FIȘA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Tehnică din Cluj-Napoca
1.2 Facultatea	Automatică și Calculatoare
1.3 Departamentul	Calculatoare
1.4 Domeniul de studii	Calculatoare și Tehnologia Informaţiei
1.5 Ciclul de studii	Master
1.6 Programul de studii / Calificarea	Retele de Comunicaţii și Sisteme Distribuite / Master
1.7 Forma de învăţământ	IF – învăţământ cu frecvenţă
1.8 Codul disciplinei	14.

2. Date despre disciplină

2.1 Denumirea disciplinei				***Securitatea Informatiilor***	
2.2 Titularii de curs				Sl. dr. ing. Marius Joldos - marius.joldos@cs.utcluj.ro	
2.3 Titularul / Titularii activităţilor de seminar / laborator / proiect				Sl. dr. ing. Marius Joldos - marius.joldos@cs.utcluj.ro	
2.4 Anul de studiu	I	2.5 Semestrul	1	2.6 Tipul de evaluare *(E – examen, C – colocviu, V – verificare)*	E
2.7 Regimul disciplinei	*DA – de aprofundare, DS – de sinteza, DC – complementară*				DS
	DI – Impusă, DOp – opțională, DFac – facultativă				DI

3. Timpul total estimat

3.1 Număr de ore pe săptămână	3	din care:	Curs	2	Seminar	0	Laborator	1	Proiect	0
3.2 Număr de ore pe semestru	42	din care:	Curs	28	Seminar	0	Laborator	14	Proiect	0
3.3 Distribuţia fondului de timp (ore pe semestru) pentru:										
(a) Studiul după manual, suport de curs, bibliografie şi notiţe										40
(b) Documentare suplimentară în bibliotecă, pe platforme electronice de specialitate şi pe teren										20
(c) Pregătire seminarii / laboratoare, teme, referate, portofolii şi eseuri										21
(d) Tutoriat										0
(e) Examinări										2
(f) Alte activităţi:										0

3.4 Total ore studiu individual (suma (3.3(a)...3.3(f)))	83
3.5 Total ore pe semestru (3.2+3.4)	125
3.6 Numărul de credite	5

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	N/A
4.2 de competenţe	Arhitectura sistemelor de operare, Arhitectura calculatoarelor, Cunoștințe de bază de rețele de calculatoare

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	Prezență la curs minim 50% pentru admiterea la examenul final
5.2. de desfăşurare a seminarului / laboratorului / proiectului	Prezență obligatorie 100% la orele de seminar pentru admiterea la examenul final

6. Competenţele specifice acumulate

6.1 Competenţe profesionale	C1 - Identificarea și înțelegerea problemelor de securitate ce pot apărea în diverse domenii de utilizare a sistemelor de calcul. Aplicarea adecvată a elementelor de bază ale managementului securității și ale modalităților de evaluare și management al riscurilor de securitate informatice • C1.1 – Cunoașterea noțiunilor, conceptelor și principiilor teoretice și practice avansate aferente domeniului general al securității informațiilor și sistemelor de calcul. Cunoașterea conceptelor aferente riscurilor, evaluării riscurilor și managementului securității

	• C1.2 – Înțelegerea riscurilor de securitate specifice unor situații noi și legătura lor cu cele cunoscute anterior. Prevederea scenariilor posibile de securitate, în momentul în care soluțiile de securitate cunoscute sunt folosite într-o situație sau domeniu nou • C1.3 – Modelarea unor noi tipuri de riscuri de securitate, evidențierea impactului asupra utilizatorului, asupra sistemelor și aplicațiilor existente. Identificarea unor soluții posibile și evaluarea lor • C1.4 – Stabilirea limitelor maxime de securitate oferite de soluții nou propuse. Plasarea corectă a riscurilor de securitate și a posibilelor soluții într-un cadru de repere bine cunoscute anterior • C1.5 – Elaborarea de modele teoretice noi de analiză a proprietăților de securitate sau evaluarea securității oferite de diverse soluții C4 - Proiectarea și dezvoltarea de software cu un înalt grad de securitate, de soluții și unelte de securitate • C4.2 – Identificarea de noi scenarii în care este nevoie de introducerea unei soluții de securitate sau utilizarea unei unelte de securitate. Analiza soluțiilor de securitate propuse și compararea lor cu cele cunoscute anterior • C4.4 – Evaluarea unor proiecte software existente și identificarea greșelilor de securitate din punctul de vedere al arhitecturii, modului de programare sau procedurilor de testare. Propunerea unor noi metode de dezvoltare și testare • C4.5 – Dezvoltarea unor module software sau a unor utilitare care să ajute la asigurarea unui înalt grad de securitate. Propunerea unor scenarii și modalități de testare a unor proiecte existente, cu scopul de a verifica și asigura calitatea lor din punctul de vedere al securității C5 - Rezolvarea corectă și eficientă a unor probleme complexe de securitate informatică din lumea reală. Operarea cu metode și modele matematice, tehnici și tehnologii aferente inginerești și informatice specifice domeniului securității informațiilor și sistemelor de calcul • C5.1 – Cunoașterea legăturilor dintre securitatea informațiilor și lumea reală. Cunoașterea elementelor matematice care stau la baza elementelor de securitate • C5.2 – Analiza și interpretarea de situații noi complexe din lumea reală, prin prisma cunoștințelor fundamentale din domeniul securității informațiilor și sistemelor de calcul. Identificarea și corelarea unor soluții similare cu cele cunoscute, precum și plasarea corectă a ideilor noi în domeniul cercetării și dezvoltării de soluții de securitate informatice • C5.4 – Stabilirea corectă a limitărilor de aplicabilitate în lumea reală a diferitelor tehnologii de securitate. Evaluarea riscurilor potențiale rămase și a priorității lor. Determinarea unor posibile noi arii și metode de cercetare teoretice sau tehnologice care ar putea soluționa riscurile și limitările identificate
6.2 Competenţe transversale	CT1 - Cunoașterea contextului economic, etic, legal și social de exercitare a profesiei pentru identificarea sarcinilor, planificarea activităților și optarea pentru decizii responsabile. Abilități de a evalua impactul social, etic și legal a desfășurării activităților profesionale

7. Obiectivele disciplinei

7.1 Obiectivul general al disciplinei	Dobândirea unei viziuni ample și globale asupra numeroaselor arii și aspecte ce fac parte din sau sunt direct conexe cu securitatea informațiilor, a sistemelor și a rețelelor de calcul. Se urmărește, totodată, înțelegerea aplicabilității noțiunilor și a elementelor specifice securității informației la diverse procese din lumea reală (și în mod particular la proiecte software și sisteme de calcul) precum și dobândirea unei abilități de a observa, a analiza și a evalua legăturile dintre securitatea informației și lumea reală.

7.2 Obiectivele specifice	1. Familiarizarea cu terminologia specifică domeniului securității informațiilor și folosirea corectă a acestei terminologii 2. Înțelegerea diverselor aspecte și moduri în și prin care criminalitatea cibernetică și securitatea informațiilor este legată de activitățile zilnice 3. Dobândirea unei abilități de a analiza un sistem informatic din punctul de vedere al securității informatice (de ex. a avea o atitudine critică) 4. Dobândirea unei viziuni de ansamblu și de a putea face legătură între variate arii inginerești, variate tipuri de proiecte software, domeniul și elementele specifice securității informațiilor și procedurile și standardele aplicabile 5. Familiarizarea cu cele 10 domenii fundamentale (conform CISSP) a securității informațiilor.

8. Conţinuturi

8.1 Curs	Nr.ore	Metode de predare	Observații
1. Introducere si context. Impactul asupra calității vieții	2		
2. Securitatea informațiilor și managementul riscurilor (I)	2		
3. Securitatea informațiilor și managementul riscurilor (II)	2		
4. Criptografie	2		
5. Securitatea telecomunicațiilor si a rețelelor de calculatoare	2		
6. Controlul accesului	2		
7. Arhitectura și proiectarea sistemelor de securitate (I)	2		
8. Arhitectura și proiectarea sistemelor de securitate (II)	2		
9. Securitatea fizică și de mediu	2		
10. Aspecte legale, reglementări, proceduri de investigație și conformare	2		
11. Securitatea în procesul de dezvoltare a aplicațiilor (I)	2		
12. Securitatea în procesul de dezvoltare a aplicațiilor (II)	2		
13. Securitatea operațiunilor (I)	2		
14. Securitatea operațiunilor (II)	2		
Bibliografie *(bibliografia minimală a disciplinei conținând cel puțin o lucrare bibliografică de referință a disciplinei, care există la dispoziția studenților într-un număr de exemplare corespunzător)* 1. CISSP Exam Guide – Harris, S. – McGraw-Hill, 2012, 6th edition 2. Computer and Information Security Handbook – Vacca, J. – Morgan Kaufmann, 2013, 2nd edition 3. Geekonomics. The Real Cost of Insecure Software – Rice, D. – Addison-Wesley, 2008 4. Numeroase articole și rapoarte tehnice elaborate de companiile din domeniu – în format electronic.			
8.2 Aplicații (seminar/laborator/proiect)*	Nr.ore	Metode de predare	Observații
Pregătire – Instalarea și configurarea mașinii virtuale	2	Explicații suplimentare, îndrumare pentru efectuarea lucrărilor de laborator	
Laborator de criptografie – Cifrarea cu cheie secretă	2		
Laborator de criptografie -- Infrastructura de chei publice (PKI)	2		
Laborator de atac: atacul Shellshock	2		
Laborator de atac: asupra DNS	2		
Laborator de atac: Falsificarea cererilor intre situri	2		
Analiza activității de laborator	2		
Bibliografie *(bibliografia minimală pentru aplicații conținând cel puțin o lucrare bibliografică de referință a disciplinei care există la dispoziția studenților într-un număr de exemplare corespunzător)* 1. CISSP Exam Guide – Harris, S., Maymi, F. – McGraw-Hill, 2016, 7th edition 2. Computer and Information Security Handbook – Vacca, J. – Morgan Kaufmann, 2017, 3nd edition 3. Geekonomics. The Real Cost of Insecure Software – Rice, D. – Addison-Wesley, 2008 4. Numeroase articole și rapoarte tehnice elaborate de companiile din domeniu – în format electronic.			

**Se vor preciza, după caz: tematica seminariilor, lucrările de laborator, tematica și etapele proiectului.*

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

Materialul de bază pentru acest curs reprezintă tematica CISSP® (Certified Information Systems Security Professional), una dintre cele mai importante certificări în domeniul securității informațiilor, recunoscut și apreciat pe plan internațional (https://www.isc2.org/cissp/default.aspx).
Se realizează totodată prin discuții periodice cu reprezentanți ai angajatorilor semnificativi, în special cei care angajează pe proiecte din domeniul securității informațiilor.
Materiale de la curs și seminar sunt încarcate pe https://moodle.cs.utcluj.ro/

10. Evaluare

Tip activitate	Criterii de evaluare	Metode de evaluare	Pondere din nota finală
Curs	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de curs	Examen scris de tip grilă	80%
Seminar	Abilitatea de rezolvare a unor probleme specifice domeniului Prezență, (inter)activitate în timpul orelor de seminar	Prezentarea unei teme de cercetare din domeniul cursului și/sau rezolvarea și prezentarea soluției unor probleme similare cu cele discutate în timpul orelor de seminar	20%
Laborator	-	-	-
Proiect	-	-	-

Standard minim de performanţă:
Demonstrarea prin interacțiunile și discuțiile la orele de seminar a înțelegerii conceptelor și a noțiunilor folosite în domeniul securității informațiilor, precum și aplicarea și folosirea lor corectă. Capacitatea de analiză critică din punct de vedere al securității informatice a unui (studiu de) caz dintre cele prezentate si analizate la curs sau seminar și posibilitatea de a defini și explica termenii specifici folosiți.

	Titulari	**Titlu Prenume NUME**	**Semnătura**
Data completării: 24.06.2023	Curs	Sl. dr. ing. Marius Joldos	
	Aplicații	Sl. dr. ing. Marius Joldos	

Data avizării în Consiliul Departamentului Calculatoare	Director Departament, Prof. dr. ing. Rodica Potolea
Data aprobării în Consiliul Facultății de Automatică și Calculatoare	Decan, Prof. dr. ing. Liviu Miclea