FIŞA DISCIPLINEI [1]

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Politehnica Timisoara
1.2 Facultatea [2] / Departamentul[3]	Electronica, Telecomunicatii si Tehnologii Informationale / Comunicatii
1.3 Catedra	–
1.4 Domeniul de studii (denumire/cod[4])	Inginerie Electronica, Telecomunicatii si Tehnologii Informationale / 10
1.5 Ciclul de studii	Master
1.6 Programul de studii (denumire/cod/calificarea)	Tehnologii, sisteme si aplicatii pentru eActivitati

2. Date despre disciplină

2.1 Denumirea disciplinei/Categoria formativă[5]			Securitatea sistemelor pentru eActivitati				
2.2 Titularul activităţilor de curs			Sl.dr.ing. Silviu Vert				
2.3 Titularul activităţilor aplicative[6]							
2.4 Anul de studiu[7]	1	**2.5** Semestrul	2	**2.6** Tipul de evaluare	E	**2.7** Tipul disciplinei[8]	DA

3. Timp total estimat - ore pe semestru (activități directe (asistate integral), activități asistate parțial și activități neasistate[9])

3.1 Număr de ore asistate integral/săptămână	3 , din care:	**3.2** ore curs	2	**3.3** ore seminar/laborator/proiect			0/ 1/ 0
3.1* Număr total de ore asistate integral/sem.	42 , din care:	**3.2*** ore curs	28	**3.3*** ore seminar/laborator/proiect			0/ 14/ 0
3.4 Număr de ore asistate parțial/saptămână	, din care:	**3.5** ore proiect, cercetare		**3.6** ore practică		**3.7** ore elaborare lucrare de disertație	
3.4* Număr total de ore asistate parțial/ semestru	, din care:	**3.5*** ore proiect cercetare		**3.6*** ore practică		**3.7*** ore elaborare lucrare de disertație	
3.8 Număr de ore activități neasistate/ săptămână	3 , din care:	ore documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					1
		ore studiu individual după manual, suport de curs, bibliografie și notițe					1
		ore pregătire seminarii/laboratoare, elaborare teme de casă și referate, portofolii și eseuri					1
3.8* Număr total de ore activități neasistate/ semestru	42 , din care:	ore documentare suplimentară în bibliotecă, pe platformele electronice de specialitate și pe teren					14
		ore studiu individual după manual, suport de curs, bibliografie și notițe					14
		ore pregătire seminarii/laboratoare, elaborare teme de casă și referate, portofolii și eseuri					14
3.9 Total ore/săptămână[10]	6						
3.9* Total ore/semestru	84						
3.10 Număr de credite	5						

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	• Utilizarea rețelelor și protocoalelor de comunicații

[1] Formularul corespunde Fişei Disciplinei promovată prin OMECTS 5703/18.12.2011 (Anexa3), actualizată pe baza Standardelor specifice ARACIS valabile începând cu data de 1 iunie 2018.
[2] Se înscrie numele facultăţii care gestionează programul de studii căruia îi aparţine disciplina.
[3] Se înscrie numele departamentului căruia i-a fost încredinţată susţinerea disciplinei şi de care aparţine titularul cursului.
[4] Se înscrie codul prevăzut în HG nr. 376/18.05.2016 sau în HG similare actualizate anual.
[5] Categoriile formative ale disciplinelor (ARACIS – Standarde specifice, pct. 4.1.2 a) sunt: discipline fundamentale, de domeniu, de specialitate.
[6] Prin activităţi aplicative se înţeleg activităţile de: seminar (S) / laborator (L) / proiect (P) / practică (Pr).
[7] Anul de studii la care este prevăzută disciplina în planul de învăţământ.
[8] Tipurile de disciplină (ARACIS – Standarde specifice, pct. 4.1.2 a) sunt: disciplină de aprofundare / disciplină de cunoaștere avansată și disciplină de sinteză (DA / DCAV și DS).
[9] În cadrul UPT, numărul de ore de la rubricile 3.1*, 3.2*,…,3.9* se obţin prin înmulţirea cu 14 (săptămâni) a numărului de ore din rubricile 3.1, 3.2,…, 3.9.
[10] Numărul de ore total/săptămână se obţine prin însumarea numărului de ore de la punctele 3.1, 3.4 şi 3.8.

4.2 de competenţe	•

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	• Sală dotată cu echipamente multimedia. Capacitatea sălii: 25 locuri
5.2 de desfăşurare a activităţilor practice	• Sală de laborator, dotată cu calculatoare, minim 14 posturi de lucru

6. Competenţe la formarea cărora contribuie disciplina

Competenţe specifice	• Evaluarea diverselor tipuri de amenințări asupra sistemelor hardware și software • Aplicarea tehnicilor de securizare adecvate amenințărilor • Aplicarea planului de securitate al instituției
Competențele profesionale în care se înscriu competențele specifice	• Elaborarea și documentarea de tehnologii de operare și mentenanță, coordonarea și administrarea rețelelor de calculatoare și a aplicațiilor web. • Comunicare cu specialiști din domeniu
Competențele transversale în care se înscriu competențele specifice	• Comportare onorabilă, responsabilă, etică, în spiritul legii, pentru a asigura reputația profesiei

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

7.1 Obiectivul general al disciplinei	• Evaluarea amenințărilor asupra aplicațiilor/sistemelor software și asupra rețelelor de calculatoare si aplicarea unor tehnologii de operare și mentenanță și a tehnicilor de securizare
7.2 Obiectivele specifice	• Să evalueze diverse tipuri de ameninţări asupra sistemelor hardware și software • Să aplice tehnici de securizare adecvate ameninţărilor • Să aplice planul de securitate al instituţiei • Să comunice cu specialiştii din domeniu şi cu utilizatorii, respectând normele etice

8. Conţinuturi

8.1 Curs	Număr de ore	Metode de predare
Curs 1: Fundamente ale securității IT. Principii de bază de securitate (principiul privilegiului minim, securitate prin obscuritate etc).	2	Curs interactiv cu materiale didactice prezentate cu videoproiector și exemplificări, inclusiv prin secvențe video
Curs 2: Amenințări: Spyware, malware, viermi, viruși. Securitate la nivel de OS.	2	
Curs 3: Securitatea rețelelor de calculatoare.	2	
Curs 4: Securitatea rețelelor wireless.	2	
Curs 5: Securizarea sistemelor software. Vocabular. Design pentru securitate. Codare pentru securitate. Testare pentru securitate.	2	
Curs 6: Securitatea aplicațiilor web. Principii generale. Filtrarea intrărilor și controlul ieșirilor. Atacuri frecvente (XSS, SQL injection etc).	2	
Curs 7: Securitatea aplicațiilor web. Criptare. Autentificarea si autorizarea utilizatorilor. Altele (plata cu cardul online, securizarea sistemelor de versionare, securitatea bazei de date	2	

etc)		
Curs 8: Securitatea serverelor web. HTTP/HTTPS. Certificate.	2	
Curs 9: Securizarea celor mai întâlnite platforme pentru eActivități (Wordpress, Joomla etc).	2	
Curs 10: Securitate in browser. Securitatea aplicațiilor mobile.	2	
Curs 11: Securitate cibernetică. Tehnici de inginerie socială. Securitatea pe rețele sociale.	2	
Curs 12: Securitatea sistemelor IoT și cloud.	2	
Curs 13: Ethical hacking - detectarea, prevenirea si contracararea atacurilor cibernetice.	2	
Curs 14: Cibersecuritate globală. Pregătirea pentru meseria de specialist în securitate IT.	2	

Bibliografie[11]

1. M. Alexandru, S. Cocorada, Securitatea sistemelor pentru eActivitati, Ed. UT Press, 2012, ISBN-978-973-662-774-3
2. V. Patriciu, M. Pietrosanu, Semnături electronice şi securitate informatică, Ed. ALL, 2006
3. V. Patriciu, M. Pietrosanu, I. Bica, etc., Securitatea comerţului electronic, ed. ALL, 2006
4. N. Boudriga, Security of Mobile Communications, Taylor and Francis Group, 2010
5. William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Firewalls and Internet Security, Second Edition, Addison-Wesley, 2003
6. Andrew. S. Tanenbaum, Retele de calculatoare, ed. a 4-a, Byblos 2003
7. James F. Kurose, Keith W. Ross, Computer Networking - A top down approach 5/e, Pearson Education 2010
8. Juned Ahmed Ansari, Web Penetration Testing with Kali Linux - Second Edition, Packt Publishing, 2015
9. Chris Chapman, Network Performance and Security: Testing and Analyzing Using Open Source and Low-Cost Tools, Syngress Publisher, 2016
10. Kumar Velu, Mobile Application Penetration Testing Vijay, Packt Publishing, 2016

8.2 Activităţi aplicative[12]	Număr de ore	Metode de predare
Laborator: Esențializarea cunoștințelor căpătate la curs. Exemple de aplicare a principiilor de bază de securitate.	1	Studii de caz, Exerciții si probleme
Laborator: Aplicarea principiilor securizării sistemelor software. Recunoașterea vulnerabilităților.	2	
Laborator: Securitatea comerțului electronic. Securitatea sistemelor IoT și cloud.	2	
Laborator: Exemplificarea tehnicilor de inginerie socială.	2	
Laborator: Aplicarea de tehnici de securizare a rețelelor de calculatoare și a rețelelor wireless.	1	Lucru pe PC, cu conexiune internet. Lucru pe dispozitive în rețea cablată și wireless.
Laborator: Detectarea vulnerabilităților din aplicațiile web și securizarea acestora.	2	Lucru pe PC, cu acces la un server web.
Laborator: Exemplificarea securizării aplicațiilor mobile și web pentru eActivități.	2	Lucru pe PC, cu acces la un server web.
Laborator: Utilizarea certificatelor si a semnăturii digitale.	1	Lucru pe PC, cu acces la un server web.
Laborator: Exemple de reţele VPN, configurări.	1	Lucru pe PC, cu acces la un server web.

[11] Cel puţin un un titlu trebuie să aparţină colectivului disciplinei. De asemenea, cel puţin un titlu trebuie să se refere la o lucrare de referință pentru disciplină, lucrare de circulaţie naţională şi internaţională, existentă în biblioteca UPT.

[12] Tipurile de activităţi aplicative sunt cele precizate în nota de subsol 6. Dacă disciplina conţine mai multe tipuri de activităţi aplicative atunci ele se trec consecutiv în liniile tabelului de mai jos. Tipul activităţii se va înscrie într-o linie distinctă sub forma: „Seminar:”, „Laborator:”, „Proiect:” şi/sau „Practică:”.

Bibliografie[13]
1. M. Alexandru, S. Cocorada, Securitatea sistemelor pentru eActivitati, Ed. UT Press, 2012, ISBN-978-973-662-774-3
2. V. Patriciu, M. Pietrosanu, Semnături electronice şi securitate informatică, Ed. ALL, 2006
3. V. Patriciu, M. Pietrosanu, I. Bica, etc., Securitatea comerţului electronic, ed. ALL, 2006
4. N. Boudriga, Security of Mobile Communications, Taylor and Francis Group, 2010
5. William R. Cheswick, Steven M. Bellovin, Aviel D. Rubin, Firewalls and Internet Security, Second Edition, Addison-Wesley, 2003
6. Andrew. S. Tanenbaum, Retele de calculatoare, ed. a 4-a, Byblos 2003
7. James F. Kurose, Keith W. Ross, Computer Networking - A top down approach 5/e, Pearson Education 2010
8. Juned Ahmed Ansari, Web Penetration Testing with Kali Linux - Second Edition, Packt Publishing, 2015
9. Chris Chapman, Network Performance and Security: Testing and Analyzing Using Open Source and Low-Cost Tools, Syngress Publisher, 2016
10. Kumar Velu, Mobile Application Penetration Testing Vijay, Packt Publishing, 2016

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

- Competențele dobândite vor fi necesare angajaților care își desfășoară activitatea în domeniul securizării rețelelor de calculatoare și a securizării aplicațiilor web și mobile.

10. Evaluare

Tip activitate	**10.1** Criterii de evaluare[14]	**10.2** Metode de evaluare	**10.3** Pondere din nota finală
10.4 Curs	Claritatea, coerența, concizia expunerii și explicării funcționalității. Identificarea corectă a cel puţin 3 ameninţări de securitate IT. Evaluarea ameninţărilor. Descrierea tehnicilor de securizare. Aplicarea diferenţiată a tehnicilor de securizare. Adecvarea modalităţii de securizare la situaţia problemă identificată. Evaluare la curs (întrebări legate de cursul curent).	Examen scris cu itemi obiectivi. Evaluare continuă prin observarea comportamentului în timpul cursului.	50%
10.5 Activităţi aplicative	**S:**		
	L: Rezolvarea corectă a problemelor specifice fiecărei teme. Folosirea surselor de documentare tipărite, software specializat și resurse electronice.	Verificări la fiecare ședință de laborator și verificare finală.	50%
	P:		
	Pr:		
	Tc-R[15]:		
10.6 Standard minim de performanţă (volumul de cunoştinţe minim necesar pentru promovarea disciplinei şi modul în care se verifică stăpânirea lui)[16]			
• Identificarea și evaluarea a cel puțin 3 amenințări de securitate în contextul sistemelor pentru eActivități. Aplicarea de tehnici adecvate de securizare pentru acestea. • Obținerea unei note minime de 5 pentru examenul scris si pentru media notelor din cadrul activităților aplicative.			

[13] Cel puţin un titlu trebuie să aparţină colectivului disciplinei.
[14] Fişele disciplinelor trebuie să conţină procedura de evaluare a disciplinei cu precizarea criteriilor, a metodelor și a formelor de evaluare, precum și cu precizarea ponderilor atribuite acestora în nota finală. Criteriile de evaluare trebuie să corespundă tuturor activităților prevăzute în planul de învățământ (curs, seminar, laborator, proiect), precum și formelor de verificare pe parcurs (teme de casă, referate ș.a.)
[15] Tc-R=teme de casă - Referate
[16] Pentru acest punct se recomandă consultarea “Ghidului de completare a Fișei disciplinei” de la adresa: http://univagora.ro/m/filer_public/2012/10/21/ghid_de_completare_fisa_disciplinei.pdf

Data completării	Titular de curs (semnătura)	Titular activităţi aplicative (semnătura)
05.05.2019	……	……

Director de departament (semnătura)	Data avizării în Consiliul Facultăţii[17]	Decan (semnătura)
……		……

[17] Avizarea Fișei disciplinei a fost precedată de discutarea punctului de vedere al board-ului de care aparţine programul de studii.