R O M Â N I A
MINISTERUL EDUCAŢIEI ŞI CERCETĂRII
UNIVERSITATEA DIN CRAIOVA

ŞCOALA DOCTORALĂ „CONSTANTIN BELEA”
DOMENIUL: CALCULATOARE ŞI TEHNOLOGIA INFORMAŢIEI
FACULTATEA DE AUTOMATICĂ, CALCULATOARE ŞI ELECTRONICĂ
Craiova, Blvd. Decebal nr. 107, RO-200440, http://www.ace.ucv.ro/

FIŞA DISCIPLINEI
ANUL UNIVERSITAR 2025-2026

1. Date despre program

1.1. IOSUD – Instituția de învățământ superior	*IOSUD – Universitatea din Craiova*
1.2. Școala Doctorală	*Școala Doctorală „Constantin Belea” a Facultății de Automatică, Calculatoare și Electronică*
1.3. Domeniul de studii universitare de doctorat	*Calculatoare şi tehnologia informaţiei*
1.4. Ciclul de studii universitare	*Doctorat*

2. Date despre disciplină

2.1. Denumirea disciplinei			**Securitatea calculatoarelor**				
2.2. Titularul activităților de curs			Prof. dr. ing. Marius MARIAN				
2.3. Titularul activităților de seminar/ laborator			Prof. dr. ing. Marius MARIAN				
2.4. Anul de studiu	1	2.5. Semestrul	1	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	DOP

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

3.1. Numărul de ore pe săptămână	3	din care: 3.2 curs	2	3.3. seminar	1
3.4. Total ore din planul de învățământ	**42**	din care: 3.5 curs	28	3.6. laborator	14
Distribuția fondului de timp - ore/săpt.					
Studiul după manual, suport de curs, bibliografie și notițe					42
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					28
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					28
Tutorat					-
Examinări					3
Alte activități: consultații					7
3.7. Total ore studiu individual					**108**
3.8. Total ore pe semestru					**150**
3.9. Numărul de credite					**6**

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	Studenții doctoranzi 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	Studenții doctoranzi sunt în câștig dacă posedă competențe din lista de mai jos: • cunoașterea și utilizarea conceptelor avansate din domeniul Calculatoarelor și Tehnologiei Informației, inclusiv privind proiectarea, implementarea și testarea sistemelor de calcul moderne, precum și capacitatea de a opera cu aceste concepte. • cunoștințe privind gândirea critică, inclusiv aptitudinea de a analiza, interpreta sau formula raționamente în diferite contexte; • înțelegerea și capacitatea de aplicare a principiilor și valorilor eticii cercetării științifice în domeniul Calculatoare și Tehnologia Informației, inclusiv a aspectelor legate de utilizarea și interpretarea rezultatelor furnizate de instrumentele de inteligență artificială. • capacitatea de identificare, formulare și soluționare într-o manieră creativă a problemelor de cercetare în domeniul Calculatoare și Tehnologia Inform; • stăpânirea metodelor și tehnicilor de cercetare în domeniul Calculatoare și Tehnologia Informației, precum și a procedeelor și soluțiilor noi în cercetare; • dobândirea de abilități de documentare și valorificare a lucrărilor științifice.

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. În cadrul activităților de seminar 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 seminar.

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

Cunoştinţe	Studentul-doctorand/absolventul: • Studentul-doctorand/absolventul analizează și corelează principiile securității cibernetice, tehnologiilor blockchain și protocoalelor de rețea pentru construirea de infrastructuri digitale reziliente și de încredere.
Aptitudini (Abilităţi)	Studentul-doctorand/absolventul: • Proiectează arhitecturi securizate și protocoale de comunicare avansate pentru rețele de calculatoare; • Implementează și evaluează sisteme bazate pe tehnologia blockchain pentru asigurarea integrității și transparenței datelor; • Analizează vulnerabilitățile sistemelor software și propune mecanisme de apărare inovatoare.
Responsabilitate și autonomie	Studentul-doctorand/absolventul: • Adoptă decizii strategice privind securitatea și confidențialitatea datelor în proiectele de cercetare; • Acționează ca expert în evaluarea riscurilor tehnologice în sisteme web și infrastructuri critice.

7. Conţinuturi

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.	Față în față (cu prezență fizică)	Predarea cursului se face folosind videoproiectorul: 70% prezentare teoretică, pe baza suportului de curs, 30% activitate interactivă (discuții cu studenții doctoranzi). Materialele necesare sunt puse la dispoziția studenților în format electronic. Ca strategii de transmitere și însușire a cunoștințelor se utilizează: Expunerea; Interacțiunea prin întrebări și răspunsuri; Deducția; Testarea; Exemple teoretice; Demonstrații practice; Evaluarea finală.	2
Curs 2. Instrumente criptografice criptarea simetrică; criptarea cu cheie publică; semnătură digitală și gestiunea cheilor; generarea numerelor pseudo-aleatoare.	Față în față (cu prezență fizică)		2
Curs 3. Mecanisme de autentificare a utilizatorilor principiile de autentificare; autentificare prin parolă; autentificare pe bază de token; autentificare biometrică.	Față în față (cu prezență fizică)		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.	Față în față (cu prezență fizică)		2
Curs 5. Securitatea bazelor de date controlul accesului la o bază de date; inferența; baze de date statistice; criptarea bazelor de date	Față în față (cu prezență fizică)		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)	Față în față (cu prezență fizică)		2
Curs 7. Software malign tipuri de software malign; viruși informatici; măsuri contra virușilor informatici; viermi informatici; bots (roboți); rootkits	Față în față (cu prezență fizică)		2
Curs 8. Denial of service (Negarea utilizării serviciilor)	Față în față (cu prezență fizică)		2

atacuri de tip denial of service (DoS); atacuri de tip flooding (inundație); atacuri de tip 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

7.2. Seminar	Modalitatea de desfășurare	Metode de predare	Fond de timp alocat (ore)
Sem. 1: inițiere în utilizarea librăriei criptografice OpenSSL	Față în față (cu prezență fizică)	Ca strategii de transmitere și însușire a cunoștințelor se utilizează: Tutoriale; Demonstrații practice; Interacțiune prin întrebări și răspunsuri. Activități: 70% desfășurarea activității de expunere, 30% interpretarea rezultatelor și discuții	2
Sem. 2: utilizarea criptografiei simetrice (DES, 3DES, AES)	Față în față (cu prezență fizică)		2
Sem. 3: utilizarea criptografiei asimetrice (RSA)	Față în față (cu prezență fizică)		2
Sem. 4: utilizarea semnăturii digitale	Față în față (cu prezență fizică)		2
Sem. 5: familiarizarea cu algoritmii de determinare a valorii rezumat și cei de semnătură digitală (MD5, SHA1, DSA, DH)	Față în față (cu prezență fizică)		2
Sem. 6 : implementarea și utilizarea unei aplicații folosind liste de control al accesului (ACL)	Față în față (cu prezență fizică)		2

Sem. 7: implementarea unei arhitecturi client-server securizate pe partea de comunicație	Față în față (cu prezență fizică)	cu studenții doctoranzi.	2
Sem. 8: instalare, configurare și familiarizare cu utilitarul SNORT (sistem de detecție a intruziunilor)	Față în față (cu prezență fizică)		2
Sem. 9: exemplificare de viruși informatici și folosirea anti-virușilor	Față în față (cu prezență fizică)		2
Sem. 10: instalare, configurare și familiarizare cu un utilitar de tip firewall	Față în față (cu prezență fizică)		2
Sem. 11: instalare, configurare și familiarizare cu un utilitar de tip IDS/IPS	Față în față (cu prezență fizică)		2
Sem. 12: aplicații vulnerabile la atacuri de tip buffer overflow	Față în față (cu prezență fizică)		2
Sem. 13: familiarizarea cu o infrastructură cu cheie publică (certificate digitale, autorități de certificare, autorități de înregistrare)	Față în față (cu prezență fizică)		2
Sem. 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 prelegerilor și al aplicațiilor se aliniază cu cel al cursurilor similare de la alte universități naționale și internaționale. Rezultatele învățării și competențele dobândite corespund cerințelor marilor angajatori. Acestea au fost dezvoltate și îmbunătățite continuu pe baza informațiilor primite de la reprezentanții companiilor IT locale. Conținutul prelegerilor și al aplicațiilor se aliniază cu cel al cursurilor similare de la alte universități naționale și internaționale. Rezultatele învățării și competențele dobândite corespund cerințelor marilor angajatori. Acestea au fost dezvoltate și îmbunătățite continuu pe baza informațiilor primite de la reprezentanții companiilor IT locale.
Conținutul cursului a fost discutat cu reprezentanții:

- C-S România SA
- Forvia-Hella Craiova

9. Evaluare

Tip activitate	9.1. Criterii de evaluare	9.2. Metode de evaluare	9.3. Pondere din nota finală
9.1. Curs	Rezolvarea de exerciții și probleme care implică metode și tehnici de proiectare și analiză a algoritmilor.	Examen scris (2 subiecte teoretice) / grilă online (în funcție de structura aprobată a anului universitar).	70%
9.2. Seminar	Experiență în proiectarea și analiza algoritmilor.	Verificare pe parcurs și testare finală	30%
9.3. Standard minim de performanță: ▪ Obținerea a minimum 50 % din punctajul verificărilor pe parcurs, testării de la seminar și examenului final. ▪ Calculul notei finale se face prin rotunjirea la notă întreagă a punctajului final.			

Data completării
01.10.2025

Titular de disciplină,
Prof. dr. ing. Marius MARIAN

Semnătura titularului

……

Data avizării în Consiliul Școlii Doctorale
03.10.2025

Director Școala Doctorală „Constantin Belea”
Prof. dr. ing. Costin BĂDICĂ

Semnătura directorului Școlii doctorale,

……..……..