FIŞA DISCIPLINEI

1. Date despre program

1.1 Instituţia de învăţământ superior	Universitatea Babeş-Bolyai Cluj-Napoca
1.2 Facultatea	Facultatea de Matematică şi Informatică
1.3 Departamentul	Departamentul de Informatică
1.4 Domeniul de studii	Informatică
1.5 Ciclul de studii	Master
1.6 Programul de studiu / Calificarea	Sisteme Distribuite in Internet

2. Date despre disciplină

2.1 Denumirea disciplinei	Protocoale de securitate în comunicaţii						
2.2 Titularul activităţilor de curs	Lect. Dr. Bufnea Darius-Vasile						
2.3 Titularul activităţilor de seminar	Lect. Dr. Bufnea Darius-Vasile						
2.4 Anul de studiu	1	2.5 Semestrul	2	2.6. Tipul de evaluare	E	2.7 Regimul disciplinei	Obligatorie

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

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

Distribuţia fondului de timp:	ore
Studiul după manual, suport de curs, bibliografie şi notiţe	40
Documentare suplimentară în bibliotecă, pe platformele electronice de specialitate şi pe teren	50
Pregătire seminarii/laboratoare, teme, referate, portofolii şi eseuri	48
Tutoriat	10
Examinări	10
Alte activităţi:	0

3.7 Total ore studiu individual	158
3.8 Total ore pe semestru	200
3.9 Numărul de credite	8

4. Precondiţii (acolo unde este cazul)

4.1 De curriculum	• Arhitectura Calculatoarelor, Sisteme de operare, Reţele de calculatoare, Programare Web, Aritmetică modulară şi criptografie
4.2 De competenţe	• Cunoştinţe elementare despre structura şi modul de funcţionare a reţelei Internet, cunoştinţe elementare de criptografie, sisteme de operare, arhitectura calculatoarelor, baze de date, programare web, modelul client-server, algoritmică şi programare

5. Condiţii (acolo unde este cazul)

5.1 De desfăşurare a cursului	• Sală de curs dotată cu videoproiector
5.2 De desfăşurare a seminarului/laboratorului	•

6. Competenţele specifice acumulate

Competenţe profesionale	• Capacitate avansată de modelare a fenomenelor şi proceselor specifice din domenii economice, industriale şi ştiinţifice, folosind cunoştinţe fundamentale din matematică, statistică şi informatică • Capacitate avansată de analiză, proiectare şi construcţie a sistemelor informatice, folosind o gamă variată de platforme hardware şi software, limbaje şi medii de programare şi instrumente de modelare, verificare şi validare • Modelarea si conceptualizarea modelelor de proiectare / implementare pentru sisteme distribuite pe scară largă şi care comunică între ele prin canale nesigure (Internet). • Dezvoltarea de aplicaţii pe arhitecturi masiv paralele (cloud computing, structuri grid) şi a comunicaţiilor în timp real, mobile computing, wireless, bluetooth etc. • Conceperea şi utilizarea de modele pentru formalizarea conceptului de web semantic. • Capacitatea de a preda elevilor din ciclul liceal concepte şi teorii specifice informaticii, în măsura în care titularul diplomei de disertaţie în informatică posedă un certificat de absolvire a modulului de pregătire pedagogică
Competenţe transversale	• Cunoaşterea aprofundată a dezvoltărilor teoretice, metodologice şi practice specifice informaticii • Utilizarea sistematică a cunoştinţelor de specialitate în informatică la modelarea şi interpretarea unor situaţii noi, în contexte de aplicare mai largi decât cele cunoscute • Cunoaşterea şi utilizarea integrată a aparatului conceptual şi metodologic specific informaticii pentru soluţionarea unor situaţii incomplet definite, pentru rezolvarea unor probleme teoretice şi practice noi • Utilizarea nuanţată şi pertinentă a criteriilor şi metodelor de verificare, validare şi evaluare a soluţiilor software realizate, capacitatea de a formula judecăţi de valoare şi de a fundamenta deciziile constructive • Elaborarea şi conducerea de proiecte software complexe, de natură practică sau de cercetare, utilizând un spectru larg de metode cantitative şi calitative • Capacitate avansată de comunicare în medii profesionale diferite, de utilizarea adecvată a vocabularului informatic în comunicarea profesională, în limba engleză • Capacitate de lucru în echipă, asumarea de roluri de execuţie şi de conducere, realizarea sarcinilor profesionale în condiţii de autonomie şi responsabilitate

7. Obiectivele disciplinei (reieşind din grila competenţelor acumulate)

7.1 Obiectivul general al disciplinei	Cursul îşi propune aprofundarea de către cursant a celor mai bune mecanisme de securitate care pot fi implementate şi utilizate la elaborarea unui protocol, în Internet, la nivelul unui sistem de calcul, în elaborarea unei aplicaţii software.

7.2 Obiectivele specifice	Cursul grupează câteva subiecte avansate din domeniul securităţii în reţele de calculatoare. Cursul este structurat pe baza arhitecturii TCP/IP de organizare a reţelelor de calculatoare, aspectele teoretice orientându-se spre fiecare nivel şi set de protocoale din cadrul stivei TCP/IP. Cursul îşi propune: • să prezinte şi familiarizeze studentul cu algoritmii de criptare cei mai des întâlniţi precum şi cu diferitele protocoalele de la diverse nivele din stiva TCP/IP ce implementează aceşti algoritmi; • să familiarizeze studentul cu cele mai grave vulnerabilităţii în domeniu, precum şi cu mecanismele şi măsurile de luptă împotriva acestor vulnerabilităţi; • să prezinte cursanţilor principalele provocări de securitate pe care le ridică comerţul electronic pe Internet; • să abordeze din punct de vedere legal şi moral diferite subiecte precum infracţionalitatea pe Internet şi intimitatea utilizatorului; • să contribuie la înţelegerea acestor domenii prin studierea şi dezvoltarea unor aplicaţii practice relevante.

8. Conţinuturi

8.1 Curs	Metode de predare	Observaţii
1. Prezentarea bibliografiei şi structurii cursului. Cerinţe şi evaluare. Vulnerabilităţi informatice. Politici de securitate informatică la diferite nivele ale stivei TCP/IP.	Expuneri, explicaţii, exemple, studii de caz	
2. Istoria atacurilor informatice. Virusologie. Anatomia unui virus informatic. Sisteme antivirus.	Expuneri, explicaţii, exemple, studii de caz	
3. Securitatea sistemelor de operare. Securitatea sistemelor server în Internet. Arhitecturi de securitate în retelele Enterprise. Atacuri locale şi atacuri remote. Spyware si addware. Aplicaţii ale acestora in e-commerce.	Expuneri, explicaţii, exemple, studii de caz	
4. Anatomia unui exploit. Shell-code. Exemple.	Expuneri, explicaţii, exemple, studii de caz	
5. Mecanisme Firewall.	Expuneri, explicaţii, exemple, studii de caz	
6. Securitatea aplicaţiilor Web. SQL Injection. JavaScript Injection. SMTP Injection. Cross Site Scripting.	Expuneri, explicaţii, exemple, studii de caz	
7. Algoritmi de criptare bazaţi pe chei publice şi chei private. Semnături digitale. Certificate digitale.	Expuneri, explicaţii, exemple, studii de caz	
8. Infrastructuri bazate pe chei publice şi servicii asociate acestora.	Expuneri, explicaţii, exemple, studii de caz	
9. Securitatea poştei electronice. DKIM. Mecanisme antispam: bayesian spam filters, DNS based black lists. PGP.	Expuneri, explicaţii, exemple, studii de caz	
10. Protocoale de securitate la nivel reţea şi transport. IPSec. SSL si TLS. Securitate la nivel fizic si legatura de date.	Expuneri, explicaţii, exemple, studii de caz	
11. Vulnerabilităţi de tip Social Engineering. Infracţionalitatea informatică. Asigurarea intimităţii	Expuneri, explicaţii, exemple, studii de	

utilizatorului.	caz	
12. Smartcard-uri. Biometrice.	Expuneri, explicaţii, exemple, studii de caz	
13. Securitate în sistemul bancar şi plăţi electronice în Internet.	Expuneri, explicaţii, exemple, studii de caz	
14. Mecanisme şi scheme de autentificare. Kerberos.	Expuneri, explicaţii, exemple, studii de caz	

Bibliografie
1. V. V. Patriciu, M. Ene-Pietrosanu, C. Vaduva, I. Bica, N. Voicu, Securitatea Comerţului Electronic, Editura ALL
2. V. V. Patriciu, M. Ene-Pietrosanu, I. Bica, J. Priescu, Semnături Electronice şi Securitate Informatică, Editura ALL, 2006
3. Stalling Willliam, Cryptography and Network Security, Prentice Hall, 1999
4. Oskar Andreasson, Iptables Tutorial, http://www.frozentux.net/iptables-tutorial/iptables-tutorial.html
5. F. Cohen, A Short Course on Computer Viruses, Wiley Professional Computing, 2 edition, April 1994
6. Mostafa Hashem, Protocols for Secure Electronic Commerce, CRC Press, 2004
7. B. Gladman, C. Ellison, N. Bohm, Digital Signatures, Certificates and Electronic Commerce, http://jya.com/bg/digsig.pdf
8. O'Mahony D., Electronic Payment Systems for E-Commerce, Artech House, 2001
9. Ford W., Secure Electronic Commerce, Prentice Hall, 2001
10. Weidong Kou, Payment Technologies for E-Commerce, Springer Verlag 2003
11. Vancea, Al. si altii, Programarea in limbaj de asamblare 80x86, Exemple si aplicatii, pag. 317-323, Ed. Risoprint, 2005
12. Martin Boldt, Privacy-Invasive Software, cap. 2, cap. 7, Blekinge Institute of Technology, ISBN 978-91-7295-100-6

8.2 Seminar / laborator	Metode de predare	Observaţii
1. Vulnerabilităţi informatice. Virusologie. Anatomia unui virus informatic. Sisteme antivirus.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	Seminarul se desfăşoară din două în două săptămâni
2. Exploit-uri. Shell-code.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
3. Mecanisme Firewall.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
4. Securitatea aplicaţiilor Web	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
5. Algoritmi de criptare bazaţi pe chei publice şi chei private. Semnături digitale. Certificate digitale.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
6. Securitatea poştei electronice	Dezbaterea, dialogul, exemple, conversaţii de aplicare	
7. Protocoale de securitate la nivel reţea şi transport.	Dezbaterea, dialogul, exemple, conversaţii de aplicare	

Bibliografie
1. E. Rescorla, HTTP Over TLS, RFC 2818, May 2000
2. Kerberos: The Network Authentication Protocol, http://web.mit.edu/Kerberos/
3. T. Ylonen, C. Lonvick, The Secure Shell (SSH) Protocol Architecture, RFC 4251, January 2006
4. P. Hoffman, SMTP Service Extension for Secure SMTP over TLS, RFC 2487, January 1999

5. OpenSSL: The Open Source toolkit for SSL/TLS, www.openssl.org
6. T. Dierks, E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.1, RFC 4346, April 2006
7. S. Kent, Security Architecture for the Internet Protocol, RFC 2401, S. Kent, R. Atkinson

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

- Cursuri cu un conţinut similar există în planul de învăţământ al tuturor marilor universităţi din România şi din străinătate.
- Cursul abordează probleme fundamentale de securitate şi deosebit de actuale în Internet.
- Conţinutul cursului acoperă principalele aspecte necesare a fi însuşite de către cursant pentru a ocupa cu succes o poziţie corespunzătoare în cadrul unei companii de profil.

10. Evaluare

Tip activitate	10.1 Criterii de evaluare	10.2 Metode de evaluare	10.3 Pondere din nota finală
10.4 Curs	Cunoaşterea principalelor aspecte teoretice prezentate la curs	Examen parţial din prima jumătate a materiei	1/4
	Cunoaşterea principalelor aspecte teoretice prezentate la curs	Examen final din a doua jumătate a materiei	1/4
10.5 Seminar/laborator	Elaborarea unui referat şi a unui proiect pe o temă de securitate stabilită de comun acord de cursant cu cadrul didactic dintre cele discutate la seminar.	Susţinere orală de către cursant	1/2
10.6 Standard minim de performanţă			
Pentru promovare trebuie cumulate următoarele două condiţii: • prezentarea referatului şi a proiectului, activitate ce trebuie notată cel puţin cu nota 5; • minim media 5 între nota examenului parţial şi cea obţinuta la examenul din sesiune.			

Data completării	Semnătura titularului de curs	Semnătura titularului de seminar
.....	Lect. Dr. Bufnea Darius-Vasile	Lect. Dr. Bufnea Darius-Vasile

Data avizării în departament	Semnătura directorului de departament
.....	….....