FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	**Universitatea “Alexandru Ioan Cuza” din Iaşi**
1.2 Facultatea	**Facultatea de Informatică**
1.3 Departamentul	**Informatică**
1.4 Domeniul de studii	**Informatică**
1.5 Ciclul de studii	**Studii universitare de Masterat**
1.6 Programul de studii / Calificarea	Informatica/Licentiat in informatica

2. Date despre disciplină

2.1 Denumirea disciplinei			**Securitatea retelelor de calculatoare**				
2.2 Titularul activităţilor de curs			**Prof.Dr. Tiplea Ferucio Laurentiu**				
2.3 Titularul activităţilor de seminar			**Lect.Dr. Onica Emanuel**				
2.4 An de studiu	**I**	**2.5** Semestru	**2**	**2.6** Tip de evaluare	**M**	**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	**4**	din care: **3.2** curs	**2**	**3.3** seminar/laborator	**2**
3.4 Total ore din planul de învăţământ	**56**	din care: **3.5** curs	**28**	**3.6** seminar/laborator	**28**
Distribuţia fondului de timp					ore
Studiu după manual, suport de curs, bibliografie şi altele					**14**
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren					**14**
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					**28**
Tutoriat					**-**
Examinări					**4**
Alte activităţi					**-**

3.7 Total ore studiu individual	**56**
3.8 Total ore pe semestru	**114**
3.9 Număr de credite	**8**

4. **Precondiţii** (dacă este cazul)

4.1 De curriculum	**-**
4.2 De competenţe	**-**

5. **Condiţii** (dacă este cazul)

5.1 De desfăşurare a cursului	Este recomandata prezenta la curs
5.2 De desfăşurare a seminarului	Prezenta la seminar

6. Competenţe specifice acumulate

Competenţe profesionale	**C1.** Expunerea unor noţiuni şi rezultate avansate din domeniul cretelelor de calculatoare, în vederea însuşirii lor **C2.** Aplicarea conceptelor asimilate în domenii specializate, precum securitatea informatiei
Competenţe transversale	**CT1.** Eficientizarea activităţilor desfăşurate în cadru organizat, prin aplicarea regulilor academice de muncă riguroasă şi creativă **CT2.** Utilizarea optimă a surselor informaţionale şi a resurselor de comunicare din domeniu **CT3.** Exprimarea unei atitudini responsabile faţă de înţelegerea rolului domeniului în informatică **CT4.** Valorificarea eficace a potenţialului stiinţific însuşit în domeniu

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

7.1 Obiectivul general	Cursul introduce studentilor teme avansate in securitatea retelelor de calculatoare, precum criptografie bazata pe identitate si atribute, si discuta modul in care acestea sunt deja utilizate in practica avansata pentru obtinerea de tehnici de securitate a informatiei.
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenţii vor fi capabili să: ▪ Utilizeze corespunzator concepte de criptografie avansata; ▪ Inteleaga corespunzator, la nivel ridicat, securitatea retelelor de calculatoare.

8. Conţinut

8.1	**Curs**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)

1.	Scurta incursiune in criptografie	Expunere si demonstratii realizate la tabla	2
2.	Criptografie bazata pe identitate (partea I – schema Cocks)	Expunere si demonstratii realizate la tabla	2
3.	Criptografie bazata pe identitate (partea II – schema Cocks)	Expunere si demonstratii realizate la tabla	2
4.	Criptografie bazata pe identitate (partea I – schema BGH)	Expunere si demonstratii realizate la tabla	2
5.	Criptografie bazata pe identitate (partea II – schema BGH)	Expunere si demonstratii realizate la tabla	2
6.	Criptografie bazata pe identitate : anonimizare	Expunere si demonstratii realizate la tabla	2
7.	Criptografie bazata pe identitate : schema Boneh-Franklin	Expunere si demonstratii realizate la tabla	2
8.	Criptografie bazata pe atribute (partea I – scheme bazate pe secret sharing si aplicatii biliniare)	Expunere si demonstratii realizate la tabla	2
9.	Criptografie bazata pe atribute (partea II – scheme bazate pe secret sharing si aplicatii biliniare)	Expunere si demonstratii realizate la tabla	2
10.	Criptografie bazata pe atribute (partea I – scheme bazate pe aplicatii multiliniare)	Expunere si demonstratii realizate la tabla	2
11.	Criptografie bazata pe atribute (partea II – scheme bazate pe aplicatii multiliniare)	Expunere si demonstratii realizate la tabla	2
12.	Constructii de aplicatii multiliniare (partea I)	Expunere si demonstratii realizate la tabla	2
13.	Constructii de aplicatii multiliniare (partea II)	Expunere si demonstratii realizate la tabla	2
14.	Aplicatii la “searchable encryption”	Expunere si demonstratii realizate la tabla	2

Bibliografie

Referinţe principale:

- L. Martin: Introduction to Identity-based Encryption, Artech House, 2008
- S. Chatterjee, P. Sarkar: Identity-based Encryption, Springer, 2010
- Articole de specialitate

Referinţe suplimentare:

- F.L. Tiplea. Fundamentele Algebrice ale Informaticii, Ed. Polirom, 2006
- F.L. Tiplea: Introducere in criptografie, Curs Facultatea de Informatica, 2017

8.2	**Seminar / Laborator**	**Metode de predare**	**Observaţii** (ore şi referinţe bibliografice)

1.	Recapitulare notiuni de baza privind comunicarea in retea. Prezentarea de aplicatii pentru monitorizare si simulare trafic.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
2.	Pregatirea unui mediu controlat pentru simularea de atacuri in retea.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
3.	Exemple de atacuri la nivel legatura de date si internet. Propunerea unei teme aplicative spre rezolvare.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
4.	Scurta recapitulare legata de functionarea protocoalelor de transport. Exemple de atacuri asupra TCP bazate pe ICMP.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
5.	Evaluarea temelor propuse spre rezolvare.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
6.	Exemple de atacuri asupra TCP bazate pe injectare de pachete la nivel transport (resetarea conexiunii). Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
7.	Exemple de atacuri de tip SYN flood. Detalii privind protectia asupra atacurilor de tip SYN flood si resetare conexiune. Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
8.	Discutare de articole stiintifice privind mecanisme de protectie in aria atacurilor la nivel transport.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
9.	Exemple de atacuri bazate pe injectare de pachete cu efect de "deturnare" a sesiunii - session hijacking. Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
10.	Scurta descriere SSH ca mecanism de protectie impotriva atacurilor la nivel sesiune si aplicatie. Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2

11.	Scurta descriere a diverselor metode de organizare a atacurilor de tip DDoS. Discutare de articole in domeniu.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
12.	Chestiuni generale legate de functionarea DNS si DNSSEC. Exemple de atacuri asupra DNS cu acces la mediu si in mod blind. Propunerea unei teme aplicative.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
13.	Evaluare prin exercitii recapitulative.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2
14.	Evaluarea temelor propuse spre rezolvare. Prezentarea de tematici de cercetare in domeniul securitatii retelelor de calculatoare.	Demonstratii aplicate in laborator. Discutarea de articole in domeniu prin participarea studentilor si propunerea de implementari.	2

Bibliografie

- W. Stallings: Cryptography and Network Security, Pearson, 2013
- M. Gregg: The Network Security Test Lab: A Step-by-Step Guide, Wiley 2015
- Wireshark – Online: https://www.wireshark.org/#learnWS
- Articole de specialitate

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

Cursul este corelat cu asteptarile moderne in securitatea informatiei (de exemplu, Amazon si-a format recent echipe de securitatea informatiei, multi dintre fostii studenti ai masterului de securitatea informatiei fiind membri ai acestor echipe).

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală (%)
10.4 Curs	Cunoasterea conceptelor si a rezultatelor fundamentale in domeniu; Abilitatea de aplicare a lor	Test scris	50%
10.5 Seminar/ Laborator	Cunoasterea conceptelor si a rezultatelor fundamentale in domeniu;	Exercitii realizate in clasa de fiecare student, precum si evaluarea de	50%

	Abilitatea de aplicare a lor	implementari	
10.6 Standard minim de performanţă			
Minim nota 5 atat la testul scris cat si la activitatea de seminar/laborator			

Data completării	Titular de curs	Titular de seminar
1 martie 2018	Prof.Dr. Tiplea Ferucio Laurentiu	Lect.Dr. Emanuel Onica

Data avizării în departament Director de departament