FIȘA DISCIPLINEI
ANUL UNIVERSITAR 2025 – 2026

1. Date despre program

1.1. Instituția de învățământ superior	*UNIVERSITATEA DIN CRAIOVA*
1.2. Facultatea	*Automatică, Calculatoare și Electronică*
1.3. Departamentul	*Calculatoare și Tehnologia Informației*
1.4. Domeniul de studii	Calculatoare și Tehnologia Informației
1.5. Ciclul de studii universitare	Licență
1.6. Forma de organizare	IF
1.7. Programul de studii	Calculatoare / L2060101010

2. Date despre disciplină

2.1. Denumirea disciplinei			**Securitatea datelor**				
2.2. Titularul activităților de curs			Prof. univ. dr. ing. Marius MARIAN				
2.3. Titularul activităților de seminar/ laborator			Asist. univ. drd. ing. Claudiu TRĂISTARU				
2.4. Anul de studiu	4	2.5. Semestrul	1	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	DOB

3. Timpul total estimat (ore pe semestru a activităților didactice)

3.1. Numărul de ore pe săptămână	4	din care: 3.2 curs	2	3.3. sem.	2
3.4. Total ore din planul de învățământ	56	din care: 3.5 curs	28	3.6. sem.	28
Distribuția fondului de timp - ore/săpt.					
Studiul după manual, suport de curs, bibliografie și notițe					10
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					6
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					10
Tutorat					-
Examinări					14
Alte activități: consultații					4
3.7. Total ore studiu individual					**44**
3.8. Total ore pe semestru					**100**
3.9. Numărul de credite					**4**

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Studentul trebuie să posede cunoștințe fundamentale și de specialitate dobândite la următoarele discipline: Algebră liniară și geometrie, Matematici speciale, Metode numerice, Programarea calculatoarelor, Tehnici de programare, Bazele proiectării logice a calculatoarelor, Structuri de date și algoritmi, Sisteme de operare, Comunicații de date, Structura și organizarea calculatoarelor, Baze de date, Programare orientată pe obiecte, Arhitectura calculatoarelor, Proiectarea sistemelor cu microprocesoare, Rețele de calculatoare, Dezvoltarea aplicațiilor distribuite în rețea, Verificarea și testarea sistemelor de calcul, Ingineria programării.
4.2. de competențe	Studentul este în câștig dacă posedă deja competențele din lista de mai jos (însă studiul disciplinei în lipsa acestor competențe nu este penalizant):

	• Operarea cu fundamente științifice, inginerești și ale informaticii; • Comportarea onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputația profesiei; • Demonstrarea spiritului de inițiativă și acțiune pentru actualizarea cunoștințelor profesionale, economice și de cultură organizațională.

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	Predarea cursului se face folosind calculatorul, rețeaua Internet și videoproiectorul. Pentru unele explicații mai detaliate ale conceptelor ilustrate în diapozitivele suport de curs și pentru a răspunde întrebărilor adresate de studenții din sală se folosește tabla. Studenților li se recomandă să exerseze luarea notițelor (în scris, pe caiete de tip matematică). Se asigură suport de curs în format electronic și acces la documentații actualizate. Procesul de predare are următoarea structură: • 70% prezentare teoretică, pe baza suportului de curs (diapozitive); • 30% activitate interactivă (demonstrații practice și dialog cu studenții). Strategii de transmitere și însușire a cunoștințelor utilizate: expunerea, interogarea, deducția, testarea, evaluarea continuă și sumativă. OBS: cursul poate îmbină mai multe metode de predare: clasic, online (în funcție de decizia Senatului universității și Consiliului facultății), cu videoproiector.
5.2. de desfășurare a seminarului/ laboratorului	Sunt prezentate exemple și sunt rezolvate diverse exerciții și probleme pe baza noțiunilor teoretice prezentate la curs, clasic și cu utilizarea unor medii de programare și simulare specifice. La seminar și laborator se utilizează tabla pentru exemplificarea algoritmilor și a diferitelor tehnici de programare studiate, plus o rețea de calculatoare. Acestea sunt folosite împreună cu medii de programare integrate pentru exemplificarea conceptelor prezentate la curs, precum și pentru rezolvarea unor tipuri de probleme propuse studenților la laborator. Studenții vor fi expuși și se va stimula experimentarea mai multor tehnici și librării criptografice de uz comun. Studenții vor fi implicați în exerciții practice de manipulare a algoritmilor criptografici și a mecanismelor de securitate predate. Notițele și caietele de curs sunt obligatorii la curs, seminar și laborator, studenților urmărindu-li-se strategia de abordare și de rezolvare practică a problemelor propuse.

6. Obiectivele disciplinei - rezultate așteptate ale învățării la formarea cărora contribuie parcurgerea și promovarea disciplinei

Cunoștințe	Studentul/absolventul identifică și explică conceptele, teoriile și metodele de bază ale domeniului securității datelor.

Aptitudini (Abilități)	Studentul/absolventul selectează și aplică criterii, principii și metode de evaluare pentru identificarea, modelarea, simularea și experimentarea fenomenelor și proceselor din domeniul securității datelor.
Responsabilitate și autonomie	Studentul/absolventul 1. selectează și analizează sursele bibliografice specifice domeniului. 2. demonstrează autonomie în învățare pe problematici specifice domeniului.

7. Conținuturi

7.1. Curs	Modalitatea de desfășurare	Metode de predare	Fond de timp alocat (ore)
Curs 1. Introducere în securitatea informației • noțiuni de bază; cripto-sisteme clasice; amenințări, atacuri și informații critice; cerințe funcționale de securitate; strategii de securitate a informației.	Online sincron	Predarea cursului se face folosind video-proiectorul. Exemplificarea practică a conceptelor prezentate și rezolvarea problemelor se face direct în mediul vizual de prezentare / programare / etc. Cursul este structurat în raportul de mai jos: 1. 80% prezentare teoretică, pe baza suportului de curs (diapozitive); 2. 20% activitate interactivă (dialog cu studenții) Materialele necesare vor fi puse la dispoziția studenților în format electronic și în format tipărit. Ca strategii de transmitere și însușire a cunoștințelor se utilizează: Expunerea; Interogarea; Deducția; Testarea; Evaluarea finală.	2
Curs 2. Instrumente criptografice • criptarea simetrică; criptarea cu cheie publică; semnătură digitală și gestiunea cheilor; generarea numerelor pseudo-aleatoare.	Online sincron		2
Curs 3. Mecanisme de autentificare a utilizatorilor • principiile de autentificare; autentificare prin parolă; autentificare pe bază de token; autentificare biometrică.	Online sincron		2
Curs 4. Mecanisme de control al accesului • principii de control al accesului; subiecte, obiecte și drepturi de acces; controlul discreționar; controlul bazat pe roluri.	Online sincron		2
Curs 5. Securitatea bazelor de date • controlul accesului la o bază de date; inferența; baze de date statistice; criptarea bazelor de date	Online sincron		2
Curs 6. Detecția intruziunilor • identificarea intrușilor; detecția intrușilor în sisteme de calcul individuale; detecția intrușilor în sisteme de calcul distribuite; detecția intrușilor în rețele de calculatoare; detecția adaptativă a intrușilor în sisteme distribuite; mecanism de pândă de tip „borcan cu miere” (honeypots) sau „rețea cu miere” (honeynet)	Online sincron		2
Curs7. Software malign • tipuri de software malign; viruși informatici; măsuri contra virușilor informatici; viermi informatici; bots (roboți); rootkits	Față în față (cu prezență fizică)		2
Curs8. Denial of service (Negarea utilizării serviciilor) • atacuri de tip denial of service (DoS); atacuri de tip flooding (inundație); atacuri de tip	Față în față (cu prezență fizică)		2

denial of service distribuit; atacuri de tip reflector și de tip amplificator; contramăsuri posibile la atacuri DoS			
Curs 9. Sisteme firewall și de prevenire a intruziunilor • necesitatea „zidurilor ignifuge” (firewall); tipuri de firewall-uri; arhitecturi de rețele și locația firewall-urilor; sisteme de prevenire a intruziunilor	Față în față (cu prezență fizică)		2
Curs 10. Securitatea multi-nivel; modele de încredere • modelul Bell-LaPadula; alte modele formale de securitatea sistemelor; conceptul unui sistem de încredere; aplicarea securității multi-nivel; criteriile comune pentru evaluarea securității IT	Față în față (cu prezență fizică)		2
Curs 11. Buffer overflow • atacuri de tip stack overflow; contramăsuri de protecție; alte atacuri de tip overflow; scriere de cod sigur din punct de vedere al securității	Față în față (cu prezență fizică)		2
Curs 12. Chestiuni de securitate fizică și infrastructurală • amenințări contra securității fizice a sistemelor; prevenirea și contramăsuri la atacurile fizice asupra sistemelor; recuperarea sistemelor după un atac fizic; identificarea amenințărilor; planificarea și implementarea contramăsurilor; integrarea securității fizice a sistemelor cu cea logică	Față în față (cu prezență fizică)		2
Curs 13. Gestiunea securității IT și identificarea riscurilor • gestiunea securității IT; contextul organizațional și politicile de securitate; identificarea riscurilor la adresa securității sistemului; analiza riscurilor	Față în față (cu prezență fizică)		2
Curs 14. Aspecte legale și etice • criminalistică informațională; proprietatea intelectuală; confidențialitate și privacy; chestiuni de etică	Față în față (cu prezență fizică)		2
Bibliografie:			
1. W. Stallings, L. Brown, “Computer Security: Principles and Practice”, Prentice-Hall, 2008, ISBN-13: 9780136004240 2. W. Stallings, “Network Security Essentials: Applications and Standards”, Prentice-Hall, 2007, ISBN-13: 9780132380331 3. B. Schneier, “Applied Cryptography: Protocols, Algorithms and Source Code in C”, Wiley, 1996, ISBN-13: 978-0471117094			

7.3. Laborator	Modalitatea de desfășurare	Metode de predare	Fond de timp alocat (ore)
Lab. 1: inițiere în utilizarea librăriei criptografice OpenSSL	Online sincron	Sunt prezentate exemple și sunt rezolvate diverse exerciții și probleme pe baza noțiunilor teoretice prezentate la curs.	2
Lab. 2: utilizarea criptografiei simetrice (DES, 3DES, AES)	Online sincron		2
Lab. 3: utilizarea criptografiei asimetrice (RSA)	Online sincron		2
Lab. 4: utilizarea semnăturii digitale	Față în față (cu prezență fizică)		2

Lab. 5: familiarizarea cu algoritmii de determinare a valorii rezumat și cei de semnătură digitală (MD5, SHA1, DSA, DH)	Față în față (cu prezență fizică)	Studentul este încurajat să își asume responsabilități în direcția analizei problemei și a soluționării algoritmice/software pentru aceasta.	2
Lab. 6 : implementarea și utilizarea unei aplicații folosind liste de control al accesului (ACL)	Față în față (cu prezență fizică)		2
Lab. 7: implementarea unei arhitecturi client-server securizate pe partea de comunicație	Față în față (cu prezență fizică)		2
Lab. 8: instalare, configurare și familiarizare cu utilitarul SNORT (sistem de detecție a intruziunilor)	Față în față (cu prezență fizică)		2
Lab. 9: exemplificare de viruși informatici și folosirea anti-virușilor	Față în față (cu prezență fizică)		2
Lab. 10: instalare, configurare și familiarizare cu un utilitar de tip firewall	Față în față (cu prezență fizică)		2
Lab. 11: instalare, configurare și familiarizare cu un utilitar de tip IDS/IPS	Față în față (cu prezență fizică)		2
Lab. 12: aplicații vulnerabile la atacuri de tip buffer overflow	Față în față (cu prezență fizică)		2
Lab. 13: familiarizarea cu o infrastructură cu cheie publică (certificate digitale, autorități de certificare, autorități de înregistrare)	Față în față (cu prezență fizică)		2
Lab. 14 : familiarizarea cu serviciile unei infrastructuri cu cheie publică (PKI)	Față în față (cu prezență fizică)		2

Bibliografie:

1. W. Stallings, L. Brown, "Computer Security: Principles and Practice", Prentice-Hall, 2008, ISBN-13: 9780136004240
2. W. Stallings, "Network Security Essentials: Applications and Standards", Prentice-Hall, 2007, ISBN-13: 9780132380331
3. B. Schneier, "Applied Cryptography: Protocols, Algorithms and Source Code in C", Wiley, 1996, ISBN-13: 978-0471117094

8. Coroborarea conținuturilor disciplinei cu așteptările reprezentanților comunității epistemice, asociațiilor profesionale și angajatori reprezentativi din domeniul aferent programului

Conținutul cursului a fost discutat cu reprezentanții:

- C-S România SA
- Forvia-Hella Craiova
- Netrom Software Craiova

9. Evaluare

Tip activitate	9.1. Criterii de evaluare	9.2. Metode de evaluare	9.3. Pondere din nota finală
9.1. Curs	▪ Înțelegerea fundamentelor teoretice corespunzătoare securității calculatoarelor; ▪ Capacitatea de a rezolva cele mai des întâlnite clase de probleme de securitate cu ajutorul tehnologiilor existente; ▪ Capacitatea de a realiza conexiuni între noțiunile predate; ▪ Capacitatea de analiză și sinteză într-un	Examen: probă scrisă. Asistență examen: 2 examinatori interni. Condiția de participare la examen: efectuarea tuturor lucrărilor de laborator și rezolvarea tuturor temelor de casă. Examenul se susține în sala repartizată de decanat, iar testul de laborator se desfășoară, în principiu, în ultima săptămână a semestrului.	70 – 90% (se corelează cu nota de laborator)

	scenariu concret de securitate.		
9.2. Laborator	Laborator: ▪ Capacitatea de analiză, identificare soluție optimă și rezolvare a problemelor propuse; ▪ Rezolvarea corectă a temelor de casă propuse; ▪ Identificarea corectă a principiilor precum și aplicarea de soluții optime; ▪ Soluțiile aplicațiilor se prezintă și se discută în cadrul grupei.	Evaluare pe parcurs a performanței individuale a studentului și rezolvarea tuturor temelor de casă de către acesta.	30 – 10% (se corelează cu nota de la examen)
9.4. Standard minim de performanță: ▪ Obținerea a minimum 50 % din punctajul verificărilor pe parcurs, testărilor la seminar și verificării finale. ▪ Calculul notei finale se face prin rotunjirea la notă întreagă a punctajului final.			

Data completării
29.09.2025

Titular de disciplină,

Prof. univ. dr. ing. Marius MARIAN

Semnătura titularului

Data avizării în departament
30.09.2025

Director de departament,
Ș.l. dr. ing. Nicolae ENESCU

Semnătura directorului de departament,

Decan,
Prof. dr. ing. Dorin ȘENDRESCU

Semnătura decanului