FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Babeş-Bolyai
1.2 Facultatea	Drept
1.3 Departamentul	Drept public
1.4 Domeniul de studii	Drept
1.5 Ciclul de studii	Master
1.6 Programul de studiu / Calificarea	**ŞTIINŢE PENALE ŞI CRIMINALISTICĂ**

2. Date despre disciplină

2.1 Denumirea disciplinei	**CRIMINALITATE INFORMATICĂ**						
2.2 Titularul activităţilor de curs	Prof. Univ. Dr. Ioana Vasiu						
2.3 Titularul activităţilor de seminar	Prof. Univ. Dr. Ioana Vasiu						
2.4 Anul de studiu	1	2.5 Semestrul	2	2.6. Tipul de evaluare	Exam	2.7 Regimul disciplinei	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	1
3.4 Total ore din planul de învăţământ	42	Din care: 3.5 curs	28	3.6 seminar/laborator	14
Distribuţia fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					28
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					46
Tutoriat					12
Examinări					2
Alte activităţi:					10

3.7 Total ore studiu individual	128
3.8 Total ore pe semestru	170
3.9 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Nu este cazul
4.2 de competenţe	Nu este cazul

5. Condiţii (acolo unde este cazul)

5.1 De desfăşurare a cursului	• Este necesară existenţa unui sistem de proiectare video • Este necesară punerea la dispoziţie a unei săli cu o capacitate de aproximativ 30 de locuri, în care să poată fi utilizată o tablă albă.
5.2 De desfăşurare a seminarului/laboratorului	• Este necesară existenţa unui sistem de proiectare video • Este necesară punerea la dispoziţie a unei săli cu o capacitate de aproximativ 30 de locuri, în care să poată fi utilizată o tablă albă • Referatele trebuie predate titularului de curs în termenul stabilit la începutul semestrului.

6. Competenţele specifice acumulate

Competenţe profesionale	C1.3 Aplicarea corecta a tehnicilor si instrumentelor specifice domeniului de studiu criminalitate informatica, pentru a raspunde adecvat la intrebari fundamentale: care sunt tipurile de infractiuni (atacuri) informatice, cine comite atacurile informatice, ce legi interzic aceste atacuri, care sunt riscurile prezentate de atacurile informatice? Cum pot fi prevenite atacurile informatice? C2.2 Utilizarea adecvata a conceptelor și teoriilor din domeniul criminalitatii informatica, pentru explicarea şi interpretarea textelor de lege (normelor juridice) naţionale, europene şi internaţionale. C2.3 Insusirea, fixarea si utilizarea limbajului de specialitate şi a terminologiei în elaborarea unor argumentări specifice domeniului criminalitate informatica în scris şi oral. C2.5 Elaborarea unor proiecte profesionale cu utilizarea teoriilor, principiilor şi metodelor specifice criminalitatii informatice. C3.1 Identificarea normelor juridice din sistemul de drept românesc, european şi a principalelor instrumente juridice internaţionale privind criminalitatea informatica. C3.2 Explicarea şi interpretarea normelor juridice naţionale, a celor europene şi a prevederilor internaţionale privind criminalitate informatica. C4.5 Elaborarea de proiecte profesionale cu utilizarea metodelor de comparare a legislaţiei naţionale, europene şi a legislaţiei altor state. In domeniul prevenirii, combaterii si investigarii infractiunilor informatice C5.1 Identificarea surselor de informare în domeniul dreptului (legislaţie, doctrină şi jurisprudenţă), aplicabile la o problemă de drept specifica domeniului criminalitatii informatice,, inclusiv utilizarea bazelor de date juridice. C5.4 Evaluarea critică a textelor din legislaţie, doctrină şi jurisprudenţă, referitoare la probleme specifice criminalitate informatica.
Competenţe transversale	CT1 Abilitatea de a analiza comprehensiv, din punct de vedere legal, tehnic si managerial cazuistica relevanta in domeniul criminalitatii informatice CT2 Aplicarea tehnicilor de muncă eficientă în echipă (cu elemente de interdisciplinaritate, avand in vedere specificul disciplinei) CT3 Capacitatea de a prezenta in mod clar si complet aspectele esentiale in domeniu, precum si capacitatea de a le utiliza pentru elaborarea de proiecte şi referate in domeniul prevenirii, combaterii si investigarii criminalitatii informatice CT4 Capacitatea de a utiliza eficient resursele de comunicare şi sursele de informare (baze de date juridice cu practica judiciara in domeniul criminalitatii informatice) şi de formare profesională asistată, atât în limba română, cât şi într-o limbă străină de circulaţie internaţională.

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	Insuşirea si utilizarea adecvata a conceptelor fundamentale din domeniul prevenirii, combaterii si investigarii criminalitatii informatice. .
7.2 Obiectivele specifice	La finalizarea cu succes a studiului acestei discipline, studentii vor fi capabili -sa explice corect si complet conceptele fundamentale din domeniul prevenirii, combaterii si investigarii criminalitatii informatice - sa utilizeze adecvat terminologia specifica reglementarilor in acest domeniu - sa analizeze, intr-o maniera comprehensiva, principalele aspecte privind tipurile de infractiuni (atacuri) informatice, autorii infractiunilor informatice, legile care interzic aceste atacuri, care sunt riscurile prezentate de atacurile informatice, cum pot fi prevenite atacurile informatice, cum poate fi detectat un atac informatic care a avut loc, cum se poate “administra” situatia dupa ce

	un atac informatic s-a produs, cum are loc investigarea unui asemenea atac.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Aspecte introductive privitoare la mediul, formele si particularitatile criminalitatii informatice.	Introducere, prelegere interactiva si studiu de caz	Aspecte transfrontaliere, Alegerea legii aplicabile
2. Sisteme si date informatice. Riscuri, amenintari si vulnerabilitati.	Prelegere interactiva si studiu de caz	Explicarea conceptelor esentiale: riscuri, amenintari si vulnerabilitati
3. Politici si proceduri in domeniul prevenirii criminalitatii informatice.	Prelegere in teractiva si studiu de caz	Confidentialitate, integritate, disponibilitate si autenticitate
4. Criminalitatea informatica. Definitii si taxonomie. Evolutia cadrului legal intern si international.	Prelegere interactive si studiu de caz	Definitii, tipuri si cadrul legal intern si international
5. Atacuri de tip hacking (*Cyberintrusions*).	Prelegere interactive si studiu de caz	Aspecte privind atacurile informatice
6. Hartuirea electronica (*Cyberstalking, Cyberharassment, Cyberbullying, Grooming*): Aspecte teoretice si practice.	Prelegere interactive si studiu de caz	Caracteristici, modalitati de comitere si prevenire
7. Pornografia infantila in sistemele informatice.	Prelegere interactive si studiu de caz	Definitie si prevenire
8 . Aspecte actuale privitoare la legatura dintre criminalitatea informatica si crima organizata.	Prelegere interactive si studiu de caz	Caracteristici, cazuri si aspecte privind colaborarea internationala in prevenirea acestora
9. Distinctia dintre terorism informatic (*Cyberterrorism*) si hacktivism.	Prelegere interactive si studiu de caz	Caracteristici, cazuri si aspecte privind colaborarea internationala in prevenirea acestora
10. Aspecte esentiale cu privire la mesajele de ura online (*Cyberhate*).	Prelegere interactive si studiu de caz	Caracteristici, cazuri si aspecte privind prevenirea acestora
11. Pirateria digitala: Aspecte teoretice si practice.	Prelegere interactive si studiu de caz	Tipuri, exemple, prevenire
12. Fraude informatice (*Cyberfrauds*): Taxonomie si particularitati.	Prelegere interactive si studiu de caz	Concepte, exemple, clasificare si masuri de prevenire
13. Furtul de identitate in mediul online. Provocari legate de evolutia cadrului legal la nivel global, legaturi cu alte infractiuni.	Prelegere interactive si studiu de caz	Concepte si masuri de prevenire
14. Investigarea infractiunilor informatice (*Cyber forensics*). Particularitati privind investigarea in mediul digital.	Prelegere interactive si studiu de caz	Concepte si utilitare

Bibliografie

1. Ioana Vasiu & Lucian Vasiu, *A Framework for Effective Smart Contracting*, BRATISLAVA LAW REVIEW, 7(2), 107–122 (2023).

2. Bill Hefley, Małgorzata Pańkowska, Ioana Vasiu, *Cyber Trust Cultivation Premise and Development*, In "Trust, Digital Business and Technology" (J. Paliszkiewicz, J. Goluchowski & J.L. Guerrero Cusumano,

Eds.), 33-48, Routledge, 2022.

3. 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.

4. 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).

5. Ioana Vasiu & Lucian Vasiu, *Backdoor Man: A Radiograph of Computer Source Code Theft Cases*, JOURNAL OF HIGH TECHNOLOGY LAW, Vol. 18, 1-37 (2017).

6. Ioana Vasiu & Lucian Vasiu, *Malicious Cyber Activity Distribution, Attribution, and Retribution*, In "Advanced Cyberlaw and Electronic Security", 9-19, Ed. Accent (2017)

7. Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, AMERICAN JOURNAL OF TRIAL ADVOCACY, Vol. 40(1), 41-68 (2016).

8. 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).

9. 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).

10. Lucian Vasiu & Ioana Vasiu, *Riscul de atac electronic asupra sistemelor de informatii*, In "Fenomene si procese cu risc major la scara nationala" (Coords. Filip, F.G. & Simionescu, B. C.), Ed. Academiei Romane, 145-165 (2004).

11. Ioana Vasiu & Lucian Vasiu, *Criminalitatea in cyberspatiu*, Ed. Universul Juridic, Bucuresti (2011).

1. DIRECTIVA 2011/92/EU
2. DIRECTIVA 2013/40/EU
3. DIRECTIVA (UE) 2016/680
4. DIRECTIVA (EU) 2016/1148
5. General Data Protection Regulation
6. Cybercrime Convention cu modificari si completari.
7. CIS Agreement
8. Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information
9. African Union Convention on Cyber Security and Personal Data Protection
10. Noul Cod Penal
11. Legea nr. 8/1996 cu modificari si completari.
12. Legea nr. 535/2004.

8.2 Seminar / laborator	Metode de predare	Observaţii
Stabilire titlul lucrare de cercetare	Conversatie, dezbatere, studiu de caz	
Prezentare lucrare si progres proiect	Conversatie, dezbatere, studiu de caz	
Prezentare lucrare si progres proiect	Conversatie, dezbatere, studiu de caz	
Prezentare lucrare si progres proiect	Conversatie, dezbatere, studiu de caz	
Prezentare lucrare si progres proiect	Conversatie,	

	dezbatere, studiu de caz	
Prezentare lucrare si progres proiect	Conversatie, dezbatere, studiu de caz	
Prezentare lucrare si progres proiect	Conversatie, dezbatere, studiu de caz	
Prezentare lucrare si progres proiect	Conversatie, dezbatere, studiu de caz	

Bibliografie

1. Ioana Vasiu & Lucian Vasiu, *A Framework for Effective Smart Contracting*, BRATISLAVA LAW REVIEW, 7(2), 107–122 (2023).

2. Bill Hefley, Małgorzata Pańkowska, Ioana Vasiu, *Cyber Trust Cultivation Premise and Development*, In "Trust, Digital Business and Technology" (J. Paliszkiewicz, J. Goluchowski & J.L. Guerrero Cusumano, Eds.), 33-48, Routledge, 2022.

3. 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).

4. 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).

5. Ioana Vasiu & Lucian Vasiu, *Backdoor Man: A Radiograph of Computer Source Code Theft Cases*, JOURNAL OF HIGH TECHNOLOGY LAW, Vol. 18, 1-37 (2017).

6. Ioana Vasiu & Lucian Vasiu, *Malicious Cyber Activity Distribution, Attribution, and Retribution*, In "Advanced Cyberlaw and Electronic Security", 9-19, Ed. Accent (2017).

7. Ioana Vasiu & Lucian Vasiu, *Light My Fire: A Roentgenogram of Cyberstalking Cases*, AMERICAN JOURNAL OF TRIAL ADVOCACY, Vol. 40(1), 41-68 (2016).

8. 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).

9. 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).

10. Lucian Vasiu & Ioana Vasiu, *Riscul de atac electronic asupra sistemelor de informatii*, In "Fenomene si procese cu risc major la scara nationala" (Coords. Filip, F.G. & Simionescu, B. C.), Ed. Academiei Romane, 145-165 (2004), http://ssrn.com/abstract=2578509.

11. Ioana Vasiu & Lucian Vasiu, *Criminalitatea in cyberspatiu*, Ed. Universul Juridic, Bucuresti (2011).

1. DIRECTIVA 2011/92/EU
2. DIRECTIVA 2013/40/EU
3. DIRECTIVA (UE) 2016/680
4. DIRECTIVA (EU) 2022/2555 (NIS2 Directive)
5. General Data Protection Regulation
6. Cybercrime Convention
7. CIS Agreement
8. Shanghai Cooperation Organization Agreement on Cooperation in the Field of International Information

9. African Union Convention on Cyber Security and Personal Data Protection
10. Noul Cod Penal.
11. Legea nr. 8/1996 cu modificari si completari.
12. Legea nr. 535/2004.

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

Pentru realizarea conținutului acestui curs, titularul disciplinei a colaborat si colaborează cu titulari de disciplină din alte instituții de învățământ superior din U.E. și S.U.A. și participă activ la Conferințe naționale și internaționale pentru a actualiza permanent la necesitatile actuale materialele si metodele de studiu.

Titularul disciplinei organizează Conferințe și seminarii cu participare internațională de nivel înalt, întâlniri științifice cu specialisti din teorie si practica relevanta prevenirii, combaterii si investigarii criminalitatii informatice.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Cunoașterea adecvata, completa si corecta a aspectelor privind prevenirea si combaterea criminalitatii informatice	Examen scris	80%
10.5 Seminar/laborator	Capacitatea de a efectua analize şi de interpretare a rezultatelor obţinute.	Contribuţii pe parcursul semestrului	20%
10.6 Standard minim de performanţă			

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, 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, să le definească şi utilizeze în mod corect;
2. să utilizeze corect limbajul de specialitate.

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
10 IX 2024	Prof. Univ. Dr. Ioana Vasiu	Prof. Univ. Dr. Ioana Vasiu

Data avizării în departament ..... Semnătura directorului de departament ….....