Universitatea POLITEHNICA din Bucureşti
Facultatea de Stiinte Aplicate

FISA DISCIPLINEI
Securitatea datelor si protectia antivirus (S.D.P.A.)

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea POLITEHNICA din Bucureşti
1.2 Facultatea	Facultatea de Stiinte Aplicate
1.3 Departamentul	Departamentul de Metode si Modele Matematice
1.4 Domeniul de studii	Stiinte Ingineresti Aplicate
1.5 Ciclul de studii	MASTER
1.6 Programul de studii/Calificarea	TCSI/Specialist SIG/IT COD.COR 252901

2. Date despre disciplină

2.1 Denumirea disciplinei				Securitatea datelor si protectia antivirus (S.D.P.A.)			
2.2 Titularul activităţilor de curs				Conf. Dr. Ing. Eduard-Cristian Popovici			
2.3 Titularul activităţilor de seminar				Conf. Dr. Ing. Eduard-Cristian Popovici			
2.4 Anul de studiu	II	2.5 Semestrul	I	2.6 Tipul de evaluare	Examen	2.7 Regimul disciplinei	Obligatoriu

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

3.1 Număr de ore pe săptămână din care	3	3.2 curs	1	3.3 seminar/laborator	2
3.4 Total ore din planul de învăţământ din care	42	3.5 curs	14	3.6 seminar/laborator	28

Distribuţia fondului de timp	ore
Studiul după manual, suport de curs, bibliografie şi notiţe	30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate	14
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	14
Tutoriat	0
Examinări	4
Alte activităţi	0

3.7 Total ore studiu individual	62
3.9 Total ore pe semestru	104
3. 10 Numărul de credite	4

4. Precondiţii (acolo unde este cazul)

4.1 de curriculum	Nu este cazul
4.2 de competenţe	Nu este cazul

5. Condiţii (acolo unde este cazul)

5.1 de desfăşurare a cursului	Nu este cazul
5.2 de desfăşurare a seminarului	Prezenţa obligatorie la seminarii

6. Competenţe specifice acumulate

Competenţe profesionale	- Dezvoltarea capacităţii de a folosi în domeniul cercetării informatice cunoştinţe de matematică modernă; - Dezvoltarea abilităţilor de folosire a sistemelor de operare UNIX şi LINUX; - Dezvoltarea capacităţii de a proiecta şi administra reţele de calculatoare; - Dezvoltarea capacităţii de a proteja serverele de atacurile informatice si de a asigura un trafic informaţional securizat; - Dezvoltarea capacităţii de lucru în echipă; - Dezvoltarea capacităţii de cercetare ştiinţifică; - Cunoaşterea procesului continuu de evolutie al amenintarilor asupra securităţii datelor si a programelor calculatoarelor personale. Planificarea procesului de management al securităţii sistemelor de calcul fixe sau portabile. Proiectarea şi operarea unor aplicaţii pentru detectia si stoparea programelor malitioase cat si securizarea calculatorului personal.
Competenţe transversale	Comportarea onorabilă, responsabilă, etică, în spiritul legii pentru a asigura reputaţia profesiei.

7. Obiectivele disciplinei (reieşind din grila de competenţe specifice acumulate)

7.1 Obiectivul general al disciplinei	Studiul programelor cu actiuni malitioase si a modului lor de functionare; a principalelor mecanisme de protectie impotriva programelor malitioase, principiilor şi tehnologiilor aplicate în securizarea calculatoarelor personale; managementului securităţii calculatoarelor personale fixe şi/sau portabile cu sisteme de operare standard; mecanismelor de protectie a retelelor de calculatoare impotriva virusilor; utilitarelor folosite în recuperarea datelor distruse prin atacuri informatice sau şterse de utilizatori.
4.2 Obiective specifice	**1. Cunoştinţe teoretice - Cunoaştere şi înţelegere:** Prezentarea programelor cu actiuni malitioase si a modului lor de functionare; a principalelor mecanisme de protectie impotriva programelor malitioase, principiilor şi tehnologiilor aplicate în securizarea calculatoarelor personale; managementului securităţii calculatoarelor personale fixe şi/sau portabile cu sisteme de operare standard; mecanismelor de protectie a retelelor de calculatoare impotriva virusilor. **2. Deprinderi dobândite - Explicare şi interpretare:** Formarea deprinderilor necesare recunoaşterii particularităţilor contextului de aplicare a tehnologiilor de securitate studiate şi selectarea soluţiei optime; configurarea şi operarea principalelor tehnologii corespunzătoare ariei acoperite de curs. **3. Abilităţi dobândite - Instrumental-aplicative:** Obtinerea de catre studenti a abilitatilor si deprinderilor privind realizarea scenariilor de test pentru validarea functionala a diferitelor solutii de protectie si filtrare; auditul securităţii pentru configuraţiile realizate, determinarea problemelor şi propunerea soluţiilor corespunzătoare. **4. Atitudinale:** Capacitatea de lucru în echipă pentru rezolvarea unor probleme practice. Responsabilitate şi corectitudine în activităţile desfăşurate.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii

Principii şi probleme de securitate ale calculatoarelor personale	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă). Materialele de curs sunt: notele şi prezentările de curs (disponibile în format electronic), tutorialele online corespunzătoare ultimelor versiuni ale limbajelor si toolurilor software folosite.	4 ore
Managementul securităţii calculatoarelor personale fixe sau portabile		2 ore
Vectori ai atacurilor informatice		4 ore
Întreţinerea calculatorului personal		2 ore
Resurse avansate de securitate		2 ore

Bibliografie

- K. Sriram, D. Montgomery, O. Borchert, O. Kim, and R. Kuhn, Border Gateway Protocol (BGP): Investigation of Vulnerabilities and Simulation Studies of Attack Impacts, National Institute of Standards and Technology Gaithersburg, MD 20878, 2006
- Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, Network Security Bible, Wiley Publishing, Inc., ISBN: 0-7645-7397-7, 2005
- Ramaswamy Chandramouli, Scott Rose, Secure Domain Name System (DNS) Deployment Guide, NIST Special Publication 800-81, 2006
- Gene Spafford, Securing Network Devices, 2009

8.2 Laborator	Metode de predare	Observaţii
Familiarizarea cu mediile de Configurarea si testarea solutiilor antivirus	Predarea se bazează pe parcurgerea punctelor esențiale din platformele de laborator si tutoriale online. Studenţii utilizeaza calculatorul şi mediul software. Materialele didactice sunt platformele de laborator cuprinse în îndrumarul de laborator si tutoriale online.	2 ore
Management-ul politicilor de securitate (globale/locale)		6 ore
Sisteme de tip firewall		4 ore
Securitatea protocoalelor de rutare		6 ore
Securitatea serviciilor multimedia		4 ore
Sisteme de detectie/prevenire e intruziunilor (IDS/IPS)		4 ore
Colocviu final de laborator		2 ore

Bibliografie

- K. Sriram, D. Montgomery, O. Borchert, O. Kim, and R. Kuhn, Border Gateway Protocol (BGP): Investigation of Vulnerabilities and Simulation Studies of Attack Impacts, National Institute of Standards and Technology Gaithersburg, MD 20878, 2006
- Dr. Eric Cole, Dr. Ronald Krutz, and James W. Conley, Network Security Bible, Wiley Publishing, Inc., ISBN: 0-7645-7397-7, 2005
- Ramaswamy Chandramouli, Scott Rose, Secure Domain Name System (DNS) Deployment Guide, NIST Special Publication 800-81, 2006
- Gene Spafford, Securing Network Devices, 2009

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

Programa cursului răspunde concret acestor cerinţe actuale de dezvoltare şi evoluţie, subscrise economiei europene a serviciilor din domeniul Calculatoare şi Tehnologia Informaţiei (CTI). Se asigură astfel absolvenţilor competenţe adecvate cu necesităţile calificărilor actuale si o pregătire ştiinţificăşi tehnică moderne, de calitate şi competitive, care să le permită angajarea rapidă după absolvire, fiind perfect încadrat în politica Universităţii Politehnica din Bucureşti, atât din punctul de vedere al conţinutului şi structurii, cât şi din punctul de vedere al aptitudinilor şi deschiderii internaţionale oferite studenţilor. **Cursul are ca obiectiv dobindirea competentelor necesare realizarii scenariilor de test pentru validarea functionala a diferitelor solutii de protectie si filtrare; auditul securităţii pentru configuraţiile realizate, determinarea problemelor şi propunerea soluţiilor corespunzătoare.**

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere în nota finală

10.4 Curs	- cunoaşterea noţiunilor teoretice fundamentale; - cunoaşterea modului de aplicare a teoriei	Verificarea orala a cunostintelor cu ocazia evaluarii unui mini-proiect	50%
10.5 Laborator	- demonstrarea validitatii solutiilor propuse in mini-proiect pentru scenariile date	Evaluare pe baza unui mini-proiect creat pe baza exemplelor din laborator si a unor tutoriale externe	50%
10.6 Standard minim de performanţă			
Cunoaşterea noţiunilor teoretice de bază prezentate la curs şi propunerea unor solutii concrete la scenario propuse.			

Data completării **01.09.2018**

Semnătura titularului de curs
Conf.Dr.Ing. Eduard-Cristian Popovici

Semnătura titularului de aplicaţii
Conf.Dr.Ing. Eduard-Cristian Popovici

Data avizării în departament
.....

Semnătura sefului de department
Prof. Dr. Mircea Olteanu

Responsabil program master
lector dr. Emil Simion