

FIȘA DISCIPLINEI

Mediul, formele și particularitățile criminalității informatice

Anul universitar 2025-2026

1. Date despre program

1.1. Instituția de învățământ superior	UNIVERSITATEA „BABEȘ-BOLYAI” din CLUJ-NAPOCA
1.2. Facultatea	DREPT
1.3. Departamentul	DREPT PUBLIC
1.4. Domeniul de studii	DREPT
1.5. Ciclu de studii	DOCTORAT

2. Date despre disciplină

2.1. Denumirea disciplinei		Mediul, formele și particularitățile criminalității informatice				Codul disciplinei	DDR1015
2.2. Titularul activităților de curs			Prof.dr. Ioana Vasiiu				
2.3. Titularul activităților de seminar			Prof.dr. Ioana Vasiiu				
2.4. Anul de studiu	1	2.5. Semestrul	1	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	opțională
2.7. Regimul disciplinei		Optional		2.8. Tipul disciplinei		Disciplină de specializare (DS)	

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

3.1. Număr de ore pe săptămână	3	din care: 3.2. curs	2	3.3. seminar/ laborator/ proiect	1
3.4. Total ore din planul de învățământ	36	din care: 3.5. curs	28	3.6 seminar/laborator	14
Distribuția fondului de timp pentru studiul individual (SI) și activități de autoinstruire (AI)					Ore
Studiul după manual, suport de curs, bibliografie și notițe (AI)					76
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					76
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii și eseuri					55
Tutoriat (consiliere profesională)					
Examinări					1
Alte activități					
3.7. Total ore studiu individual (SI) și activități de autoinstruire (AI)				208	
3.8. Total ore pe semestru				250	
3.9. Numărul de credite				10	

4. Precondiții (acolo unde este cazul)

4.1. de curriculum	-
4.2. de competențe	-

5. Condiții (acolo unde este cazul)

5.1. de desfășurare a cursului	
5.2. de desfășurare a seminarului/ laboratorului	

6. Rezultatele învățării specifice disciplinei

Cunoștințe
1. Cunoaște conceptele, teoriile și modelele avansate din domeniu.

2. Înțelege metodologia științifică aplicată domeniului său.
3. Cunoaște standardele de documentare științifică.
4. Cunoaște structura și rigorile scrierii academice internaționale.
Aptitudini
1. Aplică cunoștințele pentru analiza problemelor complexe.
2. Proiectează și aplică metode sofisticate pentru investigarea problemelor.
3. Aplică metode și soluții noi pentru probleme complexe.
Responsabilitate și autonomie
1. Lucrează autonom în investigarea și extinderea cunoștințelor.
2. Își asumă responsabilitatea pentru corectitudinea procedurilor aplicate.
3. Își asumă responsabilitatea pentru originalitatea și calitatea lucrărilor.

7. Conținuturi

7.1 Curs	Metode de predare	Observații
1. Considerații introductive privitoare la mediul, formele și particularitățile criminalității informatice.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Explicatii generale ale legaturii între Cyberspatiu si criminalitatea informatica
2. TIC, mediul de comitere al criminalității informatice. Sisteme, date informatice, rețele informatice: definiții și taxonomie.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Explicarea conceptelor esentiale: descriere si clasificare
3. Criminalitatea informatică. Evoluția cadrului legal intern și internațional.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Definitii si taxonomie
4. Atacuri de tip hacking (<i>Cyberintrusions</i>).	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Definitii si taxonomie
5. Riscuri, amenințări și vulnerabilități.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Descriere. Clasificarea vulnerabilitatilor si amenintatilor
6. Hărțuirea electronică (<i>Cyberstalking, Cyberharassment, Cyberbullying, Grooming</i>): Aspecte teoretice și practice.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Caracteristici, cazuri si aspecte privind colaborarea internationala in combaterea acestora
7. Rolul tehnologiilor informațiilor și comunicațiilor în comiterea agresiunilor împotriva minorilor. Pornografia infantilă în sistemele informatice.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Caracteristici, cazuri si aspecte privind colaborarea internationala in combaterea acestora
8. C2C (Criminal către Criminal): aspecte actuale privitoare la legătura dintre criminalitatea informatică și crima organizată.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Caracteristici, cazuri si aspecte privind colaborarea internationala in combaterea acestora
9. Distinctia dintre terorism informatic (<i>Cyberterrorism</i>) și hacktivism.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Caracteristici, cazuri si aspecte privind colaborarea internationala in prevenirea acestora

10. Aspecte esențiale cu privire la mesajele de ură online (<i>Cyberhate</i>): detectarea acestora cu ajutorul inteligenței artificiale.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Caracteristici, cazuri si aspecte privind colaborarea internaționala în prevenirea acestora
11. Pirateria digitală: Aspecte teoretice și practice.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Caracteristici, cazuri si aspecte privind colaborarea internaționala în prevenirea acestora
12. Fraude informatice (<i>Cyberfrauds</i>): Taxonomie și particularități.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Caracteristici, cazuri si aspecte privind colaborarea internaționala în prevenirea acestora
13. Furtul de identitate în mediul online. Provocări legate de evoluția cadrului legal la nivel global și legături cu alte infracțiuni.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Caracteristici, cazuri si aspecte privind colaborarea internaționala în prevenirea acestora
14. Particularități legate de violarea vieții private.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Aspecte actuale privind evoluția legislației la nivel european și global în domeniul prevenirii acestui tip de atacuri

Bibliografie

1. EUROPOL, *Internet Organised Crime Threat Assessment* (2025).
2. Ioana Vasiu, *Infracțiuni contra siguranței și integrității sistemelor și datelor informatice*, Explicațiile Codului penal, Vol. IV: Articolele 257-366, Ed. Universul Juridic, 819-884 (2025).
3. Ioana Vasiu, *Fraude comise prin sisteme informatice și mijloace de plată electronice*, Explicațiile Codului penal, Vol. III: Articolele 188-256¹, Ed. Universul Juridic, 634-678 (2025).
4. Ioana Vasiu, *Infracțiuni ce aduc atingere domiciliului și vieții private*, Explicațiile Codului penal, Vol. III: Articolele 188-256¹, Ed. Universul Juridic, 271-313 (2025).
5. Shuai Chen et al., *Exploring the global geography of cybercrime and its driving forces*, Humanities and Social Sciences Communications, Vol. 10(1), 1-10 (2023). Ioana Vasiu & Lucian Vasiu, *Cyber Extortion and Threats: Analysis of the United States Case Law*, MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY, 14(1), 3-28 (2020)
6. Ioana Vasiu & Lucian Vasiu, *Criminal Copyright Infringement: Forms, Extent, and Prosecution in the United States*, UNIVERSITY OF BOLOGNA LAW REVIEW, Vol. 4:2, 229-260 (2019).
7. Ioana Vasiu & Lucian Vasiu, *Cybersecurity as an Essential Sustainable Economic Development Factor*, EUROPEAN JOURNAL OF SUSTAINABLE DEVELOPMENT, Vol. 7 (4), 171-178 (2018).
8. Ioana Vasiu & Lucian Vasiu, *Backdoor Man: A Radiograph of Computer Source Code Theft Cases*, Journal of High Technology Law, Vol. 18, 1-37 (2017).
9. Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, AMERICAN JOURNAL OF TRIAL ADVOCACY, Vol. 40(1), 41-68 (2016).
10. Ioana Vasiu & Lucian Vasiu, *Riders on the Storm: An Analysis of Credit Card Fraud Cases*, SUFFOLK JOURNAL OF TRIAL & APPELLATE ADVOCACY, Vol. XX, 185-218 (2015).
11. Ioana Vasiu & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, PITTSBURGH JOURNAL OF TECHNOLOGY LAW & POLICY, Vol. XIV, Spring, 158-201 (2014).

7.2 Seminar / laborator	Metode de predare	Observații
1. Introducere în terminologia mediului digital. Prezentarea componentelor sistemelor informatice.	Conversatie, dezbatere, studiu de caz	Seminar/laborator
2.Hacking. Modalitati de realizare.	Conversatie, dezbatere, studiu de caz	Seminar/laborator
3.Cracking. Modalități de realizare.	Conversatie, dezbatere, studiu de caz	Seminar/laborator
4.Clasificarea modalităților de comitere a fraudelor cu carduri.	Conversatie, dezbatere, studiu de caz	Seminar/laborator
5.Modalități de realizare a cyberstalking.	Conversatie, dezbatere, studiu de caz	Seminar/laborator
6.Utilizarea mijloacelor oferite de mediul digital pentru realizarea pornografiei infantile.	Conversatie, dezbatere, studiu de caz	Seminar/laborator
7.Utilizarea mediului DarkNet de către criminalii informatici.	Conversatie, dezbatere, studiu de caz	Seminar/laborator

8.Utilizarea SNS pentru răspândirea contaminanților informatici.	Conversatie, dezbateri, studiu de caz	Seminar/laborator
9.Libertatea de exprimare vs. Cyberhate. Distincții.	Conversatie, dezbateri, studiu de caz	Seminar/laborator
10.Tipuri de piraterie digitală.	Conversatie, dezbateri, studiu de caz	Seminar/laborator
11.Dezinformare online(1): definiții și aspect tehnice și legale.	Conversatie, dezbateri, studiu de caz	Seminar/laborator
12. Dezinformare online(2): forme și attribute.	Conversatie, dezbateri, studiu de caz	Seminar/laborator
13. Dezinformare online(3): aspect privind utilizarea inteligenței artificiale.	Conversatie, dezbateri, studiu de caz	Seminar/laborator
14. Recapitulare și pregătire pentru examenul final		

Bibliografie

1. EUROPOL, *Internet Organised Crime Threat Assessment* (2025).
2. Ioana Vasiu, *Infrațiuni contra siguranței și integrității sistemelor și datelor informatice*, Explicațiile Codului penal, Vol. IV: Articolele 257-366, Ed. Universul Juridic, 819-884 (2025).
3. Ioana Vasiu, *Fraude comise prin sisteme informatice și mijloace de plată electronice*, Explicațiile Codului penal, Vol. III: Articolele 188-256¹, Ed. Universul Juridic, 634-678 (2025).
4. Ioana Vasiu, *Infrațiuni ce aduc atingere domiciliului și vieții private*, Explicațiile Codului penal, Vol. III: Articolele 188-256¹, Ed. Universul Juridic, 271-313 (2025).
5. Ioana Vasiu & Lucian Vasiu, *Cyber Extortion and Threats: Analysis of the United States Case Law*, MASARYK UNIVERSITY JOURNAL OF LAW AND TECHNOLOGY, 14(1), 3-28 (2020)
6. Ioana Vasiu & Lucian Vasiu, *Criminal Copyright Infringement: Forms, Extent, and Prosecution in the United States*, UNIVERSITY OF BOLOGNA LAW REVIEW, Vol. 4:2, 229-260 (2019).
7. Ioana Vasiu & Lucian Vasiu, *Cybersecurity as an Essential Sustainable Economic Development Factor*, EUROPEAN JOURNAL OF SUSTAINABLE DEVELOPMENT, Vol. 7 (4), 171-178 (2018).
8. Ioana Vasiu & Lucian Vasiu, *Backdoor Man: A Radiograph of Computer Source Code Theft Cases*, Journal of High Technology Law, Vol. 18, 1-37 (2017).
9. Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, AMERICAN JOURNAL OF TRIAL ADVOCACY, Vol. 40(1), 41-68 (2016).
10. Ioana Vasiu & Lucian Vasiu, *Riders on the Storm: An Analysis of Credit Card Fraud Cases*, SUFFOLK JOURNAL OF TRIAL & APPELLATE ADVOCACY, Vol. XX, 185-218 (2015).
11. Ioana Vasiu & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, PITTSBURGH JOURNAL OF TECHNOLOGY LAW & POLICY, Vol. XIV, Spring, 158-201 (2014).

Directiva (UE) 2022/2555

Directiva (UE) 2013/40.

Directiva (UE) 2019/790

Regulamentul (UE) 2016/679.

Regulamentul 910/2014.

Legea nr. 214/2024.

Legea nr. 8/1996 cu modificari si completari.

Legea nr. 365/2002

8. Evaluare

Tip activitate	8.1 Criterii de evaluare	8.2 Metode de evaluare	8.3 Pondere din nota finală
8.4 Curs	Cunoașterea notiunilor de bază în domeniul criminalității informatice. Cunoașterea aspectelor privind prevenirea și combaterea criminalității informatice.	Examen scris	80%
8.5 Seminar/laborator	Capacitatea de a efectua analize și de interpretare a rezultatelor obținute.	Contribuții pe parcursul semestrului	20%

8.6 Standard minim de performanță

Pentru absolvirea acestei discipline este necesară obținerea unei note finale de minim 5(cinci);

Notele acordate sunt între 1 (unu) și 10 (zece);

La examenul scris din sesiunea de examen studenții trebuie să obțină minim jumătate din punctajul aferent acestei probe;

Examenul este scris și durează 60 minute.

Studentul va trebui să:

1. cunoască bine principalele concepte, să le recunoască și definească în mod corect;

2. să utilizeze corect limbajul de specialitate.

9. Etichete ODD (Obiective de Dezvoltare Durabilă / Sustainable Development Goals)

	Eticheta generală pentru Dezvoltare durabilă						
							
							

Data completării:

30.09.2025

Semnătura titularului de curs

.....

Semnătura titularului de seminar

.....

Data avizării în departament:

...

Semnătura directorului de departament

.....