



## FIȘA DISCIPLINEI

### 1. Date despre program

1.1 Instituția de învățământ superior	Universitatea “Alexandru Ioan Cuza” din Iași
1.2 Facultatea	Facultatea de Informatică
1.3 Departamentul	Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Licență
1.6 Programul de studii / Calificarea	Informatica/Licentiat in informatica

### 2. Date despre disciplină

2.1 Denumirea disciplinei	Securitatea Informatiei						
2.2 Titularul activităților de curs	Prof.Dr. Tiplea Ferucio Laurentiu						
2.3 Titularul activităților de seminar	Prof.Dr. Tiplea Ferucio Laurentiu						
2.4 An de studiu	III	2.5 Semestru	1	2.6 Tip de evaluare	M	2.7 Regimul disciplinei*	OB

\* OB – Obligatoriu / OP – Opțional

### 3. Timpul total estimat (ore pe semestru și activități 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 învățământ	56	din care: 3.5 curs	28	3.6 seminar/laborator	28
Distribuția fondului de timp					ore
Studiu după manual, suport de curs, bibliografie și altele					14
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					14
Pregătire seminarii/laboratoare, teme, referate, portofolii și eseuri					28
Tutoriat					-
Examinări					4
Alte activități					-
3.7 Total ore studiu individual					56
3.8 Total ore pe semestru					114
3.9 Număr de credite					5

### 4. Precondiții (dacă este cazul)

4.1 De curriculum	-
4.2 De competențe	-

**5. Condiții** (dacă este cazul)

5.1 De desfășurare a cursului	Este recomandată prezența la curs
5.2 De desfășurare a seminarului	Prezența la seminar/laborator

**6. Competențe specifice acumulate**

Competențe profesionale	<b>C1.</b> Expunerea unor concepte fundamentale asupra securității informatice <b>C2.</b> Utilizarea potențialului științific dobândit în activitatea practică cu specific informatic
Competențe transversale	<b>CT1.</b> Eficientizarea activităților desfășurate în cadrul organizat, prin aplicarea regulilor academice de muncă riguroasă și creativă <b>CT2.</b> Utilizarea optimă a surselor informaționale și a resurselor de comunicare din domeniu <b>CT3.</b> Exprimarea unei atitudini responsabile față de înțelegerea rolului domeniului în informatică <b>CT4.</b> Valorificarea eficace a potențialului științific însușit în domeniu

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

7.1 Obiectivul general	Cursul introduce studenților o tematică majoră în informatică, și anume securitatea informației, atrage atenția asupra necesității ei și discută aparatul științific necesar atingerii securității informatice (în anumite limite: domeniul este foarte vast și cursul de față nu discută decât o zonă limitată a domeniului, în concordanță cu abordarea în multe universități de prestigiu din lume)
7.2 Obiectivele specifice	La finalizarea cu succes a acestei discipline, studenții vor fi capabili să: <ul style="list-style-type: none"><li>▪ Utilizeze corespunzător concepte de criptografie în securitatea informației;</li><li>▪ Înțeleagă corespunzător, la nivel ridicat, securitatea sistemelor informatice.</li></ul>

**8. Conținut**

8.1	Curs	Metode de predare	Observații (ore și referințe bibliografice)
1.	Introducere în teoria controlului accesului	Expunere și demonstrații realizate la tablă	2



2.	Controlul accesului: modele discreționare	Expunere și demonstrații realizate la tablă	2
3.	Controlul accesului: modele mandatate	Expunere și demonstrații realizate la tablă	2
4.	Controlul accesului: modelul bazat pe roluri	Expunere și demonstrații realizate la tablă	2
5.	Elemente de criptografie (partea I)	Expunere și demonstrații realizate la tablă	2
6.	Elemente de criptografie (partea II)	Expunere și demonstrații realizate la tablă	2
7.	Managementul cheilor (partea I)	Expunere și demonstrații realizate la tablă	2
8.	Managementul cheilor (partea II)	Expunere și demonstrații realizate la tablă	2
9.	Extensii de securitate pentru DNS (DNSsec)	Expunere și demonstrații realizate la tablă	2
10.	Extensii de securitate pentru IP (partea I)	Expunere și demonstrații realizate la tablă	2
11.	Extensii de securitate pentru IP (partea II)	Expunere și demonstrații realizate la tablă	2
12.	Protocolul SSL&TLS	Expunere și demonstrații realizate la tablă	2
13.	Protocolele S/MIME și PGP	Expunere și demonstrații realizate la tablă	2
14.	Directii noi: securitatea calculului în cloud	Expunere și demonstrații realizate la tablă	2

**Bibliografie****Referințe principale:**

- M. Bishop: Introduction to Computer Security, Addison-Wesley, 2005
- W. Stallings: Cryptography and Network Security: Principles and Practices, Pearson Education, 3<sup>rd</sup> Edition, 2003
- Specific technical documentation such as RFCs
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, third printing, 1997

**Referințe suplimentare:**

- F.L. Tiplea. Fundamentele Algebrice ale Informaticii, Ed. Polirom, 2006

8.2	Seminar / Laborator	Metode de predare	Observații (ore și referințe bibliografice)
1.	Introducere în teoria controlului accesului	Exerciții realizate la tablă prin participarea studenților și propunerea de implementări	2
2.	Controlul accesului: modele discreționare	Exerciții realizate la tablă prin participarea studenților și propunerea de implementări	2



3.	Controlul accesului: modele mandatate	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
4.	Controlul accesului: modelul bazat pe roluri	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
5.	Elemente de criptografie (partea I)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
6.	Elemente de criptografie (partea II)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
7.	Managementul cheilor (partea I)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
8.	Managementul cheilor (partea II)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
9.	Extensii de securitate pentru DNS (DNSsec)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
10.	Extensii de securitate pentru IP (partea I)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
11.	Extensii de securitate pentru IP (partea II)	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
12.	Protocolul SSL&TLS	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
13.	Protocoalele S/MIME si PGP	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2
14.	Directii noi: securitatea calculului in cloud	Exercitii realizate la tabla prin participarea studentilor si propunerea de implementari	2

**Bibliografie**

- M. Bishop: Introduction to Computer Security, Addison-Wesley, 2005
- W. Stallings: Cryptography and Network Security: Principles and Practices, Pearson Education, 3<sup>rd</sup> Edition, 2003
- Specific technical documentation such as RFCs
- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. Handbook of Applied Cryptography, CRC Press, third printing, 1997

**9. Coroborarea conținutului disciplinei cu așteptările reprezentanților comunității, asociațiilor profesionale și 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; Abilitatea de aplicare a lor	Exercitii realizate in clasa de fiecare student, precum si evaluarea de implementari	50%
<b>10.6 Standard minim de performanță</b>			
Minim nota 5 atat la testul scris cat si la activitatea de seminar/laborator			

Data completării

Titular de curs  
Prof.Dr. Tiplea Ferucio LaurentiuTitular de seminar  
Prof.Dr. Tiplea Ferucio laurentiu

Data avizării în departament

Director de departament