FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	UNIVERSITATEA TITU MAIORESCU
1.2. Facultatea	INFORMATICĂ
1.3. Departamentul	INFORMATICĂ
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Masterat
1.6. Programul de studii/ Calificarea/ Specializarea	SECURITATEA SISTEMELOR INFORMATICE ŞI A REŢELELOR INFORMAŢIONALE
1.7. Limba de studiu	Română

2. Date despre disciplină

2.1 Denumirea disciplinei			**SECURITATEA REȚELELOR DE COMUNICAȚII**				
2.2 Titularul/titularii activităţilor de curs			**Prof. univ. dr. ing. Ciprian RĂCUCIU**				
2.3 Titularul/titularii activităţilor de seminar/laborator			**Prof. univ. dr. ing. Ciprian RĂCUCIU**				
2.4 Anul de studiu	**II**	2.5 Semestrul	**3**	2.6 Tipul de evaluare	**E**	2.7 Regimul disciplinei	**APR**

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 seminar/ laborator	**2**
3.4 Total ore din planul de învăţământ/ Total ore online din planul de învățământ	56/ 24	din care: 3.5 curs - față în față online	28/ 12/ 16	3.6 seminar/ laborator - față în față online	28/ 20/ 8

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie și notițe	66
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	38
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	48
Tutoriat	18
Examinări	4
Alte activităţi:	10
3.7. Total ore studiu individual	184
3.8. Total ore de studiu pe semestru	240
3.9 Numărul de credite	**8**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Algebra în câmpuri finite, Teoria probabilităţilor
4.2 de competențe	• Abilități de utilizare a limbajelor de programare a calculatoarelor

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Teoria transmiterii şi codificării informaţiei • Criptografie şi securitatea informației
5.2. de desfășurare a seminarului/laboratorului	• Orele se vor desfăşura în laborator dotat cu tehnica de calcul şi aparatură multimedia. • Cunoaşterea limbajelor de programare.

6.1. Competenţele specifice acumulate	
Competențe profesionale	**Cunoaştere şi înţelegere:** • cunoaşterea noţiunilor specifice din domeniul securității informației aplicate în reţele de comunicaţii; • înţelegerea structurii şi elementelor algoritmilor de cifrare, compresie si codificare; • înţelegerea utilizării algoritmilor de criptare / cifrare în implementare software. **Utilizarea cunoștințelor:** • explicarea metodelor de utilizare a algoritmilor de cifrare; • interpretarea unor noţiuni utilizate în domeniul criptografiei și securității informației; **Aplicarea unor principii și metode de bază pentru rezolvarea de probleme tipice domeniului:** • corelarea cunoştinţelor teoretice cu abilitatea de a le aplica în practică; • întocmirea algoritmilor criptografici şi implementarea acestora; • aplicarea modelelor de analiză și sinteză în rezolvarea unor probleme specifice. **Utilizarea adecvată de criterii și metode standard de evaluare pentru a aprecia calitatea, meritele și limitele unor procese, programe, proiecte, concepte, metode și teorii**: • utilizarea instrumentelor matematice, statistice si a metodelor specifice pentru a caracteriza si evalua performantele sistemelor şi reţelelor de comunicaţii. **Elaborarea de proiecte profesionale cu utilizarea unor principii și metode consacrate în domeniu:** • înţelegerea importanţei domeniului securității informației aplicate în cadrul reţelelor de comunicaţii; • înţelegerea necesităţii metodelor de securizare a informației în sistemele informaţionale şi de comunicații; • proiectarea și implementarea unor aplicații specifice securităţii informaţionale.
Competențe transversale	**Executarea responsabilă a sarcinilor profesionale:** • analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluții consacrate, asigurând astfel îndeplinirea sarcinilor profesionale; **Familiarizarea cu rolurile şi activităţile specifice muncii în echipă:** • definirea activităților pe etape și repartizarea acestora membrilor echipei, având grijă să fie precizate și explicate îndatoririle, în funcție de nivelul de acces la informație și de poziție în structura funcțională a temelor; • asigurarea unui feed-back eficient de informații și promovarea unui sistem de comunicare în scopul propriu-zis de comunicare astfel încât interlocutorul să fie influenţat şi în același timp (în funcție de necesități) să își schimbe comportamentul; **Conştientizarea nevoii de formare continuă:** • adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare tipărite, software specializat și resurse electronice în limba româna și, cel puțin, într-o limbă de circulație internațională;

	• implicarea în activităţi ştiinţifice de cercetare, de participare la elaborarea unor articole şi studii de specialitate.

6.2. Rezultatele învățării

Cunoștințe	Studentul cunoaște: - cele mai bune mecanisme de securitate care pot fi implementate în cadrul rețelelor de comunicații, vocale și date, Internet; - cunoaște algoritmii de codificare cei mai des folosiți în: compresia datelor, codarea de canal a datelor, criptografie precum și cele mai importante protocoale din cadrul rețelelor informatice/informaționale care implementează acești algoritmi.
Aptitudini	Studentul este capabil: - să identifice posibilele probleme de securitate în sistemele de comunicații și în rețelele informaționale, vulnerabilitățile și riscurile de securitate; - să proiecteze și să implementeze instrumente de verificare a securității sistemelor tehnice.
Responsabilitate și autonomie	Studentul are capacitatea de a înțelege: - conceptele fundamentale de administrare de sistem tehnic de comunicații și de rețea; - aspectele de securitate conexe acestui proces; - își asumă responsabilitatea pentru produsul muncii sale, solicită feedback și îl utilizează constructiv.

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

7.1 Obiectivul general al disciplinei	• dezvoltarea de competenţe profesionale în domeniul securității informaţiei din reţelele de comunicaţii.
7.2 Obiectivele specifice	• asimilarea cunoştinţelor teoretice privind proiectarea şi simularea funcționării blocurilor de prelucrare a informaţiei din sistemele de comunicaţii, • utilizarea programelor de simulare moderne (CRYPTOOL, etc.); • obţinerea deprinderilor şi abilităţilor necesare pentru testarea performanţelor algoritmilor de secretizare informațională.

8. Conţinuturi

8. 1 Curs	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
1. Noțiuni generale privitoare la securitatea sistemelor de comunicații. Principii și metode de secretizare a informațiilor din sistemele de comunicații (4c);	Interactiva	(2/2) h
2. Algoritmi de criptare. Sisteme simetrice și asimetrice (4c);	Interactiva	(2/2) h

3. Cerințe de bază pentru algoritmii de criptare guvernamentali utilizați în sistemele de comunicații (2c);	Interactiva	(0/2) h
4. Reţele de comunicaţii mobile. Tipuri de reţele mobile. Arhitectura sistemelor de comunicaţii mobile. Ameninţări şi vulnerabilităţi. (2c).	Interactiva	(0/2) h
5. Securitatea reţelelor de comunicații. Riscurile comune asociate folosirii reţelelor de comunicaţii. Vulnerabilități ale sistemelor de comunicații, care favorizează interceptările ilegale sau scurgerea accidentală de informații. Măsuri de protecție împotriva interceptării comunicaţiilor şi pentru securizarea informaţiilor. (8c)	Interactiva	(4/4) h
6. Managementul protecției informațiilor și a sistemelor de comunicații (4c).	Interactiva	(0/2) h
7. Elemente de criptanaliză (2c).	Interactiva	(0/2) h
8. Digitalizare si profesii emergente ale viitorului (2c).	Interactiva	(2/0) h

Bibliografie

1. Ciprian Răcuciu, Marius Rogobete, Madlena Nen, Criptografie şi securitatea informaţiei. Curs pentru învăţământ la distanţă – Bucureşti, Editura Academiei Tehnice Militare, 2016. ISBN 978-973-640-255-5.
2. Ciprian Răcuciu, Dan Grecu, Criptografie si securitatea informaţiei, Editura Renaissance, Bucureşti, 2010, ISBN 978-606-8321-89-9.
3. Ciprian Răcuciu, Criptografie si securitatea informaţiei, Editura UTM, Bucureşti, 2008, ISBN 978-606-8002-06-4.
4. Ciprian Răcuciu, Dan-Laurenţiu Grecu, Metode şi sisteme criptografice secvenţiale, Editura ERICOM, Bucureşti, 2008, ISBN(13) 978-973-88290-9-1.
5. Roger J. Sutton, “Secure Communications”, Applications and Management, John Wiley & Sons, 2000.
6. Roger Anderson, “Security Engineering – A guide to building dependable distributed systems”, John Wiley & Sons, 2001.

8. 2 Seminar/ Laborator	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
1. Noțiuni generale privitoare la securitatea sistemelor de comunicații. (2s)	Interactiva	(2/2) h
2. Principii și metode de secretizare a informațiilor din sistemele de comunicații. (4s)	Interactiva	(2/2) h
3. Algoritmi de criptare. Sisteme simetrice și asimetrice. (4s)	Interactiva	(2/0) h
4. Cerințe de bază pentru algoritmii de criptare guvernamentali utilizați în sistemele de comunicații. (2s)	Interactiva	(2/0) h

5. Reţele de comunicaţii mobile. Tipuri de reţele mobile. Arhitectura sistemelor de comunicaţii mobile. Ameninţări şi vulnerabilităţi. (2s)	Interactiva	(6/2) h
6. Securitatea reţelelor de comunicații. Riscurile comune asociate folosirii reţelelor de comunicaţii. Vulnerabilități ale sistemelor de comunicații, care favorizează interceptările ilegale sau scurgerea accidentală de informații. Măsuri de protecție împotriva interceptării comunicaţiilor şi pentru securizarea informaţiilor. (8s)	Interactiva	(2/2) h
7. Managementul protecției informațiilor și a sistemelor de comunicații (4s).	Interactiva	(2/0) h
8. Elemente de criptanaliză (2s).	Interactiva	(2/0) h

Bibliografie

1. Ciprian Răcuciu, Marius Rogobete, Madlena Nen, Criptografie şi securitatea informaţiei. Curs pentru învăţământ la distanţă – Bucureşti, Editura Academiei Tehnice Militare, 2016. ISBN 978-973-640-255-5.
2. Ciprian Răcuciu, Dan Grecu, Criptografie si securitatea informaţiei, Editura Renaissance, Bucureşti, 2010, ISBN 978-606-8321-89-9.
3. Ciprian Răcuciu, Criptografie si securitatea informaţiei, Editura UTM, Bucureşti, 2008, ISBN 978-606-8002-06-4.
4. Roger J. Sutton, "Secure Communications", Applications and Management, John Wiley & Sons, 2000.
5. Victor -Valeriu Patriciu - Criptografia şi securitatea reţelelor de calculatoare cu aplicaţii în C şi Pascal - Editura Tehnică, Bucureşti, 1994.

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

- Adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare tipărite, software specializat și resurse electronice în limba romana și, cel puțin, într-o limbă de circulație internațională;
- Implicarea în activităţi ştiinţifice de cercetare, de participare la elaborarea unor articole şi studii de specialitate, de implicare în activitățile cercurilor științifice studențești.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Răspunsuri la teste si examen	Examen	60 %
	Aprecierea interesului şi activităţii la cursuri	Teste pe parcursul semestrului	10%
10.5 Seminar/ Laborator	Aprecierea activităţilor aplicative	Colocviu de laborator; Dezbateri	5%

	Aprecierea lucrărilor practice	Proiect	25%
10.6. Standard minim de performanţă			
• Promovarea examenului cu nota minimă 5 şi realizarea lucrărilor practice solicitate.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar/ laborator
25.09.2025	.....	.....

Data avizării în departament — Semnătura directorului de departament

26.09.2025 — Conf. univ. dr. ing. Tudor Cătălin APOSTOLESCU

FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea Titu Maiorescu
1.2. Facultatea	Informatică
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Masterat
1.6. Programul de studii/ Calificarea/ Specializarea	SECURITATEA SISTEMELOR INFORMATICE ȘI A REȚELELOR INFORMAȚIONALE
1.7. Limba de studiu	Română

2. Date despre disciplină

2.1 Denumirea disciplinei			**Fiabilitatea și testarea sistemelor de calcul**				
2.2 Titularul/titularii activităţilor de curs			**Conf.dr.Viorel IONESCU**				
2.3 Titularul/titularii activităţilor de seminar/laborator			**Conf.dr.Viorel IONESCU**				
2.4 Anul de studiu	**II**	2.5 Semestrul	**3**	2.6 Tipul de evaluare	**E**	2.7 Regimul disciplinei	**SINT**

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 seminar/ laborator	**2**
3.4 Total ore din planul de învăţământ/ Total ore online din planul de învățământ	56 / 24	din care: 3.5 curs față în față online	28/ 12 16	3.6 seminar/ laborator față în față online	28/ 20/ 8

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie și notițe	70
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	38
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	34
Tutoriat	8
Examinări	4
Alte activităţi:	
3.7. Total ore studiu individual	154
3.8. Total ore de studiu pe semestru	210
3.9 Numărul de credite	**7**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Probabilităţi si statistică matematica, Arhitectura calculatoarelor, Programare

4.2 de competențe	1. Capacitatea de a opera cu notiuni si tehnici ale Teoriei probabilitatilor si proceselor stochastice, Statisticii matematice, ale constructiei si utilizarii calculatoarelor, ale elaborarii si utilizarii programelor. 2. Capacitatea de a-si forma reprezentari integratoare ale unor concepte si notiuni ale teoriei proceselor Markov, Poisson in vederea intelegerii si considerarii acestora ca elemente de baza ale modelului teoretic, care face posibila testarea produselor software.

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Stație de lucru Windows/Linux conectată Internet, proiector , tabla inteligenta
5.2. de desfășurare a seminarului/laboratorului	• Stații de lucru Windows/Linux conectate Internet • programe specifice KALI, RSM,SELENIUM, EIFFEL

6.1 Competenţele specifice acumulate

Competenţe profesionale	• Programarea în limbaje de nivel înalt • Dezvoltarea şi întreținerea aplicațiilor informatice. • Utilizarea instrumentelor informatice in context interdisciplinar • Utilizarea bazelor teoretice ale informaticii si a modelelor formale
Competenţe transversale	• Aplicarea regulilor de muncă organizată şi eficientă, a unor atitudini responsabile faţă de domeniul didactic-ştiinţific, pentru valorificarea creativă a propriului potenţial, cu respectarea principiilor şi a normelor de etică profesională; • Desfăşurarea eficientă a activităţilor organizate într-un grup inter-disciplinar și dezvoltarea capacităţilor empatice de comunicare inter-personală, de relaţionare şi colaborare cu grupuri diverse; • Utilizarea unor metode şi tehnici eficiente de învăţare, informare, cercetare şi dezvoltare a capacităţilor de valorificare a cunoştinţelor, de adaptare la cerinţele unei societăţi dinamice și de comunicare în limba română și într-o limbă de circulație internațională.

6.2. Rezultatele învățării

Cunoștințe	• Masterandul analizează critic fundamentele teoretice ale ciclului de viață al testării (STLC) și metodologiile avansate de testare a securității software, diferențiind între analiza statică/dinamică a aplicațiilor și abordarea black-box • Masterandul explică în detaliu tehnicile de atac cibernetic, clasificarea malware și conceptul de Ethical Hacking, recunoscând implicațiile juridice și etice ale acestora • Cursantul demonstrează cunoștințe foarte specializate despre conceptele de imprevizibilitate a sistemelor complexe, erori latente, defecte/defectări și modul în care acestea contribuie la crearea de vulnerabilități Web și de rețea
Aptitudini	• Masterandul utilizează eficient distribuții și instrumente specializate (precum KALI, Metasploit, Nmap, Wireshark) pentru a efectua teste de penetrare a rețelelor, sistemelor și aplicațiilor, conform protocoalelor acceptate • Masterandul evaluează (evaluare critică) și proiectează contramăsuri eficiente și soluții de securitate, bazate pe înțelegerea tehnicilor de atac cibernetic și a vulnerabilităților identificate • Masterandul elaborează și simulează exerciții practice de recuperare în urma dezastrelor (DRP), folosind tehnologii moderne de virtualizare și containere (Docker, KUBERNETES) pentru a restabili operațiunile sistemelor
Responsabilitate și autonomie	• Masterandul își asumă responsabilitatea pentru gestionarea și transformarea situațiilor de securitate complexe și imprevizibile, propunând noi abordări strategice pentru îmbunătățirea securității digitale a organizație • Masterandul demonstrează autonomie și inovație în dezvoltarea și implementarea de planuri de securitate și politici de prevenire a încălcărilor de securitate a datelor • Masterandul **conduce și coordonează** echipe în **executarea auditurilor și testelor de securitate TIC**, asumând responsabilitatea pentru identificarea problemelor critice și recomandarea de soluții bazate pe standarde

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

7.1 Obiectivul general al disciplinei	1. Inţelegerea de ansamblu a importanţei disciplinei studiate şi a legăturii cu celalalte discipline fundamentale. 2. Cunoasterea si intelegerea problemelor legate de realizarea, achizitionarea si calitatea produselor software. 3. Capacitatea de a formula ipoteze si de a preciza conditii legate de rezolvarea unei probleme de calitate a unui produs software. 4. Capacitatea de a alege demersuri teoretice adecvate verificarii ipotezelor si validarii unui model software.
7.2 Obiectivele specifice	1. Capacitatea de a opera cu notiuni si tehnici ale Teoriei probabilitatilor si proceselor stochastice, Statisticii matematice, ale constructiei si utilizarii calculatoarelor, ale elaborarii si utilizarii programelor. 2. Capacitatea de a-si forma reprezentari integratoare ale unor concepte si notiuni ale teoriei proceselor Markov, Poisson in vederea intelegerii si considerarii acestora ca elemente de baza ale modelului teoretic, care face posibil studiul calitatii produselor software.

	3. Capacitatea de a transfera cunoștințe, idei si rezultate ale teoriei calităţii produselor software, la probleme legate de arhitectura calculatoarelor, de construcția și utilizarea programelor.

8. Conţinuturi

8. 1 Curs	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
Curs 1.Digitalizare si profesii emergente ale viitorului Ciclu de viaţă al produselor software (SDLC) vs Ciclul de viata al testarii (STLC); .	Prelegere participativa. Expunere, Exemplu demonstrativ	4 ore din care 2 ore online/ 2 ore față în față
Curs 2. Metodologii de testare a securitatii software. Testarea securității. Procesul de testare a penetrării. Analiza statică / dinamică a aplicațiilor		4 ore din care 4 ore online/ 0 ore față în față
Curs 3. Imprevizibilitatea sistemelor complexe. Erori latente şi bug-uri. Defecte si defectari. Identificarea vulnerabilităților Web și de rețea. Exploatarea vulnerabilităților web de securitate		4 ore din care 4 ore online/ 0 ore față în față
Curs 4. Ethical hacking. Wi-fi hacking		6ore din care 2 ore online/ 4 ore față în față
Curs 5.Introducere. Clasificare malware. Tehnici de analiză malwareModele statice ale sistemelor complexe software ; abordarea de tip black-box		4 ore din care 2 ore online/ 2 ore față în față
Curs 6.Proiectarea software-lui în vedera testării (DFT)		2 ore din care 0 ore online/ 2 ore față în față
Curs 7.Principii privind asigurarea continuităţii operaţionale (BC) ISO 22301;Implementarea unui plan de recuperare în caz de dezastre (DRP). Metrici Recovery Point Objective (RPO) and Recovery Time Objective (RTO)		2 ore din care 2 ore online/ 0 ore față în față
Curs 8.Tehnologii de virtualizare; Utilizarea containerelor.		2 ore din care 0 ore online/ 2 ore față în față

Bibliografie

- Occupytheweb, Linux Basics for Hackers, 2nd Edition: Getting Started with Networking, Scripting, and Security in Kali, ISBN-13 : 978-1718503540 , 2025
- Dale Meredith,The OSINT Handbook: A practical guide to gathering and analyzing online informationI SBN-13 978-1837638277 , 2024
- Occupytheweb Network Basics for Hackers: How Networks Work and How They Break,ISBN-13 : 979-8373290043, 2023

- Zhassulan Zhussupov Malware Development for Ethical Hackers: Learn how to develop various types of malware to strengthen cybersecurity, ISBN-13 : 978-1801810173 , 2024
- Maurício Aniche, Effective Software Testing: A developer's guide, Manning (April 26, 2022) ISBN-13 : 978-1633439931
- Vijay Kumar Velu, Mastering Kali Linux for Advanced Penetration Testing: Become a cybersecurity ethical hacking expert using Metasploit, Nmap, Wireshark, and Burp Suite, 4th Edition, 2022, ISBN-10 : 1801819777
- Practical Software Testing – Chindam Damodar , ebook, 2018
- Testing Computer Software, 2nd Edition, Cem Kaner, ISBN-13: 978-0471358466
- Enterprise Software Security: A Confluence of Disciplines (Addison-Wesley Software Security) 1st Edition by Kenneth R. van Wyk , Mark G. Graff , Dan S. Peters, Diana L. Burley Ph.D.
- R. Anderson, Security Engineering: A Guide to Building Dependable Distributed System, 2nd ed., John Wiley & Sons, 2008; www.cl.cam.ac.uk/~rja14/book.html
- How to Break Software: A Practical Guide to Testing, James Whittaker, ISBN-10: 9780201796193
- B. Chess and J.West, Secure Programming with Static Analysis, Addison-Wesley, 2007; http://buildingsecurityin.com
- K. Schmidt, "High Availability and Disaster RecoveryConcepts, Design, Implementation", Springer, 2006
-
- The Certified Software Tester (**CSTE) book**
- Jones, Capers and Bonsignour, Olivier; The Economics of Software Quality; Addison Wesley, Boston, MA; 2011; ISBN 978-0-13-258220-9
- Dumke, Reiner; Braungarten, Rene; Büren, Günter; Abran, Alain; Cuadrado-Gallego, Juan J; (editors); Software Process and Product Measurement; Springer-Verlag, Berlin; ISBN 10: 3-540-89402-0; 2008
- Ghita A., Ionescu V. Metode de calcul in Fiabilitate, editura ATM,1996
- Ghita A., Ionescu V. Metode de calcul in Mentenabilitate, editura ATM,2000
- ENISA, "IT Business Continuity Management", 2010

8. 2 Seminar/ Laborator	Metode de predare	Observații
Laborator 1 Prezentarea suitei Application Lifecycle Management (ALM), UFT și WEBINSPECT pentru executare teste de securitate.	Exemplu, algoritm, utilizare produse proprietar și/sau COTS, interpretarea rezultatelor	8 ore din care 2 ore online/ 6 ore față în față
Laborator 2 Teste de penetrare folosind KALI. Prezentare generala		6 ore din care 2 ore online/ 4 ore față în față
Laborator 3 Instrumente pentru testarea penetrării rețelelor.		4 ore din care 2 ore online/ 2 ore față în față
Laborator 4 Instrumente pentru testarea penetrării sistemelor		2 ore online
Laborator 5 Tehnici de testare black-box		2 ore
Laborator 6 Atacuri cu parolă. Tipuri de parole		2 ore
Laborator 7 Utilizare docker și KUBERNETES		4 ore

Bibliografie

1. Vijay Kumar Velu, Mastering Kali Linux for Advanced Penetration Testing: Become a cybersecurity ethical hacking expert using Metasploit, Nmap, Wireshark, and Burp Suite, 4th Edition, 2022, ISBN-

10 : 1801819777
2. Suport de curs
3. The Certified Software Tester **(CSTE)** book
4. suita de produse MICROFOCUS ALM, UFT, WEBINSPECT
5. mediulRSM
6. mediul EIFFEL
7. SELENIUM

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

- Conţinutul disciplinei este în concordanţă cu ceea ce se face în alte centre universitare din tara și din străinătate. Pentru o mai buna adaptare la cerinţele pieţei muncii a conţinutului disciplinei au avut loc întalniri atât cu reprezentaţi ai mediului de afaceri.(MICROFOCUS, MICROSOFT)

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	- corectitudinea și completitudinea cunoștinţelor asimilate; - o înţelegere de ansamblu a importanţei disciplinei studiate şi a legăturii cu celalalte discipline fundamentale - coerenţa logică; - gradul de asimilare a limbajului de specialitate; - criterii ce vizeaza aspectele atitudinale: interesul pentru studiul individual si dezvoltarea profesionala	Test grila	40
	- testarea periodică	Lucrare de control C2 și C5	10
10.5 Seminar/ Laborator	- capacitatea de a opera cu notiuni abstracte; - capacitatea de aplicare în practică; - criterii ce vizeaza aspectele atitudinale: seriozitatea, interesul pentru studiul individual.	Susținere	40
	- teme / referate / eseuri / traduceri / proiecte prezenta	Conversație de evaluare	10
10.6. Standard minim de performanţă			
• Însuşirea cunoştinţelor de bază și aplicarea lor în realizarea unor aplicații simple; • Obţinerea unui număr de 5 puncte din totalul de 10 repartizat pentru diferite categorii de subiecte; • Realizarea unui referat despre o categorie de teste software studiata (sau un model testare software studiat).			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar/ laborator
25.09.2025	.....	.....

Data avizării în departament

Semnătura directorului de departament

26.09.2025 .....

.....

FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	UNIVERSITATEA TITU MAIORESCU
1.2. Facultatea	INFORMATICĂ
1.3. Departamentul	INFORMATICĂ
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Master
1.6. Programul de studii/ Calificarea/ Specializarea	Informatică
1.7. Limba de studiu	Română

2. Date despre disciplină

2.1 Denumirea disciplinei			**Securitatea Aplicaţiilor Web**				
2.2 Titularul/titularii activităţilor de curs			**Conf.dr.ing. Mironela PÎRNĂU**				
2.3 Titularul/titularii activităţilor de seminar/laborator			**Conf.dr.ing. Mironela PÎRNĂU**				
2.4 Anul de studiu II		2.5 Semestrul 3		2.6 Tipul de evaluare	**E**	2.7 Regimul disciplinei	APR

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 seminar/ laborator	**2**
3.4 Total ore din planul de învățământ/ Total ore online din planul de învățământ	56 / 24	din care: 3.5 curs - față în față - online	28/ 12/ 16	3.6 seminar/ laborator - față în față - online	28/ 20/ 8
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					70
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					38
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					34
Tutoriat					8
Examinări					4
Alte activităţi:					
3.7. Total ore studiu individual					**154**
3.8. Total ore de studiu pe semestru (numărul de credite * 30)					**210**
3.9 Numărul de credite ECTS					**7**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Legislaţie în domeniul securităţii informatice; Securitatea documentelor electronice; Securitatea bazelor de date;Securitatea rețelelor de calculatoare

4.2 de competențe	• Să cunoască terminologia utilizată în domeniul securității informatice, securității documentelor electronice, securității bazelor de date și rețelelor de calculatoare.

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Cursurile se vor desfășura în modul mixt (față în față și online) atât în săli dotate cu echipamente pentru predare multimedia cât și online pe platforma MS-Teams. În modul mixt toti masteranzii utilizează resursele din Centrul Cyberx-UTM.
5.2. de desfășurare a seminarului/laboratorului	Masteranzii se vor prezenta la laboratorul mixt cu materia aferentă cursului anterior parcursă și cu temele rezolvate. Laboratoarele se vor desfășura în cloud pe platforma Cyberx-UTM

6.1 Competenţele specifice acumulate

Competenţe profesionale	• Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice aferente domeniului general al securității informațiilor. Identificarea și înțelegerea problemelor de securitate ce pot apărea în contextul aplicatiilor WEB. Deprinderea conceptelor esențiale legate de securitatea aplicatiilor WEB; • Cunoasterea noţiunilor de bază pentru identificarea vulnerabilitatilor aplicatiilor WEB. • Dezvoltarea abilitatilor pentru recunoasterea principalelor atacuri asupra aplicatiilor WEB; • Însuşirea noţiunilor fundamentale privind utilizarea instrumentelor software automate pentru detectarea vulnerabilităților aplicatiilor WEB; • Abilitatea de a evalua și documenta, din perspectiva securității WEB, vulnerabilitatile anei aplicatii WEB; • Dezvoltarea abilitatilor masteranzilor pentru alte disciplinele de specialitate; • Utilizarea instrumentelor informatice în context interdisciplinar; • Utilizarea adecvată în comunicarea profesională a conceptelor, metodelor și teoriilor specifice domeniului securitatii Web; • Aplicarea principiilor și metodelor specifice domeniului pentru rezolvarea unor situații și probleme specifice cu asigurarea unei asistențe calificate.
Competenţe transversale	• Executarea responsabilă a sarcinilor profesionale, în condiţii de autonomie restransă şi asistenţă calificată • Familiarizarea cu rolurile şi activităţile specifice muncii în echipă şi distribuirea de sarcini pentru nivelurile subordonate • Conştientizarea nevoii de formare continuă; utilizarea eficientă a resurselor şi tehnicilor de învăţare pentru dezvoltarea personală şi profesională

6.2. Rezultatele învățării

Cunoștințe	• Masterandul identifică și explică conceptele fundamentale privind arhitectura aplicațiilor web, tipurile de aplicații și principiile de comunicare client–server. • Masterandul descrie și argumentează etapele de dezvoltare și proiectare a aplicațiilor web, evidențiind diferențele dintre tehnologiile client-side și server-side. • Masterandul analizează și evaluează riscurile, vulnerabilitățile și atacurile specifice aplicațiilor web, precum și metodele de prevenire și protecție, în conformitate cu ghidurile OWASP.
Aptitudini	• Masterandul aplică metodele și mecanismele de securizare a aplicațiilor web, inclusiv autentificarea, autorizarea, criptarea, validarea datelor și protecția parolelor. • Masterandul dezvoltă și configurează instrumente de testare și monitorizare a securității aplicațiilor, utilizând aplicații specializate pentru analiza vulnerabilităților. • Masterandul elaborează rapoarte tehnice și justifică soluțiile propuse pentru asigurarea securității aplicațiilor web și protejarea informațiilor în mediile online și rețelele sociale.
Responsabilitate și autonomie	• Masterandul respectă principiile de etică academică, citând corect sursele bibliografice utilizate. • Masterandul demonstrează receptivitate pentru contexte noi de învățare. • Masterandul manifestă colaborare cu ceilalți colegi și cadre didactice în desfășurarea activităților didactice. • Masterandul coordonează activitățile de proiectare și dezvoltare a aplicațiilor web, asumând decizii responsabile privind securitatea, performanța și integrarea componentelor software. • Masterandul aplică principii etice și deontologice în asigurarea securității aplicațiilor web, respectând normele de confidențialitate, protecția datelor și bunele practici în mediul online. • Masterandul gestionează în mod autonom procesele de testare, monitorizare și evaluare a vulnerabilităților aplicațiilor web și propune soluții adecvate de remediere și prevenire. • Masterandul colaborează eficient cu echipe interdisciplinare pentru dezvoltarea de soluții sigure și robuste și demonstrează responsabilitate în utilizarea resurselor tehnologice, precum și în informarea utilizatorilor asupra riscurilor cibernetice.

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

7.1 Obiectivul general al disciplinei	• Capacitatea evaluării caracteristicilor de securitate ale unei aplicații WEB la nivelul codului sursă. Dobândirea deprinderilor fundamentale minimale de scriere a unui cod sursă fără vulnerabilități.
7.2 Obiectivele specifice	• Cunoașterea mecanismelor de bază ce definesc securitatea

	sistemului și a mediului software în care se execută o aplicație, cum ar fi: permisiunile de acces, politicile de securitate, interacțiunea cu mediul exterior etc. • Cunoașterea principalelor tipuri de vulnerabilități software cat si atacuri posibile, la care sunt expuse aplicatiile WEB.

8. Conţinuturi

8. 1 Curs	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
Curs introductiv. In cadrul cursului introductiv sunt prezentate: obiectivele disciplinei si structura cursului, bibliografia, modalitatea de examinare, ponderea examenului în nota finală. Se prezinta principalele surse bibliografice care abordeaza metodele de securizare a aplicatiilor WEB.	Prezentari, dezbateri, parcurgere, tutoriale, ghiduri de lucru, demonstrații	2 ore față în față/
Documente si aplicaţii Web - Realizarea şi proiectarea unui document web; Tipuri de aplicaţii web; Arhitectura /dezvoltarea aplicaţiilor web.		4 ore online
Comunicarea client/server pe web -tehnologii client-side si tehnologii server-side.		2 ore față în față/
Aspecte ale securităţii aplicaţiilor web - atacuri /mecanisme de securitate.		6 ore față în față/
Riscuri cu privire la securitatea aplicatiilor web.		2 ore față în față/
Vulnerabilităţi web şi metode de prevenire a acestora; Aplicaţii care evaluează vulnerabilităţi; Tipuri de vulnerabilităti specifice aplicaţiilor web (conform owasp.org) şi metode de prevenire a acestora.		3 ore online
Atacuri asupra aplicaţiilor web. Tipuri de atacuri web şi protejarea impotriva acestora/ Atacuri asupra parolelor/Acţiunile virușilor și antivirușilor.		6 ore online
Securitatea aplicaţiilor web - Testarea /monitorizarea securităţii aplicaţiilor informatice; Reguli de securitate în reţelele sociale.		2 ore online
Digitalizare si profesii emergente ale viitorului		1 ore online

Bibliografie

1. Wilhelm, Thomas. Professional Penetration Testing: Creating and Learning in a Hacking Lab. Elsevier, 2025.
2. Rojabi, Muhammad Afdan. Pengantar OWASP. Afdan Rojabi Publisher, 2025.
3. Hoffman, Andrew. Web Application Security. O'Reilly Media, 2024.
4. Wen, Shao-Fang, and Basel Katt. "A Quantitative Security Evaluation and Analysis Model for Web Applications Based on OWASP Application Security Verification Standard." Computers & Security 135 (2023): 103532.
5. Lala, S. K., & Kumar, A. "Secure Web Development Using OWASP Guidelines." In 2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS), pp. 323–332. IEEE, 2021.
6. David Silver, Suman Jana, Dan Boneh, Eric Chen, and Collin Jackson. "Password Managers:

Attacks and Defenses." In Proceedings of the 23rd USENIX Security Symposium (Security), USENIX Association, San Diego, CA, 2014, pp. 449–464.
7. Kim, P. The Hacker Playbook: Practical Guide to Penetration Testing. Secure Planet, 2014.
8. M. Shema. Seven Deadliest Web Application Attacks. Elsevier Inc., 2010, pp. 47–69.
9. Barnett, Ryan C. Web Application Defender's Cookbook: Battling Hackers and Protecting Users. Wiley Publishing, Inc., 2010, pp. 20, 21, 402–411.
10. Brad Hill. "Attacking XML Security, Message Oriented Madness, XML Worms and Web Service Security Sanity." Black Hat Briefings USA, iSEC Partners, 2007.
11. Stuttard, D., & Pinto, M. The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws. Wiley, 2007.
12. S. Fogie, J. Grossman, R. Hansen, A. Rager, and P. D. Petkov. XSS Attacks: Cross Site Scripting Exploits and Defense. Syngress, 2007.
13. Eve Andersson, Philip Greenspun, Andrew Grumet. Software Engineering for Internet Applications. MIT Press, 2006. Disponibilă la: http://philip.greenspun.com/seia/
14. T. Ylonen, C. Lonvick. The Secure Shell (SSH) Protocol Architecture, RFC 4251, January 2006.
15. M. Andrews, J. A. Whittaker. How to Break Web Software. Addison Wesley, 2006.
16. Stefan Jablonski, Ilia Petrov, Christian Meiler, Udo Meyer. Guide to Web Application and Platform Architectures. Springer-Verlag, 2004.
17. James Snell, Doug Tidwell, Pavel Kulchenko. Programming Web Services with SOAP. O'Reilly, 2002.
18. Simon St. Laurent. Programming Web Services with XML-RPC. O'Reilly Internet Series, 2001.
19. Lecture Notes in Computer Science – Hot Topics in Engineering. Springer Verlag, 2001.
20. https://owasp.org/

8. 1 Seminar/ Laborator	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
1. Laborator introductiv**.** Se prezinta sursele bibliografice care fac refeire la vulnerabilitatile si atacurile posibile pentru aplicatiile WEB.	Dezbateri-simulări în Centrul Cyberx_UTM, explicații, discuții, interpretarea rezolvarilor aplicatiilor practice.	2 ore față în față
2. Realizarea diverselor tipuri de aplicaţii Web si metode de securizare a acestora.		4 ore față în față
3. Aspecte ale securităţii aplicaţiilor web si riscuri cu privire la securitatea aplicatiilor web.		2 ore față în față
4. Metode de prevenire a vulnerabilităţilor web.		2 ore față în față
5. Tipuri de atacuri web şi protejarea impotriva acestora/		2 ore față în față
6. Atacuri asupra parolelor/Acţiunile viruşilor şi antiviruşilor.		2 ore față în față
7. Testarea /monitorizarea securităţii aplicaţiilor informatice; Reguli de securitate în reţelele sociale.		2 ore față în față
8. Riscuri cu privire la securitatea aplicatiilor web.		2 ore față în față
9. Instalare, configurare si exploatare OWASP Zed Attack Proxy (ZAP)		2 ore față în față 2 ore online
10. Utilizare DVWA (Damn Vulnerable Web Application) pentru identificare vulnerabilitati WEB		4 ore online
11. Aplicatii specific care scanează aplicaţiile web pentru		2 ore online

a detecta vulnerabilităţi de securitate		
Bibliografie – aceeași ca la curs		

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

Conținutul și obiectivele disciplinei sunt corelate cu cerințele actuale pe piața muncii; sunt urmărite atât aspectele practice cât și responsabilizarea studenților în domeniul cerceării științifice. Studenții sunt încurajați pentru obținerea de atestări a cunoștințelor, prin materiale și asistență, acestea fiind benefice atât pentru corelarea abilităților practice recunoscute pentru studenți cu elementele teoretice și reprezintă un element esențial pentru integrare studenților pe piața muncii.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	• capacitatea de utilizare adecvată a noțiunilor; • cunoașterea terminologiei specifice; • aplicarea noțiunilor însușite în probleme aplicative.	Examen scris	60 %
10.5 Laborator	• implicarea în rezolvarea aplicațiilor propuse; • prezentarea temelor propuse și evaluarea calității cercetării efectuate; • rezolvarea aplicațiilor și temelor propuse.	Evaluare continuă pe tot parcursul semestrului (prezentare, teme, aplicații)	40 %
10.6. Standard minim de performanţă			
• prezentarea subiectelor de teorie/aplicaţii pentru obţinerea unei note de minim 5; • obţinerea unei note minime de 5 în cadrul probei practice de verificare a deprinderilor şi abilităţilor dobândite în urma activităţilor de laborator;			

Data completării — Semnătura titularului de curs — Semnătura titularului de seminar/ laborator

25.09.2025 ....

Data avizării în departament — Semnătura directorului de departament

26.09.2025 ....

FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	UNIVERSITATEA TITU MAIORESCU
1.2. Facultatea	INFORMATICĂ
1.3. Departamentul	INFORMATICĂ
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Masterat
1.6. Programul de studii/ Calificarea/ Specializarea	SECURITATEA SISTEMELOR INFORMATICE ŞI A REŢELELOR INFORMAŢIONALE
1.7. Limba de studiu	Română

2. Date despre disciplină

2.1 Denumirea disciplinei			**Război cibernetic**				
2.2 Titularul/titularii activităţilor de curs			**Lector univ. dr. ing. Dan – Laurentiu GRECU**				
2.3 Titularul/titularii activităţilor de seminar/laborator			**Lector univ. dr. ing. Dan – Laurentiu GRECU**				
2.4 Anul de studiu	**I**	2.5 Semestrul	**4**	2.6 Tipul de evaluare	**E**	2.7 Regimul disciplinei	**APR**

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 seminar/ laborator	**1**
3.4 Total ore din planul de învăţământ/ Total ore online din planul de învăţământ	**42 / 20**	din care: 3.5 curs - față în față online	**28/ 12/ 16**	3.6 seminar/ laborator - față în față online	**14/ 10/ 4**
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					**50**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					**50**
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					**29**
Tutoriat					**35**
Examinări					**4**
Alte activităţi:					
3.7. Total ore studiu individual					**168**
3.8. Total ore de studiu pe semestru (numărul de credite * 30)					**210**
3.9 Numărul de credite ECTS					**7**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Cunoașterea unui limbaj de programare (Python), noțiuni în domeniul securității cibernetice, cunoașterea si utilizarea programelor de securitate cibernetică specifice
4.2 de competențe	• Capacitate de analiză și sinteză

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Pentru desfășurarea față în față: sală dotată cu echipament de predare multimedia • Pentru desfășurarea online: fiecare masterand va trebui să aibă acces la platforma MS Teams
5.2. de desfășurare a seminarului/laboratorului	• Pentru desfășurarea față în față: sală dotată cu echipament de predare multimedia Pentru desfășurarea online: fiecare masterand va trebui să aibă acces la platforma MS Teams

6.1 Competenţele specifice acumulate

Competențe profesionale	• Înțelegerea etapelor atacului cibernetic: de la recunoaștere, înarmare, livrare, exploatare, instalare, comandă și control, până la execuția propriu-zisă a atacului, ceea ce ajută la anticiparea și contracararea atacurilor. • Tehnici de apărare cibernetică: implementarea de politici, proceduri și tehnologii pentru prevenirea, detectarea și răspunsul la incidentele cibernetice. • Utilizarea și interpretarea datelor de inteligență cibernetică (Cyber Intelligence): pentru identificarea amenințărilor și planificarea operațiunilor defensive și ofensive. • Cunoștințe despre vulnerabilități și exploatări: înțelegerea tehnicilor de penetrări, exploatare a vulnerabilităților și hacking etic (pentesting). • Gestionarea securității infrastructurilor critice: protejarea rețelelor, sistemelor informatice și echipamentelor militare esențiale. • Abilități practice: simulări, exerciții hands-on, răspuns rapid la incidente și colaborare în echipe specializate de tip Red vs Blue Team. • Aspecte legislative și strategice: cunoașterea cadrului juridic și a strategiilor naționale și internaționale în domeniul războiului cibern
Competențe transversale	• Gândire critică și analitică: Capacitatea de a evalua situații complexe, de a identifica vulnerabilități și de a propune soluții eficiente în contextul dinamic al războiului cibernetic. • Adaptabilitate și reziliență: Capacitatea de a răspunde rapid și eficient la incidente și amenințări cibernetice noi, în condiții de stres și incertitudine. • Lucru în echipă multidisciplinară: Abilitatea de a colabora cu specialiști din diverse domenii (tehnic, strategic, juridic) pentru a asigura securitatea cibernetică globală.

	• Comunicare eficientă: Furnizarea și primirea de informații corecte și clare, atât în situații de urgență, cât și în mediul organizațional. • Gestionarea proiectelor și operațiunilor: Planificarea, coordonarea și monitorizarea intervențiilor și răspunsurilor la atacuri cibernetice. • Conștientizare strategică: Înțelegerea contextului geopolitic și a impactului războiului cibernetic asupra securității naționale, regionale și globale. • Responsabilitate și etică profesională: Respectarea normelor legale și etice în domeniul securității cibernetice, gestionând informații sensibile și operațiuni critice cu integritate.

6.2 Rezultatele invatarii

Cunostinte	• Masterandul va înțelege principiile de bază ale securității cibernetice și ale războiului cibernetic, inclusiv terminologia specifică (atac, vulnerabilitate, vector de atac, obiective de securitate) și tipologiile de atacatori (infractori, crime organizate, actori statali). • Masterandul va dobândi abilități pentru a identifica, analiza și evalua amenințările cibernetice la adresa sistemelor informatice sau a infrastructurilor critice. • Masterandul va învăța tehnici și tactici specifice de apărare și de atac în spațiul cibernetic, inclusiv testare penetrantă (red team/blue team), simulări de scenarii, detecție și răspuns la incidente. • Masterandul va avea experiență practică privind proiectarea și evaluarea spațiilor de instruire specializate (poligoane cibernetice), necesare pentru antrenament și testare operațională. • Masterandul va înțelege aspectele legate de prevenirea, evaluarea și remedierea atacurilor, precum și managementul crizei informatice. • Masterandul va fi capabil să integrezi aspecte de apărare, atac și obținere de informații, precum și impactul operațiunilor cibernetice asupra organizațiilor și securității naționale.
Aptitudini	• Masterandul va avea capacitatea de a identifica semnele unui atac și de a analiza traficul pentru evidențierea compromiterii unui sistem sau rețea. • Masterandul va avea aptitudini de a colecta, păstra și analiza probe digitale în urma unui incident sau atac cibernetic, folosind instrumente specializate. • Masterandul va dezvolta abilității de a organiza echipe, de a prioritiza acțiunile și de a implementa rapid măsuri de remediere și atenuare. • Masterandul va avea aptitudini de a diseca și studia comportamentul codului malițios în medii de testare controlate, folosind instrumente precum Wireshark. • Reacție rapidă și eficientă la criză: Capacitatea de a acționa sub presiune, de a menține comunicarea clară și coordonarea interdepartamentală în situații de atac. • Masterandul va fi familiarizat cu tool-uri specifice investigației și securității cibernetice (SIEM, IDS, forensics) și aplicarea metodologiilor consacrate internațional
Responsabilitate	**Rezultate în materie de responsabilitate** • Masterandul va dezvolta capacitatea de a lua decizii rapide și informate în gestionarea incidentelor, protejând datele și operațiunile critice.

	• Masterandul va învăța să gestionezi informații sensibile și să acționezi cu integritate în scopul apărării spațiului cibernetic, respectând legislația și principiile eticii cibernetice. • Masterandul va dobândi disciplina necesară colaborării și gestionării responsabilităților colective în cadrul echipelor multidisciplinare de răspuns la incidente **Rezultate în materie de aptitudini** • Masterandul va dezvolta aptitudini de identificare, investigare și remediere rapidă a incidentelor cibernetice. • Masterandul va folosii instrumente de monitorizare, analiză forensică și management al incidentelor. • Masterandul va dezvolta aptitudinea de a comunica împreună cu gestionarea rolurilor în echipă, facilitând intervenția rapidă și partajarea informațiilor relevante.

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

7.1 Obiectivul general al disciplinei	• Familiarizarea masteranzilor cu problematica războiului cibernetic care este o extensie a conflictelor tradiționale în era digitală, unde tehnologia devine atât armă, cât și câmp de luptă.
7.2 Obiectivele specifice	• Înțelegerea modului de acțiune al hackerilor si modul în care sunt utilizate programele software pentru exploatarea vulnerabilităților sistemelor IT • Dezvoltarea capacitații de analiza a atacurilor cibernetice și luarea masurilor de stopare sau atenuare a acestora. • Dezvoltarea abilitaților de a folosii programele specifice pentru testarea de penetrare a sistemelor IT pentru determinarea apriori a vulnerabilităților și luarea masurilor pentru securizarea acestora.

8. Conţinuturi

8. 1 Curs	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
Generalități privind războiul cibernetic.	• Explicaţia • Descrierea şi exemplificarea • Demonstraţia • Problematizarea • Conversaţia euristică	2 ore față în față
Înțelegerea aspectelor privind razboiul cibernetic		2 ore față în față
Operații fizice – echipa RED TEAM		4 ore față în față
Razboiul cibernetic: Concepte si strategii		4 ore față în față
Analiza conflictelor în războiul cibernetic și studii de caz .Securitatea cibernetică în transformarea digitală		8 ore on line
Utilizarea sistemelor de operare linux în desfășurarea acțiunilor de analiza si atac al hackerilor.		4 ore on line

Utilizarea programului Wireshark pentru analiza sistemelor IT		4 ore on line

Bibliografie

- Cyborg Warfare:Concepts and Strategic Trends - Shmuel Even and David Siman-Tov inss memorandum_may2012_nr117
- Mazanec, Brian M._ Whyte, Christopher - Understanding cyber warfare_ politics, policy and strategy-Routledge (2018_2019)rom
- (SpringerBriefs on Cyber Security Systems and Networks) Dietmar P.F. Möller - Cybersecurity in Digital Transformation_ Scope and Applications-Springer (2021)
- Jeremiah Talamantes - Physical Red Team Operations_ Physical Penetration Testing with the REDTEAMOPSEC Methodology-Hexcode Publishing (2019)
- OcuppyTheWeb - Linux Basics for Hackers-No Starch Press (2019)
- OccupyTheWeb - Network Basics for Hackers (2023)
- Vinit Jain - Wireshark Fundamentals_ A Network Engineer's Handbook to Analyzing Network Traffic-Apress (2022)
- Justin Seitz, Tim Arnold - Black Hat Python_ Python Programming for Hackers and Pentesters-No Starch Press (2021)

8. 1 Seminar/ Laborator	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
Experimentarea comenzilor linux într-un mediu virtual	• Explicaţia • Descrierea şi exemplificarea • Studiul de caz • Exerciţiul • Problematizarea • Teme individuale • Lucrul în grup • Dezbaterea	2 ore față în față
Experimentarea comenzilor linux specifice diferitelor nivele ISO - OSI		4 ore față în față
Experimentarea programului Wireshark, într-un mediu virtual – studii de caz		4 ore față în față
Utilizarea Laboratorului de securitate cibernetică pentru analiza, detectarea și studiul virusurilor malware		4 ore on line

Bibliografie

- Jeremiah Talamantes - Physical Red Team Operations_ Physical Penetration Testing with the REDTEAMOPSEC Methodology-Hexcode Publishing (2019)
- OcuppyTheWeb - Linux Basics for Hackers-No Starch Press (2019)
- OccupyTheWeb - Network Basics for Hackers (2023)
- Vinit Jain - Wireshark Fundamentals_ A Network Engineer's Handbook to Analyzing Network Traffic-Apress (2022)
- Justin Seitz, Tim Arnold - Black Hat Python_ Python Programming for Hackers and Pentesters-No Starch Press (2021)

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

- În vederea stabilirii conținuturilor, titularii disciplinei au organizat o întâlnire cu specialiști din domeniu, atât academic, cât și din piața muncii. Întâlnirea a vizat identificarea nevoilor și

așteptărilor angajatorilor din domeniu și coordonarea cu alte programe similare din cadrul altor instituții de învățământ superior.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Evaluare finală	Probă scrisă	60%
10.5 Seminar/ Laborator	Tema de proiect Prezenţa și activitate	Verificare proiect Probă practică de laborator	40%
10.6. Standard minim de performanţă			
Note egale cu cel puțin nota 5 la proba de laborator şi la evaluarea finală (rezolvarea în proporţie de 50% a cerinţelor) și nota finală minim 5.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar/ laborator
25.09.2025	.....	.....

Data avizării în departament

Semnătura directorului de departament

26.09.2025 .....

.....

FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	UNIVERSITATEA TITU MAIORESCU
1.2. Facultatea	INFORMATICĂ
1.3. Departamentul	INFORMATICĂ
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Master
1.6. Programul de studii/ Calificarea/ Specializarea	SECURITATEA SISTEMELOR INFORMATICE ŞI A REŢELELOR INFORMAŢIONALE
1.7. Limba de studiu	Română

2. Date despre disciplină

2.1 Denumirea disciplinei			**SECURITATEA REȚELELOR MOBILE ȘI WIRELESS**				
2.2 Titularul/titularii activităţilor de curs			**Prof. univ. dr. ing. Ciprian RĂCUCIU**				
2.3 Titularul/titularii activităţilor de seminar/laborator			**Prof. univ. dr. ing. Ciprian RĂCUCIU**				
2.4 Anul de studiu	**II**	2.5 Semestrul	**4**	2.6 Tipul de evaluare	**E**	2.7 Regimul disciplinei	**APR**

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 seminar/ laborator	**2**
3.4 Total ore din planul de învăţământ/ Total ore online din planul de învățământ	56/ 24	din care: 3.5 curs - față în față online	28/ 12/ 16	3.6 seminar/ laborator - față în față online	28/ 20/ 8

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie și notițe	66
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	36
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	36
Tutoriat	12
Examinări	4
Alte activităţi:	0
3.7. Total ore studiu individual	154
3.8. Total ore de studiu pe semestru	210
3.9 Numărul de credite	**7**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Algebra în câmpuri finite, Teoria probabilităţilor
4.2 de competențe	• Abilități de utilizare a limbajelor de programare a calculatoarelor

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Teoria transmiterii şi codificării informaţiei • Criptografie şi securitatea informației • Securitatea reţelelor de comunicaţii
5.2. de desfășurare a seminarului/laboratorului	• Orele se vor desfăşura în laborator dotat cu tehnica de calcul şi aparatură multimedia. • Cunoașterea limbajelor de programare.

6.1. Competenţele specifice acumulate

Competenţe profesionale	**Cunoaştere şi înţelegere:** • cunoaşterea noţiunilor specifice din domeniul securității informației aplicate în reţele de comunicaţii mobile si wireless; • înţelegerea structurii şi elementelor modulelor de cifrare, compresie si codificare; • înţelegerea utilizării blocurilor de criptare / cifrare în implementare software. **Utilizarea cunoștințelor:** • explicarea metodelor de utilizare a algoritmilor de cifrare; • interpretarea unor noţiuni utilizate în domeniul criptografiei și securității informației; **Aplicarea unor principii și metode de bază pentru rezolvarea de probleme tipice domeniului:** • corelarea cunoştinţelor teoretice cu abilitatea de a le aplica în practică; • întocmirea algoritmilor criptografici şi implementarea acestora; • aplicarea modelelor de analiză și sinteză în rezolvarea unor probleme specifice. **Utilizarea adecvată de criterii și metode standard de evaluare pentru a aprecia calitatea, meritele și limitele unor procese, programe, proiecte, concepte, metode și teorii**: • utilizarea instrumentelor matematice, statistice si a metodelor specifice pentru a caracteriza si evalua performantele sistemelor şi reţelelor de comunicaţii mobile si wireless. **Elaborarea de proiecte profesionale cu utilizarea unor principii și metode consacrate în domeniu:** • înţelegerea importanţei domeniului securității informației aplicate în cadrul reţelelor de comunicaţii mobile si wireless; • înţelegerea necesităţii metodelor de securizare a informației în sistemele informaţionale şi de comunicaţii mobile si wireless; • proiectarea și implementarea unor aplicaţii specifice securităţii informaţionale.
Competenţe transversale	**Executarea responsabilă a sarcinilor profesionale:** • analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluții consacrate, asigurând astfel îndeplinirea sarcinilor profesionale; **Familiarizarea cu rolurile şi activităţile specifice muncii în echipă:** • definirea activităților pe etape și repartizarea acestora membrilor echipei, având grijă să fie precizate și explicate îndatoririle, în funcție de nivelul de acces la informație și de poziție în structura funcțională a temelor; • asigurarea unui feed-back eficient de informații și promovarea unui sistem de comunicare în scopul propriu-zis de comunicare astfel încât interlocutorul să fie influenţat şi în același timp (în funcție de necesități) să își schimbe comportamentul; **Conştientizarea nevoii de formare continuă:**

	• adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare tipărite, software specializat și resurse electronice în limba româna și, cel puțin, într-o limbă de circulație internațională; • implicarea în activităţi ştiinţifice de cercetare, de participare la elaborarea unor articole şi studii de specialitate.

6.2. Rezultatele învățării

Cunoștințe	Studentul cunoaște: - cele mai bune mecanisme de securitate care pot fi implementate în cadrul rețelelor de comunicații mobile și wireless; - cunoaște algoritmii de codificare cei mai des folosiți în: compresia datelor, codarea de canal a datelor, criptografie precum și cele mai importante protocoale din cadrul rețelelor comunicații mobile și wireless care implementează acești algoritmi.
Aptitudini	Studentul este capabil: - să identifice posibilele probleme de securitate în sistemele de comunicații și în rețelele comunicații mobile și wireless, vulnerabilitățile și riscurile de securitate; - să proiecteze și să implementeze instrumente de verificare a securității sistemelor de comunicații mobile și wireless.
Responsabilitate și autonomie	Studentul are capacitatea de a înțelege: - conceptele fundamentale de administrare de sistem tehnic de comunicații mobile și wireless și de rețea specifică; - aspectele de securitate conexe acestui proces; - își asumă responsabilitatea pentru produsul muncii sale, solicită feedback și îl utilizează constructiv.

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

7.1 Obiectivul general al disciplinei	• dezvoltarea de competenţe profesionale în domeniul securității informaţiei din reţelele de comunicaţii mobile si wireless.
7.2 Obiectivele specifice	• asimilarea cunoştinţelor teoretice privind proiectarea şi simularea funcţionării blocurilor de prelucrare a informaţiei din sistemele de comunicaţii mobile si wireless; • utilizarea programelor de simulare moderne (CRYPTOOL, etc.); • obţinerea deprinderilor şi abilităţilor necesare pentru testarea performanţelor algoritmilor de secretizare informațională.

8. Conţinuturi

8. 1 Curs	Metode de predare	Observații

		(nr. de ore față în față/online afectate respectivei teme)
1. Noțiuni generale privitoare la securitatea rețelelor wireless (2c);	Interactiva	(2/0) h
2. Principii și metode de secretizare a informațiilor în rețele wireless (2c);	Interactiva	(2/0) h
3. Algoritmi de criptare utilizați în rețelele wireless (4c);	Interactiva	(0/4) h
4. Cerințe de bază pentru algoritmii de criptare utilizați în rețelele WLAN; WPAN; ad-hoc (2c);	Interactiva	(2/0) h
5. Reţele de comunicaţii wireless. Reţele LAN wireless. Managementul securităţii reţelelor wireless (WLAN). Rețele wireless Ad-hoc. Managementul securităţii reţelelor wireless ad-hoc. Dispozitive handheld. Managementul securităţii dispozitivelor handheld. Ameninţări şi vulnerabilităţi. Practici curente (best practices) în securitatea rețelelor WIFI. (6c).	Interactiva	(2/4)h
6. Reţele de comunicaţii mobile. Tipuri de reţele mobile; Arhitectura sistemelor de comunicaţii mobile; Securitatea accesului si serviciilor in rețelele 2G: identități, elemente de rețea, algoritmi, proceduri; Securitatea accesului si serviciilor in retelele 3G pe baza de USIM: code management, algoritmi, proceduri, analiza comparativa 2G vs. 3G; Securitatea accesului la serviciile multimedia IMS: identitati, elemente de retea, proceduri; Securitatea accesului si serviciilor in retelele 4G – LTE. Ameninţări şi vulnerabilităţi. Atacuri de tip malware pe terminalele mobile; Standarde de securitate uzuale în practica operatorilor de rețea; (6c)	Interactiva	(2/4) h
7. Managementul protecției informațiilor în sistemele de comunicații mobile si wireless; (4c).	Interactiva	(0/4) h
8. Digitalizare si profesii emergente ale viitorului (2c).	Interactiva	(2/0) h

Bibliografie

1. Cristian-Gabriel Apostol, Ciprian Răcuciu, Securitatea sistemelor de radiocomunicații, Ciprian Răcuciu, (coord.), Editura Economică, 2018, ISBN 978-973-709-837-5.
2. Ciprian Răcuciu, Marius Rogobete, Madlena Nen, Criptografie şi securitatea informaţiei. Curs pentru învăţământ la distanţă – Bucureşti, Editura Academiei Tehnice Militare, 2016. ISBN 978-973-640-255-5.
3. Ciprian Răcuciu, Dan Grecu, Criptografie si securitatea informaţiei, Editura Renaissance, Bucureşti, 2010, ISBN 978-606-8321-89-9.
4. Ciprian Răcuciu, Dan-Laurenţiu Grecu, Metode şi sisteme criptografice secvenţiale, Editura ERICOM, Bucureşti, 2008, ISBN(13) 978-973-88290-9-1.

5. Roger J. Sutton, “Secure Communications”, Applications and Management, John Wiley & Sons, 2000. 6. Roger Anderson, “Security Engineering – A guide to building dependable distributed systems”, John Wiley & Sons, 2001.		
8. 2 Seminar/ Laborator	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
1. Noțiuni generale privitoare la securitatea rețelelor wireless; (2s)	Interactiva	(2/0) h
2. Principii și metode de secretizare a informațiilor în rețele wireless; (2s)	Interactiva	(2/0) h
3. Algoritmi de criptare utilizați în rețelele wireless; (4s)	Interactiva	(2/2) h
4. Cerințe de bază pentru algoritmii de criptare utilizați în rețelele WLAN; WPAN; ad-hoc; (2s)	Interactiva	(2/0) h
5. Reţele de comunicaţii wireless. Reţele LAN wireless. Managementul securităţii reţelelor wireless (WLAN). Reţele wireless Ad-hoc. Managementul securităţii reţelelor wireless ad-hoc. Dispozitive handheld. Managementul securităţii dispozitivelor handheld. Ameninţări şi vulnerabilităţi. Practici curente (best practices) în securitatea rețelelor WIFI; (6s)	Interactiva	(4/2)h
6. Reţele de comunicaţii mobile. Tipuri de reţele mobile; Arhitectura sistemelor de comunicaţii mobile; Securitatea accesului si serviciilor in rețelele 2G; Securitatea accesului si serviciilor in rețelele 3G, analiza comparativa 2G vs. 3G; Securitatea accesului la serviciile multimedia IMS; Securitatea accesului si serviciilor în rețelele 4G–LTE. Ameninţări şi vulnerabilităţi. Atacuri de tip malware pe terminalele mobile; Standarde de securitate uzuale în practica operatorilor de rețea; (8s)	Interactiva	(6/2) h
7. Managementul protecției informațiilor în sistemele de comunicații mobile si wireless. (4s)	Interactiva	(2/2) h
Bibliografie 1. Cristian-Gabriel Apostol, Ciprian Răcuciu, Securitatea sistemelor de radiocomunicații, Ciprian Răcuciu, (coord.), Editura Economică, 2018, ISBN 978-973-709-837-5. 2. Roger J. Sutton, “Secure Communications”, Applications and Management, John Wiley & Sons, 2000.		

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

- Adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare tipărite, software specializat și resurse electronice în limba româna și, cel puțin, într-o limbă de circulație internațională;
- Implicarea în activităţi ştiinţifice de cercetare, de participare la elaborarea unor articole şi studii de specialitate, de implicare în activitățile cercurilor științifice studențești.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Răspunsuri la teste şi examen	Examen	60 %
	Aprecierea interesului şi activităţii la cursuri	Teste pe parcursul semestrului	10%
10.5 Seminar/ Laborator	Aprecierea activităţilor aplicative	Colocviu de laborator; Dezbateri	5%
	Aprecierea lucrărilor practice	Proiect	25%
10.6. Standard minim de performanţă			
• Promovarea examenului cu nota minimă 5 şi realizarea lucrărilor practice solicitate.			

Data completării | Semnătura titularului de curs | Semnătura titularului de seminar/ laborator

25.09.2025 | ..... | .....

Data avizării în departament | Semnătura directorului de departament

26.09.2025 | Conf. univ. dr. ing. Tudor Cătălin APOSTOLESCU

FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	UNIVERSITATEA TITU MAIORESCU
1.2. Facultatea	INFORMATICĂ
1.3. Departamentul	INFORMATICĂ
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Masterat
1.6. Programul de studii/ Calificarea/ Specializarea	SECURITATEA SISTEMELOR INFORMATICE ŞI A REŢELELOR INFORMAŢIONALE
1.7. Limba de studiu	Română

2. Date despre disciplină

2.1 Denumirea disciplinei			**Practică de specialitate II**				
2.2 Titularul/titularii activităţilor de curs			Conf. univ. dr. ing. Apostolescu Tudor Cătălin				
2.3 Titularul/titularii activităţilor de seminar/laborator			Conf. univ. dr. ing. Apostolescu Tudor Cătălin				
2.4 Anul de studiu	**I**	2.5 Semestrul	**4**	2.6 Tipul de evaluare	**V**	2.7 Regimul disciplinei	**APR**

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs		3.3 seminar/ laborator	
3.4 Total ore din planul de învăţământ/ Total ore online din planul de învățământ	56	din care: 3.5 curs - față în față - online		3.6 seminar/ laborator - față în față - online	

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie și notițe	
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	
Tutoriat	
Examinări	
Alte activităţi:	34

3.7. Total ore studiu individual	34
3.8. Total ore de studiu pe semestru	90
3.9 Numărul de credite	**3**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Însușirea cunoștințelor predate la disciplinele de specialitate aferente programului de master urmat
4.2 de competențe	• Capacitatea de a evalua teoretic și cantitativ probleme specifice

	domeniului Securitatea sistemelor informatice şi a reţelelor informaţionale

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Cu fiecare student se va încheia o Convenție – cadru de practică între Universitate și partener de practică.
5.2. de desfășurare a seminarului/laboratorului	• Toate activitățile de practică se vor desfășura la sediul firmelor partenere și/sau în Centrele de cercetare ale facultății: Centrul Academic de Inteligență Articifială AI#Connect, Centrul de excelență în securitate cibernetică CyberX în cloud, Laborator virtual de practică pentru testare software; prezența este obligatorie la toate activitățile de practică.

6. Competenţele specifice acumulate

Competenţe profesionale	• Capacitatea de a rezolva probleme de securitate prin aplicarea metodelor și tehnicilor specifice securității rețelelor de comunicații, sistemelor mobile și infrastructurilor cibernetice. • Integrarea și prezentarea corectă a informațiilor și procedurilor privind securizarea aplicațiilor web, protecția datelor și investigarea incidentelor digitale. • Analiza și interpretarea datelor tehnice pentru evaluarea riscurilor, identificarea vulnerabilităților și detectarea comportamentelor malițioase în sisteme, rețele și aplicații. • Utilizarea și configurarea mecanismelor de securitate aplicate în rețele fixe și mobile, în aplicații web, precum și în procesele de monitorizare și răspuns la atacuri cibernetice. • Aplicarea tehnicilor de testare și evaluare a fiabilității sistemelor de calcul, inclusiv testarea securității, analiza performanțelor și verificarea integrității datelor. • Gestionarea securității cibernetice la nivel organizațional, prin definirea strategiilor, politicilor și procedurilor de protecție și răspuns la incidente. • Aplicarea metodelor de colectare și investigare a probelor digitale (Digital Forensics) în scopul identificării atacatorilor și reconstituirii evenimentelor cibernetice.

Competențe transversale	• Finalizarea sarcinilor și proiectelor la termen, respectând procedurile tehnice, metodologice și cerințele specifice disciplinelor de securitate informatică. • Integrarea eficientă în echipe multidisciplinare, colaborând în activități ce implică securitate cibernetică, analiză digitală, testare și investigare. • Aplicarea responsabilă a cunoștințelor tehnice și științifice, cu respectarea normelor de etică și integritate academică în activitățile profesionale și academice. • Dezvoltarea unei gândiri analitice și critice, necesară pentru evaluarea amenințărilor, detectarea atacurilor și luarea deciziilor corecte în situații de risc. • Formarea unei abordări holistice asupra securității, integrând perspective din comunicații, sisteme mobile, aplicații web, război cibernetic și forensics.

6.2. Rezultatele învățării

Cunoștințe	• Masterandul cunoaște conceptele și mecanismele fundamentale privind securitatea rețelelor de comunicații, securitatea aplicațiilor web și protecția infrastructurilor mobile și wireless. • Masterandul recunoaște, explică și argumentează tehnici de securitate cibernetică, inclusiv metode de atac și apărare utilizate în contexte de război cibernetic. • Masterandul înțelege principiile fiabilității și testării sistemelor de calcul, precum și modul în care acestea contribuie la reziliența și continuitatea infrastructurilor informatice. • Masterandul cunoaște procedurile specifice de criminalitate informatică și Digital Forensics, inclusiv colectarea, conservarea și analiza probelor digitale. • Masterandul înțelege importanța eticii și integrității academice, precum și responsabilitățile profesionale asociate activităților din domeniul securității cibernetice.
Aptitudini	• Masterandul poate lucra în echipă și poate coordona activități de identificare, testare și evaluare a riscurilor de securitate în rețele, aplicații web, sisteme mobile și infrastructuri informatice. • Masterandul poate desfășura activități de testare, auditare și evaluare a securității rețelelor de comunicații, sistemelor de calcul și aplicațiilor web, utilizând unelte și metode specifice. • Masterandul are capabilitatea de a integra și utiliza în practică conceptele studiate, aplicând corect protocoale de securitate, proceduri de testare, tehnici de analiză a traficului și metode de investigare digitală. • Masterandul poate utiliza tehnici și instrumente de Digital Forensics pentru identificarea incidentelor, analiza probelor și reconstituirea evenimentelor cibernetice.

Responsabilitate și autonomie	• Masterandul poate aplica în mod autonom și responsabil cunoștințele dobândite în domeniile securității cibernetice, rețelelor, aplicațiilor web, sistemelor wireless și investigațiilor digitale. • Poate prelua responsabilitatea evaluării și îmbunătățirii nivelului de securitate al infrastructurilor informatice, aplicațiilor și sistemelor analizate. • Își asumă responsabilități profesionale, respectă principiile de etică și integritate și colaborează eficient cu membrii echipei în activități de analiză, testare și intervenție în caz de incidente. • Demonstrează autonomie, profesionalism și inițiativă în aplicarea tehnicilor de securitate la situații complexe, inclusiv în scenarii de război cibernetic sau incidente majore.

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

7.1 Obiectivul general al disciplinei	Dezvoltarea capacității masterandului de a analiza, proiecta, implementa și evalua soluții avansate de securitate informatică și reziliență cibernetică, prin integrarea cunoștințelor acumulate în domeniile: securitatea rețelelor de comunicații, securitatea aplicațiilor web, securitatea rețelelor mobile și wireless, fiabilitatea și testarea sistemelor de calcul, securitate cibernetică ofensivă și defensivă, criminalitate informatică și investigații digitale, precum și etică și integritate academică.
7.2 Obiectivele specifice	• Înțelegerea principiilor, mecanismelor și protocoalelor de securitate utilizate în rețele de comunicații, inclusiv în infrastructuri mobile și wireless, precum și evaluarea riscurilor specifice acestor medii. • Dezvoltarea competențelor de identificare, analiză, exploatare controlată și remediere a vulnerabilităților din aplicații web, sisteme software și infrastructuri informatice, utilizând metode și instrumente moderne de testare și audit. • Formarea abilităților de proiectare și implementare a mecanismelor de fiabilitate, testare și validare în sisteme de calcul, în vederea creșterii rezilienței și disponibilității infrastructurilor IT. • Înțelegerea conceptelor, tehnicilor și strategiilor asociate războiului cibernetic, atacurilor avansate și apărării cibernetice, cu accent pe analiză, prevenție și reacție la incidente. • Dobândirea competențelor de aplicare a tehnicilor de Digital Forensics și investigare a criminalității informatice, inclusiv colectarea, conservarea și analiza probelor digitale. • Utilizarea corectă a mecanismelor de securizare a datelor și documentelor electronice (autentificare, autorizare, auditare, criptare, semnături electronice, certificate digitale, infrastructuri PKI). • Aplicarea standardelor și principiilor de etică

	profesională, integritate academică și responsabilitate în activitățile de cercetare și dezvoltare în domeniul securității cibernetice. • Redactarea unui raport tehnic complex și prezentarea orală a rezultatelor, argumentând soluțiile propuse și fundamentând deciziile tehnice pe baza cunoștințelor teoretice și practice dobândite.

8. Conţinuturi

8 Seminar/ Laborator	Metode de predare	Observații
1. Aplicații practice privind implementarea și testarea algoritmilor criptografici, generarea și gestionarea cheilor, evaluarea securității schemelor de criptare, precum și utilizarea funcțiilor hash pentru protecția datelor în sisteme informatice și comunicații.	Laborator practic bazat pe scenarii	
2. Aplicații practice axate pe configurarea și evaluarea protocoalelor de securitate în rețele de comunicații, inclusiv implementarea firewall-urilor, utilizarea sistemelor IDS/IPS, identificarea vulnerabilităților și analiza atacurilor asupra infrastructurilor fixe, mobile și wireless.	Laborator practic bazat pe scenarii	
3. Aplicații practice dedicate elaborării unui studiu științific în domeniul securității cibernetice, cu accent pe formularea ipotezelor, proiectarea experimentelor, colectarea și interpretarea datelor, redactarea academică și respectarea normelor de etică și integritate..	Laborator practic bazat pe scenarii	
4. Aplicații practice privind securitatea aplicațiilor web, incluzând identificarea și exploatarea controlată a vulnerabilităților (SQLi, XSS, CSRF etc.), configurarea mecanismelor de autentificare și autorizare, protecția sesiunilor, analiza traficului HTTP/HTTPS și utilizarea instrumentelor de testare a aplicațiilor web.	Laborator practic bazat pe scenarii	
5. Aplicații practice orientate pe securitatea mediilor cloud, vizând configurarea serviciilor cloud sigure, gestionarea accesului, criptarea datelor în tranzit și în repaus, monitorizarea și testarea securității infrastructurilor cloud.	Laborator practic bazat pe scenarii	
6. Aplicații practice în domeniul criminalității informatice și Digital Forensics, incluzând colectarea, conservarea, examinarea și interpretarea probelor digitale, precum și analiza incidentelor cibernetice în contextul tehnicilor și strategiilor asociate războiului	Laborator practic bazat pe scenarii	

cibernetic.		

Bibliografie
Referințele bilbiografice recomandate de coordonatorul activității de practică sau tutore în concordanță cu tema aleasă

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

- Conținutul și obiectivele disciplinei sunt corelate cu cerințele actuale pe piața muncii; sunt urmărite atât aspectele practice cât și responsabilizarea studenților în domeniul cercetării științifice. Studenții sunt încurajați pentru obținerea de atestări a cunoștințelor, prin materiale și asistență, acestea fiind benefice atât pentru corelarea abilităților practice recunoscute pentru studenți cu elementele teoretice și reprezintă un element esențial pentru integrare studenților pe piața muncii.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.5 Stagiu de practică	• Prezență • Grad de implicare a studentului • Activitatea în stagiul de practică • Caiet de practică	Colocviu de practică	10 % 20% 30% 40 %
10.6. Standard minim de performanţă			
• Pentru promovare este necesară obținerea notei 5 (cinci). Prezență obligatorie.			

Data completării
25.09.2025
.....

Semnătura titularului de curs
.....

Semnătura titularului de seminar/ laborator
.....

Data avizării în departament
26.09.2025
.....

Semnătura directorului de departament
.....

FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	UNIVERSITATEA TITU MAIORESCU
1.2. Facultatea	INFORMATICĂ
1.3. Departamentul	INFORMATICĂ
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Masterat
1.6. Programul de studii/ Calificarea/ Specializarea	SECURITATEA SISTEMELOR INFORMATICE ŞI A REŢELELOR INFORMAŢIONALE
1.7. Limba de studiu	Română

2. Date despre disciplină

2.1 Denumirea disciplinei			**PROTECȚIA DATELOR CU CARACTER PERSONAL (GDPR)**				
2.2 Titularul/titularii activităţilor de curs			**Conf. Univ. Dr. Ing. IUSTIN PRIESCU**				
2.3 Titularul/titularii activităţilor de seminar/laborator			**Conf. Univ. Dr. Ing. IUSTIN PRIESCU**				
2.4 Anul de studiu	**II**	2.5 Semestrul	4	2.6 Tipul de evaluare	**examen**	2.7 Regimul disciplinei	**SINT**

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 seminar/ laborator	**2**
3.4 Total ore din planul de învăţământ/ Total ore online din planul de învăţământ	56 / 24	din care: 3.5 curs - față în față online	28/ 12/ 16	3.6 seminar/ laborator - față în față online	28/ 20/ 8

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie și notițe	70
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	38
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri	34
Tutoriat	8
Examinări	4
Alte activităţi:	

3.7. Total ore studiu individual	**154**
3.8. Total ore de studiu pe semestru	**210**
3.9 Numărul de credite	**7**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Securitatea rețelelor de calculatoare • Securitatea rețelelor de comunicații
4.2 de competențe	• Programare în diferite limbaje și medii • Implementarea algoritmilor simetrici și asimetrici

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Prelegerile se desfășoară în săli dotate cu echipament • de predare multimedia
5.2. de desfășurare a seminarului/laboratorului	• Masteranzii se vor prezenta la laborator cu materia aferentă cursului anterior parcursă și cu temele rezolvate • Laboratoarele se vor desfășura cu software licențiat instalat pe serverul facultății sau pe laptop-ul propriu

6. Competenţele specifice acumulate

Competențe profesionale	**Cunoaştere şi înţelegere:** • cunoașterea noțiunilor specifice din domeniul protecției datelor cu caracter personal (DCP), precum și a legislației naționale și UE; • înţelegerea structurii şi elementelor componente ale Regulamentului GDPR; • înţelegerea necesității protejării DCP la nivel național și UE. **Utilizarea cunoștințelor:** • implementarea de mecanisme care sa asigure protecția DCP; • interpretarea unor noțiuni utilizate în domeniul protecției DCP; **Aplicarea unor principii și metode de bază pentru rezolvarea de probleme tipice domeniului:** • corelarea cunoştinţelor teoretice cu abilitatea de a le aplica în practică; • întocmirea algoritmilor criptografici şi implementarea acestora; • aplicarea modelelor de analiză și sinteză în rezolvarea unor probleme specifice. **Utilizarea adecvată de criterii și metode standard de evaluare pentru a aprecia calitatea, meritele și limitele unor procese, programe, proiecte, concepte, metode și teorii**: • utilizarea instrumentelor software dedicate, matematice, statistice, si a metodelor specifice pentru a caracteriza și evalua asigurarea protecției DCP. **Elaborarea de proiecte profesionale cu utilizarea unor principii și metode consacrate în domeniu:** • înţelegerea importanţei domeniului protecției DCP aplicate la nivel național și UE; • înţelegerea necesității funcționării în ansamblu a structurilor care raspund și asigură protecția DCP; • proiectarea și implementarea unor aplicații specifice protecției DCP.
Competențe transversale	**Executarea responsabilă a sarcinilor profesionale:** • analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluții consacrate, asigurând astfel îndeplinirea sarcinilor profesionale; **Familiarizarea cu rolurile şi activităţile specifice muncii în echipă:** • definirea activităților pe etape și repartizarea acestora membrilor echipei, având grijă să fie precizate și explicate îndatoririle, în funcție de nivelul de acces la informație și de poziție în structura funcțională a temelor; • asigurarea unui feed-back eficient de informații și promovarea unui sistem de comunicare în scopul propriu-zis de comunicare astfel încât interlocutorul să fie influenţat şi în același timp (în funcție de necesități) să își schimbe comportamentul; **Conştientizarea nevoii de formare continuă:** • adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare electronice, software specializat și resurse electronice în limba engleză;

	• implicarea în activităţi ştiinţifice de cercetare, de participare la elaborarea unor articole şi studii de specialitate.

6.2. Rezultatele învățării

Cunoștințe	• Masterandul înțelege conceptele fundamentale privind datele cu caracter personal, principiile GDPR și legislația națională și europeană aplicabilă. • Masterandul cunoaște rolurile actorilor implicați în protecția datelor (operator, persoană împuternicită, DPO) și responsabilitățile acestora. • Masterandul identifică mecanismele, procedurile și cerințele necesare pentru asigurarea securității și legalității prelucrării datelor personale.
Aptitudini	• Masterandul aplică metode și tehnici pentru implementarea protecției datelor, inclusiv evaluări de risc, DPIA și măsuri de securitate. • Masterandul utilizează instrumente software și proceduri specifice pentru auditarea și monitorizarea prelucrării datelor personale. • Masterandul elaborează documente specifice GDPR: evidențe de prelucrare, politici, proceduri, notificări și documentație aferentă proiectelor.
Responsabilitate și autonomie	• Masterandul respectă standardele de etică, confidențialitate și protecție a vieții private în activitățile profesionale. • Masterandul își asumă responsabilitatea pentru aplicarea corectă a cerințelor GDPR în contexte practice și organizaționale. • Masterandul colaborează eficient în echipă și contribuie la gestionarea conformității, adaptându-se continuu la noile reglementări și tehnologii din domeniu.

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

7.1 Obiectivul general al disciplinei	• dezvoltarea de competenţe profesionale în domeniul protecției DCP.
7.2 Obiectivele specifice	• asimilarea cunoştinţelor practice privind protecția DCP; • utilizarea programelor de testare și auditare a protecției DCP (KALI LINUX etc.); • obţinerea deprinderilor şi abilităţilor necesare pentru efectuarea de auditări privind asigurarea protecției DCP

8. Conţinuturi

8. 1 Curs	Metode de predare	Observații

		(nr. de ore față în față/online afectate respectivei teme)
1. Conceptul de "Date cu Caracter Personal (DCP)" • Domeniul de aplicare material și teritorial al GDPR • Concepte si definiții specifice protecției DCP (cf. Art. 4 GDPR) • Principii legate de prelucrarea datelor cu caracter personal și legalitatea prelucrării DCP • Prelucrarea de categorii speciale de date cu caracter personal • Condiţii privind consimţământul • Drepturile persoanei vizate • Procesul decizional individual automatizat, inclusiv crearea de profiluri	Curs interactiv	8 ore curs online
2. Operatorul şi persoana împuternicită de operator • Responsabilitatea operatorului • Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit • Operatori asociaţi • Persoana împuternicită de operator • Evidenţele activităţilor de prelucrare • Cooperarea cu autoritatea de supraveghere	Curs interactiv	6 ore curs față în față
3**. Securitatea datelor cu caracter personal** • Securitatea prelucrării • Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal • Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal • Evaluarea impactului asupra protecţiei datelor şi consultarea prealabilă	Curs interactiv	8 ore curs online
4. **Responsabilul cu protecţia datelor** • Desemnarea responsabilului cu protecţia datelor • Funcţia responsabilului cu protecţia datelor • Sarcinile responsabilului cu protecţia datelor • Coduri de conduită şi certificare • Transferurile de date cu caracter personal către ţări terţe sau organizaţii internaţionale • Autoritatea de supraveghere • Comitetul european pentru protecţia datelor • Dispoziţii referitoare la situaţii specifice de prelucrare	Curs interactiv	6 ore curs față în față
Bibliografie		

- ***, Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), 2018
- ***, Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)
- ***, Ghidul privind consimțământul în temeiul Regulamentului (UE) 2016/679, 2017
- ***, Ghidul privind deciziile automate individuale și profilare, 2017
- ***, Ghidul privind evaluarea de impact al Grupului de Lucru art. 29, 2017
- ***, Ghidul privind responsabilul pentru protecția datelor (DPO), raportat la art. 37-39 din RGDP, 2017
- Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, www.dataprotection.ro, 2018
- ***, *Latest Kali Linux News and Tutorials,* https://www.kali.org/, 2018

8. 1 Seminar/ Laborator	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
1. Conceptul de "Date cu Caracter Personal (DCP)" • Domeniul de aplicare material și teritorial al GDPR • Concepte si definiții specifice protecției DCP (cf. Art. 4 GDPR) • Principii legate de prelucrarea datelor cu caracter personal și legalitatea prelucrării DCP • Prelucrarea de categorii speciale de date cu caracter personal • Condiţii privind consimţământul • Drepturile persoanei vizate • Procesul decizional individual automatizat, inclusiv crearea de profiluri	Laborator de tip hands-on	8 ore online
2. Operatorul şi persoana împuternicită de operator • Responsabilitatea operatorului • Asigurarea protecţiei datelor începând cu momentul conceperii şi în mod implicit • Operatori asociaţi • Persoana împuternicită de operator • Evidenţele activităţilor de prelucrare • Cooperarea cu autoritatea de supraveghere	Laborator de tip hands-on	6 ore față în față
3.Securitatea datelor cu caracter personal • Securitatea prelucrării • Notificarea autorităţii de supraveghere în cazul încălcării securităţii datelor cu caracter personal • Informarea persoanei vizate cu privire la încălcarea securităţii datelor cu caracter personal • Evaluarea impactului asupra protecţiei datelor şi consultarea prealabilă	Laborator de tip hands-on	8 față în față

4. Responsabilul cu protecţia datelor • Desemnarea responsabilului cu protecţia datelor • Funcţia responsabilului cu protecţia datelor • Sarcinile responsabilului cu protecţia datelor • Coduri de conduită şi certificare • Transferurile de date cu caracter personal către ţări terţe sau organizaţii internaţionale • Autoritatea de supraveghere • Comitetul european pentru protecţia datelor Dispoziţii referitoare la situaţii specifice de prelucrare	Laborator de tip hands-on	6 față în față

Bibliografie

- ***, Regulamentul (UE) 2016/679 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor), 2018
- ***, Legea nr. 190 din 18 iulie 2018 privind măsuri de punere în aplicare a Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date şi de abrogare a Directivei 95/46/CE (Regulamentul general privind protecţia datelor)
- ***, Ghidul privind consimțământul în temeiul Regulamentului (UE) 2016/679, 2017
- ***, Ghidul privind deciziile automate individuale și profilare, 2017
- ***, Ghidul privind evaluarea de impact al Grupului de Lucru art. 29, 2017
- ***, Ghidul privind responsabilul pentru protecția datelor (DPO), raportat la art. 37-39 din RGDP, 2017
- Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, www.dataprotection.ro, 2018
- ***, *Latest Kali Linux News and Tutorials,* https://www.kali.org/, 2018

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

- Adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare tipărite, software specializat și resurse electronice în limba engleză;
- Implicarea în activităţi ştiinţifice de cercetare, de participare la elaborarea unor articole şi studii de specialitate, de implicare în activitățile cercurilor științifice studențești.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală

10.4 Curs	Răspunsuri la teste si examen	Examen	60 %
	Aprecierea interesului şi activității la cursuri	Teste pe parcursul semestrului	10%
10.5 Seminar/ Laborator	Aprecierea activităţilor aplicative	Aplicații de laborator; Prezentarrea lucrărilor	5%
	Aprecierea lucrărilor practice	Proiect	25%
10.6. Standard minim de performanţă			
• Promovarea examenului cu nota minimă 5 şi realizarea lucrărilor practice solicitate.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar/ laborator
25.09.2025		
.....	.....	.....

Data avizării în departament

Semnătura directorului de departament

26.09.2025 .....

.....

FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	UNIVERSITATEA TITU MAIORESCU
1.2. Facultatea	INFORMATICĂ
1.3. Departamentul	INFORMATICĂ
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Masterat
1.6. Programul de studii/ Calificarea/ Specializarea	SECURITATEA SISTEMELOR INFORMATICE ŞI A REŢELELOR INFORMAŢIONALE
1.7. Limba de studiu	Română

2. Date despre disciplină

2.1 Denumirea disciplinei			**CRIMINALITATEA INFORMATICĂ, COLECTAREA ŞI INVESTIGAREA PROBELOR (DIGITAL FORENSICS)**				
2.2 Titularul/titularii activităţilor de curs			**Conf. Univ. Dr. Ing. IUSTIN PRIESCU**				
2.3 Titularul/titularii activităţilor de seminar/laborator			**Conf. Univ. Dr. Ing. IUSTIN PRIESCU**				
2.4 Anul de studiu	**II**	2.5 Semestrul	3	2.6 Tipul de evaluare	**examen**	2.7 Regimul disciplinei	**SINT**

3. Timpul total estimat (ore pe semestru al activităţilor didactice)

3.1 Număr de ore pe săptămână	**4**	din care: 3.2 curs	**2**	3.3 seminar/ laborator	**2**
3.4 Total ore din planul de învăţământ/ Total ore online din planul de învăţământ	56 / 24	din care: 3.5 curs - față în față online	28/ 12/ 16	3.6 seminar/ laborator - față în față online	28/ 20/ 8
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie și notițe					70
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					38
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					34
Tutoriat					8
Examinări					4
Alte activităţi:					
3.7. Total ore studiu individual	**184**				
3.8. Total ore de studiu pe semestru	**240**				
3.9 Numărul de credite	**8**				

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	• Securitatea rețelelor de calculatoare • Securitatea rețelelor de comunicații
4.2 de competențe	• Programare în diferite limbaje și medii • Implementarea algoritmilor simetrici și asimetrici

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	• Prelegerile se desfășoară în săli dotate cu echipament • de predare multimedia
5.2. de desfășurare a seminarului/laboratorului	• Masteranzii se vor prezenta la laborator cu materia aferentă cursului anterior parcursă și cu temele rezolvate • Laboratoarele se vor desfășura cu software licențiat instalat pe serverul facultății sau pe laptop-ul propriu

6. Competenţele specifice acumulate

Competenţe profesionale	**Cunoaştere şi înţelegere:** • cunoaşterea noţiunilor specifice din domeniul criminalității informatice aplicate în IT&C; • înţelegerea structurii şi elementelor din domeniul criminalității informatice; • înţelegerea procesului de investigare și colectarea de probe. **Utilizarea cunoștințelor:** • Colectarea de artefacte si analiza acestora; • interpretarea unor noţiuni utilizate în domeniul criminalității informatice; **Aplicarea unor principii și metode de bază pentru rezolvarea de probleme tipice domeniului:** • corelarea cunoştinţelor teoretice cu abilitatea de a le aplica în practică; • întocmirea algoritmilor criptografici şi implementarea acestora; • aplicarea modelelor de analiză și sinteză în rezolvarea unor probleme specifice. **Utilizarea adecvată de criterii și metode standard de evaluare pentru a aprecia calitatea, meritele și limitele unor procese, programe, proiecte, concepte, metode și teorii**: • utilizarea instrumentelor software dedicate, matematice, statistice, si a metodelor specifice pentru a caracteriza și evalua colectarea probelor, analiza și raportarea; **Elaborarea de proiecte profesionale cu utilizarea unor principii și metode consacrate în domeniu:** • înţelegerea importanţei domeniului criminalității informtica aplicate în cadrul IT&C; • înțelegerea necesității cunoașterii domeniului de criminalitate informatică; • proiectarea și implementarea unor aplicații specifice criminalității informatice.
Competenţe transversale	**Executarea responsabilă a sarcinilor profesionale:** • analiza metodică a problemelor întâlnite în activitate, identificând elementele pentru care există soluții consacrate, asigurând astfel îndeplinirea sarcinilor profesionale; **Familiarizarea cu rolurile şi activităţile specifice muncii în echipă:** • definirea activităților pe etape și repartizarea acestora membrilor echipei, având grijă să fie precizate și explicate îndatoririle, în funcție de nivelul de acces la informație și de poziție în structura funcțională a temelor; • asigurarea unui feed-back eficient de informații și promovarea unui sistem de comunicare în scopul propriu-zis de comunicare astfel încât interlocutorul să fie influenţat şi în același timp (în funcție de necesități) să își schimbe comportamentul; **Conştientizarea nevoii de formare continuă:** • adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare electronice, software specializat și resurse electronice în limba engleză; • implicarea în activităţi ştiinţifice de cercetare, de participare la elaborarea unor articole şi studii de specialitate.

6.2. Rezultatele învățării

Cunoștințe	• Masterandul înțelege conceptele fundamentale ale criminalității informatice și etapele procesului de investigare digitală. • Masterandul cunoaște metodele, tehnicile și procedurile de colectare, analiză și interpretare a probelor informatice din sisteme Windows, Linux, mobile și rețele. • Masterandul identifică instrumentele utilizate în digital forensics și principiile de securizare, auditare și raportare a probelor digitale.
Aptitudini	• Masterandul aplică tehnici specializate de investigare digitală, colectare de artefacte și analiză a evidențelor digitale. • Masterandul utilizează instrumente software dedicate (Kali Linux, tool-uri de analiză, utilitare forensice) pentru examinarea și interpretarea probelor. • Masterandul elaborează rapoarte tehnice, documente de analiză și proiecte specifice criminalității informatice și investigării incidentelor.
Responsabilitate și autonomie	• Masterandul respectă normele etice și legale în gestionarea probelor digitale și în desfășurarea investigațiilor informatice. • Masterandul își asumă responsabilitatea în realizarea sarcinilor de colectare, analiză și raportare a probelor, respectând integritatea și confidențialitatea datelor. • Masterandul colaborează eficient în echipe de investigație, se adaptează noilor tehnologii și își dezvoltă continuu competențele profesionale.

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

7.1 Obiectivul general al disciplinei	• dezvoltarea de competenţe profesionale în domeniul criminalității informatice, colectării și inestigării probelor
7.2 Obiectivele specifice	• asimilarea cunoştinţelor practice privind colectarea, investigarea și administrarea de probe • utilizarea programelor de testare și auditare a securității informației (KALI LINUX, Xray etc.); • obţinerea deprinderilor şi abilităţilor necesare pentru efectuarea de investigații informatice

8. Conţinuturi

8. 1 Curs	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
1. Introducere în criminalitatea informatica (Digital Forensics) • Concepte și definiții specifice domeniului criminalitate informatică	Curs interactiv	6 ore curs online

• Pregătirea pentru efectuarea de investigații digitale • Proceduri pentru efectuarea de investigații digitale • Efectuarea unei investigații criminale informatice • Labolator de investigații criminale digitale și acreditările necesare		
2. Colectarea, analiza, interpretarea și raportarea probelor informatice • Metode de colectare și analiză a probelor în sisteme Windows • Metode de colectare și analiză a probelor în sisteme Linux • Metode de colectarea și analiza a probelor în sisteme mobile (Android și iOS) • Securizarea probelor obținute • Tehnici de audit pentru securitatea sistemelor informatice • Tool-uri folosite pentru colectarea, analiza și interpretarea probelor informatice	Curs interactiv	12 ore curs față în față
3. Investigatii criminale complete pentru: • Rețele de calculatoare și mașini virtuale • Rețele de socializare și sisteme email • Telefoane mobile și tablete • Cloud computing	Curs interactiv	10 ore curs online
Bibliografie • Bill Nelson , Amelia Phillips, Christopher Steuart, *Guide to Computer Forensics and Investigations Processing Digital Evidence*, Ed. 5, Cengage Learning, 2016 • Jason T. Luttgens, Matthew Pepe, *Incident Response - Computer Forensics*, 3rd Edition McGraw-Hill Education, 2014 • Johhny Long, *Google_Hacking for Penetretion Testers*, Syngress Publishing, 2005 • C. McNab, *Network Security Assessment*, O'Reilly Media, 2016 • ***, NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Rev. 4, 2013 • ***, *Latest Kali Linux News and Tutorials,* https://www.kali.org/, 2018		
8. 1 Seminar/ Laborator	Metode de predare	Observații (nr. de ore față în față/online afectate respectivei teme)
1. Introducere în criminalitatea informatica (Digital Forensics) • Concepte și definiții specifice domeniului criminalitate informatică • Pregătirea pentru efectuarea de investigații digitale • Proceduri pentru efectuarea de investigații digitale	Laborator de tip hands-on	8 h online laborator

• Efectuarea unei investigații criminale informatice • Labolator de investigații criminale digitale și acreditările necesare		
2. Colectarea, analiza, interpretarea și raportarea probelor informatice • Metode de colectare și analiză a probelor în sisteme Windows • Metode de colectare și analiză a probelor în sisteme Linux • Metode de colectarea și analiza a probelor în sisteme mobile (Android și iOS) • Securizarea probelor obținute • Tehnici de audit pentru securitatea sistemelor informatice • Tool-uri folosite pentru colectarea, analiza și interpretarea probelor informatice	Laborator de tip hands-on	10 h laborator față în față
3. Investigatii criminale complete pentru: • Rețele de calculatoare și mașini virtuale • Rețele de socializare și sisteme email • Telefoane mobile și tablete • Cloud computing	Laborator de tip hands-on	10 h laborator față în față

Bibliografie

- Bill Nelson , Amelia Phillips, Christopher Steuart, *Guide to Computer Forensics and Investigations Processing Digital Evidence*, Ed. 5, Cengage Learning, 2016
- Jason T. Luttgens, Matthew Pepe, *Incident Response - Computer Forensics*, 3rd Edition McGraw-Hill Education, 2014
- Johhny Long, *Google_Hacking for Penetretion Testers*, Syngress Publishing, 2005
- C. McNab, *Network Security Assessment*, O'Reilly Media, 2016
- ***, NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*, Rev. 4, 2013
- ***, *Latest Kali Linux News and Tutorials,* https://www.kali.org/, 2018

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

- Adaptarea la noile tehnologii, dezvoltarea profesională și personală, prin formare continuă folosind surse de documentare tipărite, software specializat și resurse electronice în limba engleză;
- Implicarea în activităţi ştiinţifice de cercetare, de participare la elaborarea unor articole şi studii de specialitate, de implicare în activitățile cercurilor științifice studențești.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Răspunsuri la teste si examen	Examen	60 %
	Aprecierea interesului şi activității la cursuri	Teste pe parcursul semestrului	10%
10.5 Seminar/ Laborator	Aprecierea activităţilor aplicative	Aplicații de laborator; Prezentarrea lucrărilor	5%
	Aprecierea lucrărilor practice	Proiect	25%
10.6. Standard minim de performanţă			
• Promovarea examenului cu nota minimă 5 şi realizarea lucrărilor practice solicitate.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar/ laborator
25.09.2025		
.....	.....	.....

Data avizării în departament

Semnătura directorului de departament

26.09.2025 .....

.....