FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea “Alexandru Ioan Cuza” din Iaşi**
1.2 Facultatea	**Facultatea de Drept**
1.3 Departamentul	**Drept public**
1.4 Domeniul de studii	**Drept**
1.5 Ciclul de studii	**Ciclul II – studii universitare de master**
1.6 Programul de studii / Calificarea	Criminalistică

2. Date despre disciplină

2.1 Denumirea disciplinei			**Investigarea criminalităţii informatice**				
2.2 Titularul activităţilor de curs			**Atasiei Daniel**				
2.3 Titularul activităţilor de seminar			**Atasiei Daniel**				
2.4 An de studiu	**I**	**2.5** Semestru	**II**	**2.6** Tip de evaluare	**EF**	**2.7** Regimul disciplinei*	**OB**

** OB – Obligatoriu / OP – Opţional*

3. Timpul total estimat (ore pe semestru şi activităţi didactice)

3.1 Număr de ore pe săptămână	**3**	din care: **3.2** curs	**2**	**3.3** laborator		**1**
3.4 Total ore din planul de învăţământ	**42**	din care: **3.5** curs	**28**	**3.6** laborator		**14**
Distribuţia fondului de timp						ore
Studiu după manual, suport de curs, bibliografie şi altele						**42**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren						**40**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri						**43**
Tutoriat						**4**
Examinări						**4**
Alte activităţi						

3.7 Total ore studiu individual	**133**
3.8 Total ore pe semestru	**175**
3.9 Număr de credite	**7**

4. Precondiţii (dacă este cazul)

4.1 De curriculum	
4.2 De competenţe	Folosirea calculatorului și a internetului în activități de documentare și informare.

5. Condiţii (dacă este cazul)

5.1 De desfăşurare a cursului	
5.2 De desfăşurare a laboratorului	

6. Competenţe specifice acumulate [definitiile conceptelor de mai jos se gasesc la adresa http://docis.acpart.ro/uploads/Fisiere/Metodologie%20CNCIS.pdf]

Competenţe profesionale	**C1. Cunoașterea avansată a domeniului criminalității informatice.** **C2. Identificarea și analizarea situațiilor noi de criminalitate informatică.** **C3. Aplicarea principiilor din cadrul probelor digitale.**
Competenţe transversale	**CT1.** Desfășurarea eficientă a activităților organizate într-un grup inter-disciplinar și dezvoltarea capacităților empatice de comunicare inter-personala, de relaționare și colaborare cu grupuri diverse

7. Obiectivele disciplinei (din grila competenţelor specifice acumulate) [la fel, detalii in documentul http://docis.acpart.ro/uploads/Fisiere/Metodologie%20CNCIS.pdf]

7.1 Obiectivul general	Construirea unei viziuni profesionale asupra criminalității informatice. Studenţii vor învăţa metode şi tehnici avansate pentru depistarea, identificarea și soluționarea situațiilor în care avem probleme ce țin de criminalitatea informatică.
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să: ▪ Identifice principalele vulnerabilități care pot apare într-un sistem informatic. ▪ Lucreze colaborativ folosind utilitarele disponibile în GoogleDocs. ▪ Folosească principalele Practici internationale cu privire la investigatiile informatice ▪ Folosească convenția privind criminalitatea informatică de la nivelul Consiliul Europei ▪ Aplice principiile de bază din domeniul probelor digitale

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii**
1.	Conținutul cursului. Bibliografie. Motivație, Exemple.	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
2.	Sisteme informatice și medii de stocare	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
3.	Hardware: Arhitectura generală. Echipamente de intrare. Echipamente de ieșire	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică. Desenarea la tablă a unui sistem hardware general și discutarea detaliilor pentru componentele acestuia.	2 ore
4.	Retele informatice: Tipuri. Echipamente. Internet.	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică. Exemplificare.	2 ore
5.	Comerțul electronic	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
6.	Amenintari actuale asupra securitatii cibernetice	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore

		Lucrul pe exemple.	
7.	Criminalitiate informatica. Notiune. definiții	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
8.	Reglementări ale criminalității informatice la nivel european	Problematizare. Desenarea la tablă a soluțiilor pentru o problemă dată.	2 ore
9.	Incriminări naționale în materia criminalității informatice	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
10.	Instrumentele procedurale utilizate în lupta împotriva criminalității informatice	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
11.	Aspecte criminologice ale infractorului informatic	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
12.	Securitatea sistemelor informationale. Vulnerabilitatea microcalculatoarelor	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
13.	Amenintare, vulnerabilitate, risc. Amenintari intalnite in prezent: Virusi, Viermi, Troieni, Ransomware, Scareware	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore
14.	Alte tipuri de atacuri: Backdoors, Botnets, Spyware, DDoS, Spam, Phishing si pharming	Prezentare de slide-uri. Note de curs şi tutoriale disponibile în versiune electronică.	2 ore

Bibliografie

Referinţe principale:

[1] Sfetcu, N. Manualul investigatorului în criminalitatea cibernetică http://www.lulu.com/shop/nicolae-sfetcu/manualulinvestigatorului-in-criminalitatea-informatica/ebook/product21593963.html
[2] Ioniță, G. I. (2011) Infracțiunile din sfera criminalității informatice. Incriminare, investigare, prevenire și combatere. Universul Juridic. Bucureşti. https://www.ujmag.ro/drept/dreptpenal/infractiunile-din-sfera-criminalitatii-informatice/rasfoire/
[3] Dobrinoiu, M. (2006) Infracțiuni în domeniul informatic. București http://ecrime.ro/ecrime/site/files/93361241097364Infractiuniindomeniulinformatic.pdf
(4) George Zlati, Tratat de criminalitate informatică. Vol.I. Editura Solomon, București, 2020
(5) Adrian Cristian Moise, Metodologia investigării criminalistice a infracţiunilor informatice, Ed. Universul Juridic, Bucuresti, 2011

Referințe secundare:

[6] Adrian-Cristian Moise, Dimensiunea criminologică a criminalităţii din cyberspaţiu, Ed. C.H. Beck, Bucureşti, 2020
(7) resurse internet

8.2	**Laborator**	**Metode de predare**	**Observaţii** (ore)
1.	PED - Prelucrarea automata a datelor	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
2.	Sisteme informatice și medii de stocare	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
3.	Hardware: Arhitectura generală. Echipamente de intrare. Echipamente de ieșire	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora

4.	Retele informatice: Tipuri. Echipamente. Internet.	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
5.	Comerțul electronic	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
6.	Amenintari actuale asupra securitatii cibernetice	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
7.	Criminalitiate informatica. Notiune. definiții	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
8.	Reglementări ale criminalității informatice la nivel european	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
9.	Incriminări naționale în materia criminalității informatice	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
10.	Instrumentele procedurale utilizate în lupta împotriva criminalității informatice	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
11.	Aspecte criminologice ale infractorului informatic	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
12.	Securitatea sistemelor informationale. Vulnerabilitatea microcalculatoarelor	Problematizare. Discuții. Schițarea la tablă a soluțiilor pentru o problemă dată.	1 ora
13.	Amenintare, vulnerabilitate, risc. Amenintari intalnite in prezent: Virusi, Viermi, Troieni, Ransomware, Scareware	Prezentare folosind video-proiectorul. Problematizare. Discuții.	1 ora
14.	Alte tipuri de atacuri: Backdoors, Botnets, Spyware, DDoS, Spam, Phishing si pharming	Prezentare folosind video-proiectorul. Problematizare. Discuții.	1 ora

Bibliografie

Referințe principale:

[1] Sfetcu, N. Manualul investigatorului în criminalitatea cibernetică http://www.lulu.com/shop/nicolae-sfetcu/manualulinvestigatorului-in-criminalitatea-informatica/ebook/product21593963.html
[2] Ioniță, G. I. (2011) Infracțiunile din sfera criminalității informatice. Incriminare, investigare, prevenire și combatere. Universul Juridic. Bucureşti. https://www.ujmag.ro/drept/dreptpenal/infractiunile-din-sfera-criminalitatii-informatice/rasfoire/
[3] Dobrinoiu, M. (2006) Infracțiuni în domeniul informatic. București http://ecrime.ro/ecrime/site/files/93361241097364Infractiuniindomeniulinformatic.pdf
(4) George Zlati, Tratat de criminalitate informatică. Vol.I. Editura Solomon, București, 2020
(5) Adrian Cristian Moise, Metodologia investigării criminalistice a infracţiunilor informatice, Ed. Universul Juridic, Bucuresti, 2011

Referințe secundare:

[6] Adrian-Cristian Moise, Dimensiunea criminologică a criminalităţii din cyberspaţiu, Ed. C.H. Beck, Bucureşti, 2020
(7) resurse internet

9. Coroborarea conţinutului disciplinei cu aşteptările reprezentanţilor comunităţii, asociaţiilor profesionale şi angajatorilor reprezentativi din domeniul aferent programului

Criminalitatea informatică este din ce în ce mai prezentă în zilele noastre. Companiile din Iași și din țară se lovesc adesea de probleme produse de sistemele informatice ca urmare a atacurilor cu viruși, viermi, malware, etc. Pe parcursul verii studenții participă la sesiuni de stagii în cadrul firmelor, fiind implicați în proiecte reale, unde aplică practic pe proiecte reale noțiunile teoretice și practice învățate la acest curs. În urma discuțiilor cu principalii angajatori, acest curs se actualizează de la an la an, adaptându-se la cerințele actuale ale pieței.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală (%)
10.4 Curs	Însușirea cunoștințelor de specialitate, capacitatea de analiză şi sinteză, formularea unor răspunsuri corecte şi complete la chestiunile puse în discuţie	Test scris + Bonus pentru activitatea de la curs	75%
10.5 Laborator	Activitatea depusă pe parcursul întregului semestru (rezultatele verificărilor efectuate la seminarii), frecvenţă; elaborarea unor lucrări de seminar; parcurgerea bibliografiei; participarea la dezbaterile seminariale	Prezență + Prezentare de soluții la temele propuse săptămânal + Bonus pentru activități suplimentare ce au legătură cu cursul de ICI	25%
10.6 Standard minim de performanţă [raportate la competențele definite la punctul 7. Obiectivele disciplinei]			
Studenții vor fi capabili să identifice principalele vulnerabilități care pot apare într-un sistem informatic. Studenții vor fi capabili să lucreze colaborativ folosind utilitarele disponibile în GoogleDocs. Studenții vor cunoaște principalele Practici internationale cu privire la investigatiile informatice și din Consiliul Europei - Conventie privind criminalitatea informatica. Studenții vor cunoaște principiile de bază din domeniul probelor digitale.			

Data completării	Titulari de curs	Titulari de seminar
24.09.2020	Lect.univ.dr. Daniel Atasiei	Lect.univ.dr. Daniel Atasiei

Data avizării în departament	Director de departament
30.09.2020	Lect. univ. dr. Carmen Moldovan