FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	Universitatea din Bucureşti
1.2. Facultatea	Facultatea de Matematică şi Informatică
1.3. Departamentul	Informatică
1.4. Domeniul de studii	Informatică
1.5. Ciclul de studii	Master
1.6. Programul de studii / Calificarea	Securitate și logică aplicată
1.7. Forma de învăţământ	ZI

2. Date despre disciplină

2.1. Denumirea disciplinei	Securitatea spațiului cibernetic							
2.2. Titularul activităţilor de curs				Drăgan Mihăiță				
2.3. Titularul activităţilor de laborator				Drăgan Mihăiță				
2.4. Anul de studiu	I	2.5. Semestrul	I	2.6. Tipul de evaluare	E	2.7. Regimul disciplinei	Conţinut[2)]	**DF**
							Obligativitate[3)]	**DI**

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

3.1. Număr de ore pe săptămână	**4**	din care: 3.2. curs	**2**	3.3. seminar/ laborator/ proiect	**2**
3.4. Total ore pe semestru	**42**	din care: 3.5. curs	**28**	3.6. SF	**14**

Distribuţia fondului de timp	**Ore**
3.4.1. Studiul după manual, suport de curs, bibliografie şi notiţe – nr. ore SI	50
3.4.2. Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	34
3.4.3. Pregătire seminare/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri	50
3.4.4.Examinări	4
3.4.5. Alte activităţi	

3.7. Total ore studiu individual	138
3.8. Total ore pe semestru	180
3.9. Numărul de credite	6

**** SI (din plan) + însumarea punctelor 3.4.2. şi 3.4.3. (vezi mai jos, în exemple, de unde rezultă nr. de ore pentru aceste puncte)**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	Cunoștințe fundamentale despre hardaware și software
4.2. de competențe	Lucru optim cu calculatorul

5. Condiţii (acolo unde este cazul)

5.1. de desfășurare a cursului	Cursul se desfășoară într-o sală cu proiector
5.2. de desfășurare a seminarului/ laboratorului/ proiectului	Laboratorul se desfășoară într-o sală cu proiector si cu echipamente dedicate de rețelistică. Promovarea testelor din platforma on-line alocate cursului

6. Competenţe specifice acumulate

Competențe profesionale	Scopul cursului este de a dobândi cunoștințele necesare pentru: - securitatea informațiilor, - securitatea sistemelor, - securitatea rețelelor, - securitatea mobilă, fizică - securitate, etică și legi conexe - tehnologii, de apărare și de atenuare.
Competențe transversale	Vor dobândi cunoștințe fundamentale și abilități esențiale în materie de securitate cibernetică, precum și oportunități de carieră în domeniul securității informatice. Cunoștințe noi în depistarea tendințelor, amenințărilor și a condițiilor de siguranță din spațiul cibernetic, protejarea datelor personale și/sau a datelor companiei.

7. Obiectivele disciplinei (reieşind din grila competenţelor specifice acumulate)

7.1. Obiectivul general al disciplinei	Noțiunile ce stau la baza procesului de acumulare de cunoștințe pentru a contracara amentințările și atacurile în securitatea informatică care necesită noi strategii pe piața forței de muncă.
7.2. Obiectivele specifice	• Actualizări privind amenințările cibernetice, atacuri și impactul • Actualizări despre vulnerabilități de securitate • Aspecte juridice și etice în securitatea cibernetică

8. Conţinuturi

8.1. Curs [capitolele de curs]	Metode de predare	Observaţii
1. Necesitatea securității spațiului cibernetic	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Să înțeleagă caracteristicile și valoarea datelor cu caracter personal și a datelor în cadrul unei organizații.
2. Atacuri, concpete și tehnici	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Să recunoască caracteristicile și funcționarea unui atac cibernetic. Interpretarea tendințelor de amenințare din peisajul cibernetic.
3. Protejarea echipamentelor si a datelor	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Înțelegerea modului în care să protejeze dispozitivele împotriva amenințărilor. Deprinderea cunoștințelor în a proteja confidențialitatea.
4. Protejarea organizațiilor	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Noi tehnici pentru a proteja organizațiile de atacuri cibernetice. Să recunoască abordarea bazată pe comportament de securitate cibernetică.
5. Lumea criminalității cibernetice	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Să descrie lumea securității cibernetice, criminali și profesioniști în atacuri cibernetice. Compararea modului în care amenințările afectează securitatea cibernetică a persoanelor fizice, oamenilor de afaceri și organizatiile.
6. Cubul de vrăjitorie cibernetică	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Să explice cele trei dimensiuni ale McCumber Cube. Detalierea modelului ISO de securitate cibernetică. Explicarea principiillor confidențialității, integrității și disponibilității, ce se referă la stări de date și contramăsuri ale securității cibernetice.
7. Vulnerabilități și atacuri în spațiul cibernetic	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Descrierea tacticilor, tehnicilor și procedurilor folosite de criminalii din spațiul cibernetic. Explicarea tipurilor de malware, coduri rău intenționat și a inginerie sociale.
8. Arta protejării secretelor	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Tehnologii, produse și proceduri utilizate pentru a proteja confidențialitate. Explicarea tehnicilor de criptare și tehnicile de control ale accesului.
9. Tehnici de asigurare a integrității.	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Explicarea tehnologiilor, produselor și procedurilor utilizate pentru a asigura integritatea. Detalierea scopului semnăturii digitale și a certificatelor.

10. Domeniul celor cinci ”nouari”	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Reprezentarea modului în care acționează planul de răspuns la incidente și în caz de catastrofe. Îmbunătățirea planificării disponibilității ridicate și de continuitate a afacerilor.
11. Fortificarea domeniului	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Arhitectura sistemelor, serverelor și protecția datelor. Cunoașterea infrastructurii de rețea și de protecție a dispozitivelor de resurse. Explicarea măsurilor de securitate fizice utilizate pentru a proteja echipamentele de rețea.
12. Introducerea în lumea specialiștilor din spațiul cibernetic.	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Explicații de etică și a legilor securității cibernetice. Instrumentele securității cibernetice. Modul de a deveni profesionisti în securitatea cibernetică.
13. Va fi viitorul specialiștilor în domeniul securitații ?	Cu videoproiectorul Explicația. Demonstrația. Descrierea și exemplificarea.	Explorarea oportunităților de a exercita o educație și o carieră în securitate cibernetică.

Bibliografie:

”Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation” *Bruce Dang; 2014*

”Threat Modeling: Designing for Security” Adam Shostack; 2014

”Android Hacker’s Handbook” Joshua J. Drake; 2014

”The Art of Computer Virus Research and Defense” Peter Szor; 2005

”Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software” Michael Sikorski; 2012

8.2. Seminar [temele dezbătute în cadrul seminariilor]	Metode de predare-învățare	Observații
1. Necesitatea securității spațiului cibernetic	Explicația. Demonstrația. Descrierea și exemplificarea.	
2. Atacuri, concpete și tehnici	Explicația. Demonstrația. Descrierea și exemplificarea.	
3. Protejarea echipamentelor si a datelor	Explicația. Demonstrația. Descrierea și exemplificarea.	
4. Protejarea organizațiilor	Explicația. Demonstrația. Descrierea și exemplificarea.	
5. Lumea criminalității cibernetice	Explicația. Demonstrația. Descrierea și exemplificarea.	
6. Cubul de vrăjitorie cibernetică	Explicația. Demonstrația. Descrierea și exemplificarea.	
7. Vulnerabilități și atacuri în spațiul cibernetic	Explicația. Demonstrația. Descrierea și exemplificarea.	
8. Arta protejării secretelor	Explicația. Demonstrația. Descrierea și exemplificarea.	
9. Tehnici de asigurare a integrității.	Explicația. Demonstrația. Descrierea și exemplificarea.	
10. Domeniul celor cinci ”nouari”	Explicația. Demonstrația. Descrierea și exemplificarea.	

11. Fortificarea domeniului	Explicația. Demonstrația. Descrierea și exemplificarea.	
12. Introducerea în lumea specialiștilor din spațiul cibernetic.	Explicația. Demonstrația. Descrierea și exemplificarea.	
13. Va fi viitorul specialiștilor în domeniul securității ?	Explicația. Demonstrația. Descrierea și exemplificarea.	
Bibliografie:		

8.3. Laborator [temele de laborator, proiecte etc, conform calendarului disciplinei]	Metode de transmitere a informației	Observații
1. Necesitatea securității spațiului cibernetic	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
2. Atacuri, concpete și tehnici	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
3. Protejarea echipamentelor si a datelor	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
4. Protejarea organizațiilor	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
5. Lumea criminalității cibernetice	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
6. Cubul de vrăjitorie cibernetică	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
7. Vulnerabilități și atacuri în spațiul cibernetic	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
8. Arta protejării secretelor	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
9. Tehnici de asigurare a integrității.	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
10. Domeniul celor cinci ”nouari”	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
11. Fortificarea domeniului	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
12. Introducerea în lumea specialiștilor din spațiul cibernetic.	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)

13. Va fi viitorul specialiștilor în domeniul securității ?	Platforma on-line Lucrul pe echipamente Utilizare programe specializate	Evaluare la sfârșit de capitol (test platformă on-line)
Bibliografie: **"Reversing: Secrets of Reverse Engineering",** Eldad Eilam; 2005 **"The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities"** Mark Dowd; 2006. **"The IDA Pro Book: The Unofficial Guide to the World's Most Popular Disassembler"** Chris Eagle; 2011**.** **"The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory"** Michael Hale Ligh; 2014.		
8.4. Proiect [doar pentru disciplinele la care exista proiect semestrial norrmat in planul de invatamant]	Metode de predare-învățare	Observaţii
Bibliografie:		

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

Oferind acces la dezvoltari actuale – teoretice, dar cu aplicabilitate practica – cursul își propune să dezvolte aptitudini de cercetare și inovare, pregătind candidați care pot urma programe doctorale și care pot deveni membrii ai departamentelor de cercetare ale firmelor din domeniu, utilizînd cunoștintele dobîndite în administrarea unei rețele ce foloește mai multe routere, switchuri, firewaluri etc.

10. Evaluare

Tip activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Intelegerea notiunilor prezentate Participara activa in prezentarea materialelor Teste rezumative la sfarsit de curs	Calculator Scris	40%
10.5.1. Seminar	Participarea activa prin prezentarea de noutati din domeniu (atacuri, soluții, rezolvări).	Colocviu	20%
10.5.2. Laborator	Activitatea desfășurată în timpul laboratorlui Punctajele obținute la testele din platformă	Calculator Lucrări practice Scris	40%
10.5.3. Proiect [doar pentru disciplinele la care exista proiect semestrial norrmat in planul de invatamant]			
10.6. Standard minim de performanţă: participarea la activitatile desfasurate la laborator; promovarea tuturor testelor intermediare; promovarea testului practic din cadrul laboratorului; un punctaj de minim 70% la testele din platforma on-line;			
Obținerea mediei 5: promovarea activitatilor desfasurate in cadrul laboratorului si obtinerea unui punctaj minim de 70% la toate testele din platforma on-line;			

Data completării

Coordonator de disciplină
Asist. Dr. Drăgan Mihăiță

Tutore de disciplină
Asist. Dr. Drăgan Mihăiță

Data avizării în departament
.....

Director de departament
Conferentiar Dr. Alin Ștefănescu

Notă:

1) Regimul disciplinei (conţinut) - *pentru nivelul de licenţă se alege una din variantele:* **DF** (disciplină fundamentală) / **DD** (disciplină din domeniu) / **DS** (disciplină de specialitate) / **DC** (disciplină complementară).
2) Regimul disciplinei (obligativitate) - *se alege una din variantele:* **DI** (disciplină obligatorie) / **DO** (disciplină opţională) / **DFac** (disciplină facultativă).
3) SI – studiu individual; TC – teme de control; AA – activităţi asistate; SF – seminar faţă în faţă; L – activităţi de laborator; P – proiect, lucrări practice.