FIŞA DISCIPLINEI

Politici şi proceduri privind prevenirea criminalităţii informatice

Anul universitar **2025-2026**

1. Date despre program

1.1. Instituţia de învăţământ superior	UNIVERSITATEA „BABEŞ-BOLYAI" din CLUJ-NAPOCA
1.2. Facultatea	DREPT
1.3. Departamentul	DREPT PUBLIC
1.4. Domeniul de studii	DREPT
1.5. Ciclul de studii	DOCTORAT

2. Date despre disciplină

2.1. Denumirea disciplinei	**Politici şi proceduri privind prevenirea criminalităţii informatice**			Codul disciplinei	**DDR1014**
2.2. Titularul activităţilor de curs	Prof.dr. Ioana Vasiu				
2.3. Titularul activităţilor de seminar	Prof.dr. Ioana Vasiu				
2.4. Anul de studiu	1	2.5. Semestrul	1	2.6. Tipul de evaluare	Examen
2.7. Regimul disciplinei	Opţional		2.8. Tipul disciplinei		Disciplină de specializare (DS)

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/ proiect	**1**
3.4. Total ore din planul de învăţământ	36	din care: 3.5. curs	28	3.6 seminar/laborator	**14**
Distribuţia fondului de timp pentru studiul individual (SI) şi activităţi de autoinstruire (AI)					**Ore**
Studiul după manual, suport de curs, bibliografie şi notiţe (AI)					76
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					76
Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri					55
Tutoriat (consiliere profesională)					
Examinări					1
Alte activităţi					
3.7. Total ore studiu individual (SI) şi activităţi de autoinstruire (AI)				**208**	
3.8. Total ore pe semestru				**250**	
3.9. Numărul de credite				**10**	

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	-
4.2. de competenţe	-

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	-
5.2. de desfăşurare a seminarului/ laboratorului	-

6. Rezultatele învăţării specifice disciplinei

Cunoştinţe

1. Cunoaşte conceptele, teoriile şi modelele avansate din domeniu.
2. Înţelege metodologia ştiinţifică aplicată domeniului său.
3. Cunoaşte standardele de documentare ştiinţifică.
4. Cunoaşte structura şi rigorile scrierii academice internaţionale.
Aptitudini
1. Aplică cunoştinţele pentru analiza problemelor complexe.
2. Proiectează şi aplică metode sofisticate pentru investigarea problemelor.
3. Aplică metode şi soluţii noi pentru probleme complexe.
Responsabilitate şi autonomie
1. Lucrează autonom în investigarea şi extinderea cunoştinţelor.
2. Îşi asumă responsabilitatea pentru corectitudinea procedurilor aplicate.
3. Îşi asumă responsabilitatea pentru originalitatea şi calitatea lucrărilor.

7. Conţinuturi

7.1 Curs	**Metode de predare**	**Observaţii**
1.Consideraţii introductive cu privire la politicile şi procedurile de prevenire a criminalităţii informatice.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
2.Sisteme informatice. Particularităţi în legătură cu metodele specifice de asigurare a rezilienţei şi prevenirea atacurilor asupra acestora.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
3.Potenţiali atacatori ai sistemelor informatice. Metode specifice de prevenire a atacurilor vs. metode de comitere (tehnici specifice utilizate de atacatori).	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
4. Particularităţi legate de diferitele tipuri de ameninţări şi vulnerabilităţi la adresa sistemelor informatice legate de metodele de prevenire a acestora.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
5. Particularităţi legate de malware (1). Descriere şi clasificare.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
6. Particularităţi legate de malware (2). Mijloace specifice de prevenire a atacurilor realizate cu ajutorul contaminanţilor informatici.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
7.Cerinţe operaţionale privind prevenirea criminalităţii informatice (1). Securitatea informatică. Concept şi caracterizare. Importanţa în asigurarea prevenirii criminalităţii informatice.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
8. Cerinţe operaţionale privind prevenirea criminalităţii informatice (2) Cadrul legal intern, regional şi global în domeniul securităţii informatice raportat la	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere

prevenirea atacurilor asupra sistemelor informatice.		
9. Politici, proceduri şi responsabilitati în domeniul prevenirii criminalităţii informatice. Descriere şi clasificare.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
10. Managentul securităţii fizice a sistemelor informatice	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
11. Proceduri de protejare împotriva contaminanţilor informatici	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
12. Responsabilităţi. Definirea responsabilităţilor funcţionale (ex. pentru manageri, angajaţi, utilizatori, etc.)	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
13. Mijloace tehnice de prevenire a criminalităţii informatice	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere
14. Recapitulare şi pregătire pentru examenul final	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web.	Prelegere

Bibliografie

EUROPOL, *Internet Organised Crime Threat Assessment* (2025).
Ioana Vasiu, *Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice*, Explicaţiile Codului penal, Vol. IV: Articolele 257-366, Ed. Universul Juridic, 819-884 (2025).
Ioana Vasiu, *Fraude comise prin sisteme informatice şi mijloace de plată electronice*, Explicaţiile Codului penal, Vol. III: Articolele 188-256[1], Ed. Universul Juridic, 634-678 (2025).
Ioana Vasiu, *Infracţiuni ce aduc atingere domiciliului şi vieţii private*, Explicaţiile Codului penal, Vol. III: Articolele 188-256[1], Ed. Universul Juridic, 271-313 (2025).
Shadi Jawhar, et al., *AI-based cybersecurity policies and procedures*, In 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC), 1-5. IEEE, (2024).
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)
Maeve Dion, *Cybersecurity policy and theory*, In Theoretical Foundations of Homeland Security, 257-284, Routledge, (2020).
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).
Ioana Vasiu & Lucian Vasiu, *Cybersecurity as an Essential Sustainable Economic Development Factor*, EUROPEAN JOURNAL OF SUSTAINABLE DEVELOPMENT, Vol. 7 (4), 171-178 (2018).
Ioana Vasiu & Lucian Vasiu, *Backdoor Man: A Radiograph of Computer Source Code Theft Cases*, Journal of High Technology Law, Vol. 18, 1-37 (2017).
Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, AMERICAN JOURNAL OF TRIAL ADVOCACY, Vol. 40(1), 41-68 (2016).
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).
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**	**Observaţii**
1.Introducere în terminologia mediului digital. Prezentare hardware şi software (1)	Studiu de caz. Discuţii	Seminar/laborator
2.Introducere în terminologia mediului digital. Prezentare hardware şi software (2)	Studiu de caz. Discuţii	Seminar/laborator

3. Prezentarea componentelor managementul securităţii informatice cu accent pe utilizarea acestora în prevenirea atacurilor informatice.	Studiu de caz. Discuţii	Seminar/laborator
4. Descrierea indentelor de securitate informatică.	Studiu de caz. Discuţii	Seminar/laborator
5.Descrierea breşelor de securitate informatică.	Studiu de caz. Discuţii	Seminar/laborator
6. Prezentarea tipurilor de ameninţări la adresa sistemelor informatice şi exemple de metode de prevenire corespunzătoare (1).	Studiu de caz. Discuţii	Seminar/laborator
7. Prezentarea tipurilor de ameninţări la adresa sistemelor informatice şi exemple de metode de prevenire corespunzătoare (2)	Studiu de caz. Discuţii	Seminar/laborator
8. Prezentare de modalităţi de securizare fizică a sistemelor informatice împotriva atacurilor informatice.	Studiu de caz. Discuţii	Seminar/laborator
9. Prezentare de mijloace de securitate a informației. Criptografia asimetrică și criptografia post quantum (1).	Studiu de caz. Discuţii	Seminar/laborator
10. Prezentare de mijloace de securitate a informației. Criptografia clasică (2)	Studiu de caz. Discuţii	Seminar/laborator
11.Protecţia datelor personale şi a aplicaţiilor. Metode specifice de prevenire a atacurilor asupra acestora	Studiu de caz. Discuţii	Seminar/laborator
12. Lanţul de custodie.	Studiu de caz. Discuţii	Seminar/laborator
13. Utilizarea software-urilor de analiză.	Studiu de caz. Discuţii	Seminar/laborator
14.Recapitulare şi pregătire pentru examenul final.	Studiu de caz. Discuţii	Seminar/laborator

Bibliografie

EUROPOL, *Internet Organised Crime Threat Assessment* (2025).
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).
Ioana Vasiu, *Fraude comise prin sisteme informatice și mijloace de plată electronice*, Explicațiile Codului penal, Vol. III: Articolele 188-256[1], Ed. Universul Juridic, 634-678 (2025).
Ioana Vasiu, *Infracțiuni ce aduc atingere domiciliului și vieții private*, Explicațiile Codului penal, Vol. III: Articolele 188-256[1], Ed. Universul Juridic, 271-313 (2025).
Shadi Jawhar, et al., *AI-based cybersecurity policies and procedures*, In 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC), 1-5. IEEE, (2024).
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)
Maeve Dion, *Cybersecurity policy and theory*, In Theoretical Foundations of Homeland Security, 257-284, Routledge, (2020).
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).
Ioana Vasiu & Lucian Vasiu, *Cybersecurity as an Essential Sustainable Economic Development Factor*, EUROPEAN JOURNAL OF SUSTAINABLE DEVELOPMENT, Vol. 7 (4), 171-178 (2018).
Ioana Vasiu & Lucian Vasiu, *Backdoor Man: A Radiograph of Computer Source Code Theft Cases*, Journal of High Technology Law, Vol. 18, 1-37 (2017).
Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, AMERICAN JOURNAL OF TRIAL ADVOCACY, Vol. 40(1), 41-68 (2016).
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).
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).

8. Evaluare

Tip activitate	8.1 Criterii de evaluare	8.2 Metode de evaluare	8.3 Pondere din nota finală
8.4 Curs	Cunoaşterea aspectelor privind politicile de	Examen scris	80%

	prevenirea și combaterea criminalității informatice.		
8.5 Seminar/laborator	Capacitatea de a efectua analize și de a interpreta rezultatelor obținute.	Contribuţii pe parcursul semestrului	20%
8.6 Standard minim de performanţă			
Pentru absolvirea acestei discipline este necesară obţinerea unei note finale de minim 5(cinci); Notele acordate sunt între 1 (unu) și 10 (zece); La examenul scris din sesiunea de examen studenţii trebuie să obţină 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)[1]

	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

.....

[1] Păstrați doar etichetele care, în conformitate cu *Procedura de aplicare a etichetelor ODD în procesul academic*, se potrivesc disciplinei și ștergeți-le pe celelalte, inclusiv eticheta generală pentru *Dezvoltare durabilă* - dacă nu se aplică. Dacă nicio etichetă nu descrie disciplina, ștergeți-le pe toate și scrieți "*Nu se aplică.*".