ciprian Răcuciu, Consideraţii asupra algoritmilor de criptanaliză statistică, A XXX-a Sesiune de Comunicări Ştiinţifice cu Participare Internaţională, Ed. Academia Tehnică Militară, Bucureşti, 2003.
8. Sendrescu Dorin, Tehnici de securizare a informației – Notițe de curs (format electronic), nr. pag 180, adresa web: www.automation.ucv.ro/TSI

8.2 Activităţi aplicative (subiecte/teme)	Nr. ore	Metode de predare
Prezentarea noţiunilor de aritmetică modulară	2	Efectuarea lucrărilor de laborator se face folosind machete și programe de simulare pe calculator. Sunt puse la dispoziția studenților platforme de laborator care conțin un breviar teoretic și modul de desfășurare al lucrării. Activități: ▪ 60% desfășurarea lucrării ▪ 40% interpretarea rezultatelor și discuții cu studenții
Implementarea algoritmilor cu cheie secretă	2	
Implementarea algoritmilor cu cheie publică	2	
Studierea și configurarea unui firewall	2	
Implementarea unui protocol de securitate	2	
Total	**10 ore**	

Bibliografie [8]

1. Held G. - Comunicaţii de date, Editura Teora, Bucureşti, 1998.
2. V. Patriciu, Criptografia şi Securitatea Reţelelor de Calculatoare cu aplicaţii în C şi Pascal, Ed. Tehnică, Bucureşti, 1994.
3. H. Beker and F. Piper, Cipher Systems: The Protection of Communications, John Wiley & Sons, New York, 1982.
4. Bruce Schneier, Applied Cryptography, John Wiley & Sons, 1996.
5. Boca Raton, Cryptography: Theory and Practice, CRC Press, , Florida, 1995.
6. Sendrescu Dorin, Tehnici de securizare a informației – Notițe de curs (format electronic), nr. pag 180, adresa web: www.automation.ucv.ro/TSI

9. COROBORAREA CONŢINUTURILOR DISCIPLINEI CU AŞTEPTĂRILE REPREZENTANŢILOR COMUNITĂŢII EPISTEMICE, ASOCIAŢIILOR PROFESIONALE ŞI ANGAJATORI REPREZENTATIVI DIN DOMENIUL AFERENT PROGRAMULUI

Conținutul cursului a fost discutat cu reprezentanții:

- CS Romania
- Net Rom
- IT Six Global Services

10. EVALUARE

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	- Înțelegerea fundamentelor teoretice corespunzătoare securității informatice. - Capacitatea de a realiza conexiuni între noțiunile predate. - Capacitatea de analiză și sinteză într-o situație concretă.	Examen scris parţial Examen scris final	30% 40%
10.5 Activități aplicative Laborator	- Interpretarea rezultatelor; - Soluţiile aplicaţiilor se prezintă şi se discută în cadrul grupei	Verificare pe parcurs şi testare finală	30%
10.6 Standard minim de performanță (volumul de cunoștințe minim necesar pentru promovarea disciplinei și modul în care se verifică stăpânirea lui)			
▪ Obţinerea a minim 50 % din punctajul verificărilor pe parcurs, testărilor de laborator şi examenului final. ▪ Calculul notei finale se face prin rotunjirea la notă întreagă a punctajului final.			

Data completării: 25.09.2023

Titular curs
Prof. dr. ing. Dorin Șendrescu

Titular activități aplicative
Asist. drd. ing. Oana Ciucă

.....

.....

Data avizării în departament: 27.09.2023

Director de departament
Prof. dr. ing. Cosmin IONETE

.....

Notă:

1) Ciclul de studii - se alege una din variantele: L (licenţă)/ M (master)/ D (doctorat).
2) Se înscrie codul prevăzut în HG nr. 493/17.07.2013.
3) Tip (conţinut) - se alege una din variantele:
   - pentru nivelul de licenţă: DF (disciplină fundamentală)/ DD (disciplină din domeniu)/ DS (disciplină de specialitate)/ DC (disciplină complementară);
   - pentru nivelul de master: DA (disciplină de aprofundare)/ DS (disciplină de sinteză)/ DCA (disciplină de cunoaştere avansată).
4) Regimul disciplinei (obligativitate) - se alege una din variantele: DI (disciplină obligatorie)/ DO (disciplină opţională)/ FC (disciplină facultativă).
5) Se obține prin însumarea numărului de ore de la punctele 3.4 și 3.7.
6) Un credit este echivalent cu 25 – 30 de ore de studiu (activităţi didactice şi studiu individual).
   În cazul DAEM 1 pct. credit este egal cu 27 de ore de studiu.
7) Aspectul competenţelor profesionale şi competenţelor transversale va fi tratat cf. Metodologiei OMECTS 5703/18.12.2011. Se vor prelua competenţele care sunt precizate în Registrul Naţional al Calificărilor din Învăţământul Superior RNCIS (http://www.rncis.ro/portal/page?_pageid=117,70218&_dad=portal&_schema=PORTAL) pentru domeniul de studiu de la pct. 1.4 şi programul de studii de la pct. 1.6 din această fişă, la care participă disciplina.
8) Se recomandă ca cel puţin un titlu să aparţină colectivului disciplinei iar cel puţin 2-3 titluri să se refere la lucrări relevante pentru disciplină, de circulaţie naţională şi internaţională, existente în biblioteca UCv.