FIŞA DISCIPLINEI

1. Date despre program

1.1. Instituţia de învăţământ superior	***Universitatea de Medicină, Farmacie, Ştiinţe şi Tehnologie din Tîrgu-Mureş***
1.2. Şcoala Doctorală	***Şcoala Doctorală de Litere, Ştiinţe Umaniste şi Aplicate***
1.3. Domeniul fundamental	***Matematică şi ştiinţe ale naturii***
1.4. Domeniul de doctorat	***Informatică***
1.5. Ciclul de studii	***Doctorat***

2. Date despre disciplină

2.1. Denumirea disciplinei	***Securitatea reţelelor de calculatoare complexe***						
2.2. Titularul activităţilor de curs				***Conf. dr. ing. habil. Genge Béla***			
2.3. Titularul activităţilor de seminar				***Conf. dr. ing. habil. Genge Béla***			
2.4. Anul de studiu	I	2.5. Semestrul	1	2.6. Tipul de evaluare	ES	2.7. Regimul disciplinei	DO

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

3.1. Număr de ore pe săptămână	**4**	***din care: 3.2. curs***	**2**	***3.3. seminar***	**2**
3.4. Total ore din planul de învăţământ	**56**	***din care: 3.5. curs***	**28**	***3.6. seminar***	**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 şi pe teren					**30**
Pregătire seminarii/ laboratoare/ proiecte, teme, referate, portofolii şi eseuri					**46**
Tutoriat					**10**
Examinări					**3**
Alte activităţi.....					
Total					**119**

3.7. Total ore studiu individual	**119**
3.8. Total ore pe semestru	**175**
3.9. Numărul de credite	**7**

4. Precondiţii (acolo unde este cazul)

4.1. de curriculum	-
4.2. de competenţe	Absolvent de licenţă şi masterat

5. Condiţii (acolo unde este cazul)

5.1. de desfăşurare a cursului	•
5.2. de desfăşurare a seminarului	•

6. Competenţe specifice acumulate

Competenţe profesionale	C 1 - Elaborarea unui Plan de cercetare cuprinzând experienţele pe care se va baza Teza de doctorat C2 - Consultarea şi bibliografierea literaturii de specialitate în domeniu în vederea motivării alegerii temei de cercetare propusă pentru Teza de doctorat C3 - Aprofundarea cunoştinţelor privind aplicarea problemelor de optimizare liniară, a calculului probabilistic, a metodelor de analiză a datelor (PCA, clustering) pentru rezolvarea unor probleme reale
Competenţe transversale	CT.1 - Soluţionarea eficientă a situaţiilor problemă cu grad mediu de dificultate, cu respectarea principiilor şi a normelor de etică profesională şi promovarea unei atitudini responsabile faţă de pregătirea universitară prin doctorantură CT.2 - Aplicarea eficientă a tehnicilor de comunicare şi de relaţionare la nivel organizaţional sau de grup profesional în conditiile asumării de roluri specifice diferitelor niveluri ierarhice CT.3 - Autoevaluarea nevoii de formare profesională, de evoluţie în profesie, de dezvoltare a competenţelor dobândite şi de adaptare la cerinţele unei societăţi dinamice

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

7.1. Obiectivul general al disciplinei	Disciplina îşi propune să familiarizeze studenţii doctoranzi cu ultimele cercetări în domeniul reţelelor complexe. Sunt analizate comunicaţiile în reţele industriale distribuite, respectiv în domenii emergente precum Internet of Things, respectiv Software-Defined Networks. Sunt prezentate atacuri şi probleme de proiectare, respectiv soluţiile pentru securizarea acestor reţele. Disciplina îşi propune totodată să aprofundeze cunoştinţele studenţilor doctoranzi cu privire la aplicaţiile metodelor matematice în rezolvarea unor probleme reale şi de interes actual.
7.2. Obiectivele specifice	- Familiarizarea cu arhitectura, protocoalele, problemele şi soluţiile de securitate în reţele complexe.

	- Familiarizarea cu probleme de securitate specifice în domenii emergente precum Internet of Things şi Software-Defined Networks. - Elaborarea de soluţii de proiectare pentru securizarea reţelelor complexe utilizând metode din teoria probabilităţilor, teoria optimizărilor, etc. - Elaborarea metodelor pentru analiza datelor şi detectarea anomaliilor în reţele complexe. - Elaborarea infrastructurii de cercetare pentru studiul securităţii reţelelor complexe.

8. Conţinuturi

8.1. Curs	Metode de predare	Observaţii
• Introducere. Arhitectura reţelelor de calculatoare complexe. Exemple: reţele backbone, infrastructura IT din domeniul transmisiei şi distribuţiei energiei electrice, reţele de tip Internet of Things (IoT). Atacuri cibernetice în reţele complexe.	Prelegerea, problematizarea, conversaţia, explicaţia	2 cursuri
• Rolul criptografiei în protejarea reţelelor. Concepte principale, triada CIA (Confidentiality, Integrity, Availability), Arhitectura de securitate ITU-T X.800. Rolul numerelor aleatoare criptografice. Algoritmi criptografici. Criptografia simetrică şi asimetrică. Funcţii hash. Semnătura digitală.	Prelegerea, problematizarea, conversaţia, explicaţia	2 cursuri
• Protocoale de securitate în reţele complexe. Protocoalele TLS, IPSec, SSH.	Prelegerea, problematizarea, conversaţia, explicaţia	1 curs
• Securitatea în reţele Multi Protocol Label Switching (MPLS). Architectura, protocoale, izolarea traficului. Experimente de securitate. Atacuri şi soluţii.	Prelegerea, problematizarea, conversaţia, explicaţia	1 curs
• Securitatea în reţele Internet of Things. Architectura, protocoale, echipamente. Experimente de securitate. Soluţii pentru securizarea reţelelor IoT.	Prelegerea, problematizarea, conversaţia, explicaţia	1 curs
• Securitatea reţelelor Software-Defined Networks (SDN). Arhitectura. Controlul centralizat, reconfigurarea. Experimente de securitate. Atacuri şi soluţii.	Prelegerea, problematizarea, conversaţia, explicaţia	1 curs
• Proiectarea infrastructurii de comunicaţie pentru securizarea reţelelor complexe. Probleme de optimizare liniară pentru garantarea lăţimii de bandă, criptarea comunicaţiei, plasarea elementelor de monitorizare şi detecţie, crearea zonelor de securitate, garantarea aspectelor de QoS. Algoritmi heuristici pentru rezolvarea problemelor. Experimente.	Prelegerea, problematizarea, conversaţia, explicaţia	2 cursuri
• Monitorizarea traficului şi detecţia anomaliilor. Aplicarea metodelor de outlier detection din teoria probabilităţilor. Analiza PCA, tehnici de clustering (K-means, Gaussian mixture model).	Prelegerea, problematizarea, conversaţia, explicaţia	2 cursuri
• Infrastructuri de cercetare cu reţele complexe. Principii de proiectare a unei infrastructuri de cercetare cu reţele complexe. Infrastructura Emulab. Infrastructura EPIC. Experimente de securitate.	Prelegerea, problematizarea, conversaţia, explicaţia	2 cursuri
BIBLIOGRAFIE		

- W. Stallings, L. Brown: *Computer security: Principles and practice*, Ed. Pearson Prentice Hall, 2008.
- B.A. Forouzan: *Introduction to cryptography and network security*, Ed. McGraw-Hill, 2008.
- L.H. Chiang, E.L. Russel, and R.D. Braatz: *Fault Detection and Diagnosis in Industrial Systems*, Ed. Springer-Verlag, 2002.
- B. Genge, P. Haller, A.V. Duka: *Engineering security-aware control applications for data authentication in smart industrial cyber-physical systems*, Future Generation Computer Systems, vol. 91, February 2019, Pages 206-222, 2019.
- B. Genge, P. Haller, C.D. Dumitru, C. Enachescu: *Designing Optimal and Resilient Intrusion Detection Architectures for Smart Grids*, IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2440-2451, Sept. 2017.
- P. Haller, B. Genge: *Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems*, IEEE Access, vol. 5, pp. 9336-9347, 2017.
- B. Genge, C. Enachescu: *ShoVAT: Shodan-based vulnerability assessment tool for Internet-facing services, Security and communication networks*, Wiley, Volume 9, Issue 15, pp. 2696-2714, 2016.
- B. Genge, P. Haller: *A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems*, IEEE/IFIP Networking, Vienna, Austria, pp. 73-81, 2016.
- B. Genge, F. Graur, P. Haller: *Experimental Assessment of Network Design Approaches for Protecting Industrial Control Systems*, International Journal of Critical Infrastructure Protection, Elsevier, vol. 11, pp. 24-38, 2015.
- I. Kiss, B. Genge, P. Haller: *A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems*, INDIN 2015 IEEE International Conference on Industrial Informatics, pp. 142-148, 22-24 July 2015.
- B. Genge, I. Kiss, P. Haller: *A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures*, International Journal of Critical Infrastructure Protection, Elsevier, Volume 10, pp. 3-17, 2015.
- B. Genge, P. Haller, I. Kiss: *A Linear Programming Approach for K-Resilient and Reliability-Aware Design of Large-Scale Industrial Networks*, International Conference on Ad Hoc, Mobile, and Wireless Networks (ADHOC-NOW), Lecture Notes in Computer Science, Volume 9143, Athens, Greece, pp. 288-302, 2015.
- C. Siaterlis, B. Genge: *Cyber-physical testbeds*, Communications of the ACM, Vol. 57, No. 6, pp. 64-73, June 2014.
- B. Genge, C. Siaterlis: *Analysis of the Effects of Distributed Denial-of-Service Attacks on MPLS Networks*, International Journal of Critical Infrastructure Protection, Elsevier, Volume 6, Issue 2, pp. 87-95, 2013.
- C. Siaterlis, B. Genge, M. Hohenadel: *EPIC: A testbed for scientifically rigorous cyber-physical security experimentation*, IEEE Transactions on Emerging Topics in Computing, Volume 1, Issue 2, pp. 319-330, 2013.

8.2 . Seminar	Metode de predare-învățare	Observații
• OptimalFlow: instalare, configurare, realizarea de experimente.	Rezolvare aplicații practice.	2 seminarii
• Construirea unei probleme de optimizare liniară. Rezolvarea cu softul AIMMS. Generarea fișierului LP. Integrarea și rularea în OptimalFlow.	Rezolvare aplicații practice.	3 seminarii
• CAIA: instalare, configurare, realizarea de experimente. Simularea atacurilor cibernetice în rețele de transport a energiei electrice. Măsurarea și evaluarea impactului.	Rezolvare aplicații practice împreună cu studenții.	2 seminarii
• Aplicarea metodei CAIA în proiectarea rețelelor complexe. Construirea și rezolvarea unei probleme de optimizare liniară pentru rețele complexe folosind AIMMS.	Rezolvare aplicații practice împreună cu studenții.	2 seminarii
• Aplicarea metodelor din teoria probabilităților și statisticii, a metodelor PCA și de clustering pentru detecția anomaliilor. Analiza datelor generate din modele industriale: Tennessee-Eastman, Vinyl acetate model, Automotive Catalyst model.	Rezolvare aplicații practice împreună cu studenții.	2 seminarii
• Elaborarea unei metode pentru închiderea buclei dintre detecție și mitigare a atacurilor cibernetice. De la detecția anomaliilor la OptimalFlow.	Rezolvare aplicații practice împreună cu studenții.	2 seminarii
• Verificarea cunoștințelor. Prezentarea referatelor.	Verificare	1 seminar

BIBLIOGRAFIE

- L.H. Chiang, E.L. Russel, and R.D. Braatz: *Fault Detection and Diagnosis in Industrial Systems*, Ed. Springer-Verlag, 2002.
- P. Haller, B. Genge: *Using Sensitivity Analysis and Cross-Association for the Design of Intrusion Detection Systems in Industrial Cyber-Physical Systems*, IEEE Access, vol. 5, pp. 9336-9347, 2017.
- B. Genge, P. Haller: *A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems*, IEEE/IFIP Networking, Vienna, Austria, pp. 73-81, 2016.
- B. Genge, I. Kiss, P. Haller: *A system dynamics approach for assessing the impact of cyber attacks on critical infrastructures*, International Journal of Critical Infrastructure Protection, Elsevier, Volume 10, pp. 3-17, 2015.
- B. Genge, P. Haller, I. Kiss: *A Linear Programming Approach for K-Resilient and Reliability-Aware Design of Large-Scale Industrial Networks*, International Conference on Ad Hoc, Mobile, and Wireless Networks (ADHOC-NOW), Lecture Notes in Computer Science, Volume 9143, Athens, Greece, pp. 288-302, 2015.
- I. Kiss, B. Genge, P. Haller: *A Clustering-based Approach to Detect Cyber Attacks in Process Control Systems*, INDIN 2015 IEEE International Conference on Industrial Informatics, pp. 142-148, 22-24 July 2015.
- AIMMS: Prescriptive Analytics and Supply Chain Management, https://aimms.com/
- OptimalFlow: A Hierarchical Control Plane for Software-Defined Networks-based Industrial Control Systems,

http://upm.ro/sereniti/optimalflow.html/

- Cyber-security-aware network design tool-suite for Networked Critical Infrastructures, http://upm.ro/sereniti/netdesign.html/
- Cross-Association and Cyber Attack Impact Assessment tool, http://upm.ro/sereniti/CrossCAIA.html/

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

Având în vedere contextul internațional actual, există o acută nevoie de specialiști în domeniul securității cibernetice, acest aspect fiind subliniat și la nivelul Comisiei Europene în August 2016, prin directiva Nr. 1148/2016 asupra securității rețelelor și a informației, care precizează necesitatea implementării de măsuri suplimentare de securitate cibernetică la nivel Pan-European. În consecință, conținutul disciplinei este coroborat cu problemele de securitate cibernetică actuale, fiind menită să familiarizeze studenții doctoranzi cu problemele actuale cu care se confruntă specialiștii în domeniu, cu vulnerabilitățile serviciilor informatice, dar și cu metodele de prevenire a atacurilor. Totodată, conținutul este coroborat cu cerințele angajatorilor de specialitate, diversele aspecte ale securității fiind astăzi o parte integrată în majoritatea aplicațiilor software.

10. Evaluare

Tip activitate	10.1. Criterii de evaluare	10.2. Metode de evaluare	10.3. Pondere din nota finală
10.4. Curs	Cunoaşterea arhitecturii, a protocoalelor şi a problemelor de securitate în reţele complexe. Elaborarea de probleme de optimizare liniară pentru proiectarea optimă a reţelelor. Identificarea metodelor matematice potrivite pentru analiza datelor şi identificarea anomaliilor.	Examen practic+scris	40%
10.5. Seminar	Realizarea de experimente de securitate cu sisteme Software-Defined Networks. Rezolvarea problemelor de optimizare liniară. Elaborarea şi implementarea metodelor de analiză a datelor pentru detectarea anomaliilor. Elaborarea referatelor ştiinţifice.	Referate, analize, aplicaţii practice, intervenţii, prezenţă	60%

10.6 Standard minim de performanţă

- Realizarea de experimente cu reţele SDN utilizând OptimalFlow.
- Elaborarea şi rezolvarea unor probleme de optimizare liniară pentru proiectarea comunicaţiilor reţelelor complexe.
- Elaborarea unei metode pentru detectarea anomaliilor în reţele complexe.
- Participarea activă la cursurile şi seminariile disciplinei.

Data completării
02.11.2018

Semnătura titularului de curs

Conf. univ. dr. ing. habil. Genge Béla

Semnătura titularului de seminar

Conf. univ. dr. ing. habil. Genge Béla

Data avizării în CSD
15.01.2019

Semnătura directorului Şcolii Doctorale,

Prof. univ. dr. Al. Cistelecan