FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Babeș-Bolyai Cluj-Napoca
1.2 Facultatea	Drept
1.3 Departamentul	Drept public
1.4 Domeniul de studii	Drept
1.5 Ciclul de studii	Doctorat
1.6 Programul de studiu / Calificarea	Doctorat

2. Date despre disciplină

2.1 Denumirea disciplinei	**Investigarea infracţiunilor in cyberspaţiu**						
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	1	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	DS

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

3.1 Număr de ore pe săptămână	4	Din care: curs	2	3.3 seminar/laborator	2
3.4 Total ore din planul de învățământ	56	Din care: curs	28	3.6 seminar/laborator	28
Distribuția fondului de timp:					ore
Studiul după manual, suport de curs, bibliografie şi notiţe					9
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					12
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					6
Tutoriat: nu e cazul					
Examinări					
Alte activităţi:					

3.7 Total ore studiu individual	378
3.8 Total ore pe semestru	56
3.9 Numărul de credite	15

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Nu sunt
4.2 de competenţe	Nu sunt

5. Condiţii (acolo unde este cazul)

5.1 De desfăşurare a cursului	Nu sunt
5.2 De desfăşurare a seminarului/laboratorului	Nu sunt

6. Competenţele specifice acumulate

Competenţe profesionale	**C1.**Capacitatea de a inţelege mediul digital, ca mediu de comitere **C2.** Capacitatea de a colecta evidenţe digitale, obţinerea conţinutului digital si a altor informaţii stocate in sisteme informatice; **C3.** Capacitatea de a investiga infracţiuni privind identificarea electronica **C4.** Capacitatea de a investiga infracţiuni privind poşta electronică, retelele de socializare; **C5.** Capacitatea de a investiga infracţiuni privind pirateria digitală, fraudele electronice, pornografia infantilă şi hărţuirea electronică.
Competenţe transversale	**CT1.** Dezvoltarea interesului pentru comunicarea interculturală, necesară în cadrul investigaţiilor privind crimele informatice transfrontaliere; **CT2.** Manifestarea flexibilităţii în cadrul lucrului în echipă, de rigoare în cadrul investigatiilor crimelor informatice; **CT3.** Utilizarea eficientă a tehnologiilor informaţiei şi comunicaţiei pentru rezolvarea problemelor specifice investigaţiei şi cultivarea unei atitudini pozitive faţă de cunoasterea completa si corecta a mediului digital.

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	Familiarizarea cursanţilor cu mediul, formele şi particularităţile criminalităţii informatice şi cu problematica specifică criminalisticii informatice; Capacitatea de a colecta, analiza şi investiga probele specifice mediului digital, precum şi "urmele" (*cyber trails*) lăsate de criminalii informatici; Însuşirea metodelor specifice investigaţiilor din mediul digital; Capacitatea de a investiga cu succes cele mai frecvente şi mai grave infracţiuni informatice (pirateria digitală, frauda şi falsul informatic, infracţiunile relative la semnătura digitală); Formarea deprinderilor de lucru în echipă în mediul digital (colaborare la nivel ethnic, legal si managerial). Dezvoltarea abilităţilor privind aplicarea corectă a cunoştinţele acumulate pentru rezolvarea diferitelor clase de probleme ridicate de investigarea în mediul digital.
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să: ▪ Explice corect conceptele de bază specifice investigaţiei în mediul digital în general, al investigaţiei infracţiunilor informatice în special; ▪ Descrie cei patru paşi de bază ai investigaţiei în mediul digital; ▪ Utilizeze corect soluţiile oferite de mediul digital pentru a obţine rezultate optime în investigarea infracţiunilor informatice; ▪ Analizeze corect evidenţele digitale; ▪ Coopereze cu experţii din domeniu; ▪ Surprindă dezvoltarea domeniului digital şi al metodelor noi folosite de

	hackeri, fraudsteri şi alte tipuri de criminali informatici la nivel naţional şi global.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1.Consideraţii introductive despre mediul digital	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
2.Cyberspace şi cybercriminali. Sistemele informatice, „loc al crimei". Particularitati	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
3. Criminalitatea informatică: Definiţie şi Taxonomie.	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
4. Introducere în investigarea infracţiunilor informatice: Concept, distincţie între culegerea probelor din mediul clasic şi culegerea lor în mediul digital	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
5. Tehnici de bază în investigarea infracţiunilor informatice. Ghidul investigatorului în mediul digital. Crearea echipei de investigare a infracţiunilor informatice	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
6. Cutia cu scule" a investigatorului informatic. Investigarea telefoanelor mobile şi a altor periferice mobile	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
7. Investigarea infracţiunilor privind semnătura digitală si alte mijloace de identificare electronica	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
8. Investigarea infracţiunilor informatice comise în cadrul reţelelor de socializare	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
9. Investigarea fraudelor electronice, cu accent pe	Prelegerea participativă,	Prelegere

frauda cu carduri	dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	
10. Investigarea infracţiunilor de pornografie infantilă	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
11. Investigarea infracţiunilor de hărţuire electronică	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
12. Investigarea infracţiunilor privind pirateria digitală (1)	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
13. Investigarea infracţiunilor privind pirateria digitală (2)	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere
14. Recapitulare. Concluzii pentru cei patru paşi ai investigaţiei in mediul digital	Prelegerea participativă, dezbaterea, expunerea, problematizarea, documentarea pe web, exemplificarea.	Prelegere

Bibliografie

Advanced Cyberlaw and Electronic Security", I. Vasiu & F. Streteanu (eds.), Ed. Accent Publishing (2017).

Ioana Vasiu & Lucian Vasiu, *Backdoor Man: A Radiograph of Computer Source Code Theft Cases*, JOURNAL OF HIGH TECHNOLOGY LAW, Vol. 18, 1-37 (2017), available at https://ssrn.com/abstract=3091468.

Ioana Vasiu, capitole in *Explicatiile noului Cod Penal* (George Antoniu, coord.), vol. II-IV, Ed. Universul Juridic, 2014-2016.

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) available at http://ssrn.com/abstract=2578486.

Ioana Vasiu & Lucian Vasiu, *Cyberstalking Nature and Response Recommendations*, ACADEMIC JOURNAL OF INTERDISCIPLINARY STUDIES, 2(9), 2013.

Ioana Vasiu & Lucian Vasiu, *Frauda cu carduri de credit şi debit: o schemă de clasificare*, REVISTA DE DREPT PENAL, 1, 2012.

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

Council of Europe, *Cybercrime investigation and the protection of personal data and privacy*, 2008.

Stephenson, P., 2002, Collecting Evidence of a Computer Crime, Computer Fraud & Security, Volume 2002, Issue 11,
Shinder D.L., Tittel E., 2002, Scene of the Cybercrime: Computer Forensics Handbook, Syngress Publishing, Inc., USA,
Sheetz M., 2007, Computer Forensics: An Essential Guide for Accountants, Lawyers, and Managers, John Wiley & Sons, USA, ISBN: 978-0471789321
Shinder D.L., Cross M., 2008, Scene of the Cybercrime, 2nd edition, Syngress Publishing, Inc., USA,

8.2 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.Configurarea unui server FTP, configurarea unui server DNS, configurarea unui server Web	Studiu de caz. Discuţii	Seminar/laborator
4.Cum se colectează evidenţele digitale?	Studiu de caz. Discuţii	Seminar/laborator
5.Care sunt particularităţile de investigare a diverselor tipuri de infracţiuni informatice? (1)	Studiu de caz. Discuţii	
6.Care sunt particularităţile de investigare a diverselor tipuri de infracţiuni informatice? (2)	Studiu de caz. Discuţii	Seminar/laborator
7.Posta electronică. Analiza antetelor, cum se sparg parolele?	Studiu de caz. Discuţii	Seminar/laborator
8.Care sunt particularităţile de investigare a device-lor mobile?	Studiu de caz. Discuţii	Seminar/laborator
9.Particularităţi de investigare a fraudelor cu carduri de debit sau credit	Studiu de caz. Discuţii	Seminar/laborator
10.Particularităţi de investigare a fraudelor informatice	Studiu de caz. Discuţii	Seminar/laborator
11.Particularităţi de investigare a infracţiunilor de pornografie infantilă în sistemele informatice	Studiu de caz. Discuţii	Seminar/laborator
12.Particularităţi de investigare a infracţiunilor de hărţuire electronica 13.Particularităţi de investigare a infracţiunilor de piraterie digital 14.Recapitulare. Pregatire pentru examenul final	Studiu de caz. Discuţii	Seminar/laborator

Bibliografie

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.

Ioana Vasiu, capitole in *Explicatiile noului Cod Penal* (George Antoniu, coord.), vol. II-IV, Ed. Universul Juridic, 2014-2016.

Ioana Vasiu & Lucian Vasiu, *Cyberstalking Nature and Response Recommendations*, ACADEMIC JOURNAL OF INTERDISCIPLINARY STUDIES, 2(9), 2013.

Ioana Vasiu & Lucian Vasiu, *Frauda cu carduri de credit şi debit: o schemă de clasificare*, REVISTA DE DREPT PENAL, 1, 2012.

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

Council of Europe, *Cybercrime investigation and the protection of personal data and privacy*, 2008.

Masters G. and Turner P., 2007, Forensic data recovery and examination of magnetic swipe card cloning devices, Digital Investigation, Vol. 4, Supplement 1,

Kessler G.C., 2004, An Overview of Steganography for the Computer Forensics Examiner, Forensic Science Communications, Volume 6 – Number 3, Internet Source, available from: http://www.fbi.gov/hq/lab/fsc/backissu/july2004/research/2004_03_research01.htm. Accessed on 13/04/2008
Kessler G.C., September 2007, Book Review: Casey, E. (2004). Digital Evidence and Computer Crime: Forensics Science, Computers and the Internet (2nd ed.). Amsterdam: Elsevier Academic Press. 690 pp, Criminal Justice Review, Vol. 32, pp. 280-282
Kessler G.C. and Fasulo M., 2007, The Case for Teaching Network Protocols to Computer Forensics Examiners, in Proc. of the Conference on Digital Forensics, Security and Law.

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

Corectitudinea și acuratețea folosirii conceptelor și teoriilor integrarii sociale însușite la nivelul disciplinei – vor satisface asteptarile reprezentantilor comunitatii locale si internationale care lupta impotriva fenomenului criminalitatii informatice.

Competențele procedurale și atitudinale ce vor fi achiziționate la nivelul disciplinei vor satisface aşteptările angajatorilor din domeniu.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 metode de evaluare	10.3 Pondere din nota finală
10.4 Curs		Examen scris	80%
10.5 Seminar/laborator		Participare la discutii	20%
10.6 Standard minim de performanţă			

Data completării

15.01.2019

Semnătura titularului de curs

……