Universitatea POLITEHNICA din Bucureşti
Facultatea de Stiinte Aplicate

FISA DISCIPLINEI
SECURITATE CIBERNETICA (S.C.)

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				SECURITATE CIBERNETICA (S.C.)			
2.2 Titularul activităţilor de curs				lector dr. Emil Simion			
2.3 Titularul activităţilor de seminar				lector dr. Emil Simion			
2.4 Anul de studiu	I	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	1	3.2 curs	2	3.3 seminar/laborator	2
3.4 Total ore din planul de învăţământ din care	56	3.5 curs	28	3.6 seminar/laborator	28
Distribuţia fondului de timp					ore
Studiul după manual, suport de curs, bibliografie şi notițe					30
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate					5
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri					10
Tutoriat					0
Examinări					3
Alte activităţi					0

3.7 Total ore studiu individual	48
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; - La absolvirea cursului Securitate cibernetica cursantii vor fi familiarizati cu mecanismele si conceptele de securitate ale retelelor de comunicatii, securitatea informatiei in format electronic si realizarea analizelor de risc in contextul amenintarilor cibernetice actuale. Totodata se va acorda o atentie sporita tehnicilor de bune practici in managementul securitatii informatiei (standarde si legislatie), securitatea retelelor (control acces, sisteme de detectie a intruziunilor, managementul securitatii serverelor, sisteme firewall), precum si securitatea sistemelor si aplicatiilor.
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	Aplicarea, în situaţii tipice, a metodelor de implementare a celor mai bune practice utilizate in protectia sistemelor informatice.
4.2 Obiective specifice	**1. Cunoştinţe teoretice - Cunoaştere şi înţelegere:** Prezentarea tehnicilor şi metodelor utilizate în protecţia sistemelor informatice. Cunoaşterea principiilor şi metodelor de proiectare a mecanismelor de protectie cibernetica. **2. Deprinderi dobândite - Explicare şi interpretare:** Formarea deprinderilor necesare proiectării, implementării şi evaluării mecanismelor de protectie a sistemelor informatice. Identificarea problemelor specifice implementării tehnicilor si mijloacelor de protectie a sistemelor informatice. **3. Abilităţi dobândite - Instrumental-aplicative:** Utilizarea instrumentelor de analiză şi evaluare a securitatii informatice. **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
1. Mecanisme si concepte de securitate: ➢ Bazele retelelor de comunicatii ➢ Securitatea informatiei ➢ Vulnerabilitati si amenintari ➢ Criptologie	Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metodele de	8 ore
2. Managementul securitatii ➢ Practici in managementul securitatii ➢ Standarde si legislatie		6 ore

<table>
<tr><td>3. Securitatea retelelor
➢ Acces control si Sisteme de detectie a intruziunilor
➢ Managementul serverelor si Firewall
➢ Securitatea VPN si Next Generation Network</td><td rowspan="3">comunicare orală utilizată sunt metoda expozitivă şi metoda problematizării, utilizate frontal.
Materialele de curs sunt: notele şi prezentările de curs, culegeri de probleme propuse (teoretice şi cu rezolvare pe calculator). Toate materialele sunt disponibile în format electronic, prin situl cursului.</td><td>6 ore</td></tr>
<tr><td>4. Securitatea sistemelor si aplicatiilor</td><td>4 ore</td></tr>
<tr><td>5. Tipologii de atacuri cibernetice</td><td>4 ore</td></tr>
<tr><td colspan="3">Bibliografie
1. 1. Information Security Management System, ISO 27001.
2. Risk Management Guide for Information Technology Systems, NIST SP 800-30.
3. Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG), www.sans.org.
4. D. Naccache, E. Simion, Cryptography and Information security. Applications, MATRIX ROM, 2011, ISBN 978-973-755-675-2, 107 pages.
5. D. Naccache, E. Simion and Gh. Simion, Operational research, Probability and Cryptology. Applications, Military Technical Academy, 2011, ISBN 978-973-640-208-1, 292 pages.
6. Nicu Bizon, Lucian Dascalescu, Naser M. Tabatabei, E. Simion et. al., Autonomous Vehicles: Intelligent Transport Systems and Smart Technologies, Chapter 6: Cyber Security Evaluation of Critical Infrastructures System, pp 185-206, Nova Publishers, 2014, ISBN 978-1-63321-326-5.
7. www.cryptool.org
8. https://cryptopals.com/</td></tr>
<tr><td>8.2 Seminar</td><td>Metode de predare</td><td>Observaţii</td></tr>
<tr><td>1. Constructia unei analize de risc</td><td rowspan="7">Predarea se bazează pe folosirea videoproiectorului (acoperind funcţia de comunicare şi demonstrativă); metoda de comunicare orală utilizată este metoda problematizării,utilizate frontal. Materialele didactice sunt postate pe platforma educaţională a UPB.</td><td>4 ore</td></tr>
<tr><td>2. Controale de securitate cibernetica (SANS)</td><td>4 ore</td></tr>
<tr><td>3. Configurarea unui firewall. Exemple de configurari corecte si exemple de configurari incorecte</td><td>4 ore</td></tr>
<tr><td>4. Utilitare de evaluare a securitatii</td><td>4 ore</td></tr>
<tr><td>5. Studii de caz. Virusul FLAME, constructie si manifestare</td><td>4 ore</td></tr>
<tr><td>6. Studii de caz. Virusul FLAME, contracarare</td><td>4 ore</td></tr>
<tr><td>7. Studii de caz. Virusul FLAME, lectii invatate</td><td>4 ore</td></tr>
<tr><td colspan="3">Bibliografie
9. Information Security Management System, ISO 27001.
10. Risk Management Guide for Information Technology Systems, NIST SP 800-30.
11. Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines (CAG), www.sans.org.
12. D. Naccache, E. Simion, Cryptography and Information security. Applications, MATRIX ROM, 2011, ISBN 978-973-755-675-2, 107 pages.
13. D. Naccache, E. Simion and Gh. Simion, Operational research, Probability and Cryptology. Applications, Military Technical Academy, 2011, ISBN 978-973-640-208-1, 292 pages.
14. Nicu Bizon, Lucian Dascalescu, Naser M. Tabatabei, E. Simion et. al., Autonomous Vehicles: Intelligent Transport Systems and Smart Technologies, Chapter 6: Cyber Security Evaluation of</td></tr>
</table>

Critical Infrastructures System, pp 185-206, Nova Publishers, 2014, ISBN 978-1-63321-326-5.
15. www.cryptool.org
16. https://cryptopals.com/

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

Intrând progresiv în era informaţiei, societăţile industrializate se găsesc în faţa unui paradox: pe de o parte, puterea şi influenţa Europei şi a Americii de Nord au crescut semnificativ, în principal datorită măiestriei modalităţilor prin care se controlează fluxurile de informaţii, precum şi valorii crescute a datelor procesate. Pe de altă parte, după cum au demonstrat-o deja criza Wikileaks, viermele Stuxnet, sau virusul WannaCry, apar noi ameninţări şi vulnerabilităţi care fac ca dependenţa noastră de sistemele informaţionale să fie crucială. De aceea, dezvoltarea atacurilor cibernetice, precum şi disponibilitatea online a instrumentelor utilizate în activitatea de piraterie conduce la obiective strategice importante şi cultivă necesitatea de a pregăti experţi pentru acest domeniu. Mediul în care trăim se schimbă în ritm alert, această evoluţie fiind rezultatul progresului în domeniul tehnologiilor informaţionale, precum şi al matematicii. **Cursul are ca obiectiv dobindirea competentelor necesare conceperii, evaluarii si implementarii controalelor de securitate cibernetica.**

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 la probleme specifice; - analiza diferenţială a tehnicilor şi metodelor teoretice.	Examen parţial, cu posibilitate de degrevare a materiei, pondere 33%. Examen final, pondere 33%	66%
10.5 Seminar	- cunoasterea aplicarii, pe exemple concrete a elementelor teoretice exemplificate in cadrul cursului.	Notare în timpul semestrului, teme de casă.	33%
10.6 Standard minim de performanţă			
Cunoaşterea noţiunilor teoretice de bază prezentate la curs şi rezolvarea unor probleme tip.			

Data completării **01.09.2018**

Semnătura titularului de curs
lector dr. Emil Simion

Semnătura titularului de aplicaţii
lector dr. Emil Simion

Data avizării în departament
.....

Semnătura sefului de department
prof. dr. Mircea Olteanu

Responsabil program master
lector dr. Emil Simion