MINISTERUL EDUCAŢIEI ȘI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică și Microelectronică
Departamentul Inginerie Software și Automatică

Admis la susținere
Șef departament:
Fiodorov Ion, conf. univ., dr.

_____

„____”_____ 2021

ASPECTE RELEVANTE PRIVIND PROTECȚIA INFRASTRUCTURILOR INFORMATICE CRITICE

Teză de master

Student: **Nicolae PANFILII**

Conducător: **prof. univ., dr.hab. Ion BOLUN**

Chișinău, 2022

ADNOTARE

la teza de master **„Aspecte relevante privind protecția infrastructurilor informatice critice”** a masterandului din grupa SI-201M, specialitatea **„Securitate informațională”,**

PANFILII Nicolae

În prezenta lucrare este expusă problema asupra căreia statul și organizațiile comerciale ar trebui să se concentreze, precum și unele exemple de soluții care ar putea duce la creșterea gradului de securitate infrastructurilor informatice critice.

Teza cuprinde introducerea, patru capitole, concluzii, bibliografia din 63 titluri, 1 anexă şi este perfectată pe 82 pagini de text de bază, inclusiv 9 figuri.

Scopul și obiectivul general al lucrării este cercetarea asupra domeniului asigurării protecției infrastructurii critice la nivel național prin prisma abordărilor internaționale. **Obiectivele cercetării** sunt: definirea conceptului de protecție a infrastructurilor critice; stabilirea unui grad acceptabil al rezilienței – sub aspect conceptual, teoretic, precum și în privința implicațiilor sociale, noutăților de abordare în privința ordinii publice și siguranței naționale; analiza și evaluarea multi-risc privind producerea unor situații de urgență.

Ca **metodologii de cercetare**, au fost utilizate: metoda observației, studiul documentelor actelor normative, procedurilor, legislației internaționale, analiza de conținut, metodele comparative și cazuistice, metodele de prezentare statistică și grafică, studiul de caz sau analiza situațională. Culegerea informațiilor și colectarea datelor de lucru s-a realizat prin folosirea statisticilor planurilor operative, analizelor de risc, procedurilor operaționale.

Motivația alegerii acestei teme este generată de stadiul de cunoaștere limitat în domeniul pe care demersul științific îl urmărește. Cercetarea în domeniul pe care îl propun se află încă la început, deoarece chiar această abordare este una în stadiul de inovație.

Astfel, în urma cercetărilor efectuate putem concluziona că protecția infrastructurilor critice cuprinde o activitate desfășurată succesiv în ceea ce privește analiza și evaluarea riscurilor, asigurarea protecției informațiilor clasificate, realizarea planurilor de securitate ale operațiunilor de infrastructură critică, stabilirea punctelor de control și a modului de realizare a comunicațiilor, precum și exerciții, rapoarte, reevaluări și reactualizări ale documentelor elaborate.

Cuvinte-cheie: infrastructură critică, securitate, riscuri, SCADA, standard, analiza vulnerabilităților, IACS, protocol.

ANNOTATION

to the graduate work **„Relevant aspects regarding the protection of critical IT infrastructures"** of the student from SI-201M group, specialty **„Information security",**

PANFILII Nicolae

This paper addresses the issue that the state and business organizations should focus on, as well as some examples of solutions that could increase the security of critical IT infrastructures.

The thesis includes the introduction, four chapters, conclusions, bibliography of 63 titles, 1 appendix and is written on 82 pages of basic text, including 9 figures.

The aim and general objective of the paper is the research on the field of ensuring the protection of critical infrastructure at national level through the prism of international approaches. **The objectives of the research** are: defining the concept of critical infrastructure protection; establishing an acceptable degree of resilience - conceptually, theoretically, as well as in terms of social implications, new approaches to public order and national security; multi-risk analysis and assessment of emergencies.

As **research methodologies**, the following were applied: observation method, normative documents, procedures, international law, content analysis, comparative and case studies methods, statistical presentation methods and case study situational analysis. The collection of information and the collection of work data was done by using statistics of operational plans, risk analysis, operational procedures.

The motivation for choosing this topic is generated by the state of limited knowledge in the field that the scientific approach pursues. The research in the field I am proposing is still in its infancy, as this approach is one of innovation.

Thus, following the research we can conclude that the protection of critical infrastructure includes a successive activity in terms of risk analysis and assessment, ensuring the protection of classified information, implementation of security plans for critical infrastructure operations, stability of control points and implementation of communications, as well as exercises, reports, reassessments and updates of the documents prepared.

Keywords: critical infrastructure, security, risks, SCADA, standard, vulnerability analysis, IACS, protocol.

CUPRINS

Lista abrevierilor

art. - articol
alin. - alineat
CIP - Critical Infrastructure Protection
CISA - Cybersecurity and Infrastructure Security Agency
CNCPIC - Centrul Național de Coordonare a Protecției Infrastructurilor Critice
CSAT - Consiliul Suprem de Apărare a Țării
GOOSE - Generic Object-Oriented Substation Events
IC - Infrastructură Critică
ICN/ICE - Infrastructură Critică Națională/Infrastructură Critică Europeană
IGSU - Inspectoratul General pentru Situații de Urgență
IEEE - Institute of Electrical and Electronics Engineers
IP - Internet Protocol
IT - Information Technology
KB - kilobyte
NATO - North Atlantic Treaty Organization
NIST - National Institute of Standards and Technology
NERC - North American Electric Reliability Corporation
nr. - număr
MHz - megahertz
PEPIC - Programul european de protecție a infrastructurilor critice
PIC - Protecția Infrastructurilor Critice
RAM - Read-Access Memory
RFID - Radio-Frequency Identification
ROM - Read-Only Memory
S.A. - Societate pe Acțiuni
SCADA - Supervisory Control And Data Acquisition
SUA - Statele Unite ale Americii
TCP - Transmission Control Protocol
TIC - Tehnologia Informației și Comunicațiilor
TLS - Transport Layer Security
UE - Uniunea Europeană

Lista figurilor

INTRODUCERE

Complexitatea și diversitatea riscurilor și amenințărilor, tot mai interconectate și caracterizate prin determinări multiple, reclamă o abordare integratoare, sistemică și comprehensivă a obiectivelor de securitate, cu accent pe protejarea acelor componente vitale pentru siguranța și buna desfășurare a vieții socio-economice.

Activitatea de protecție a infrastructurilor critice nu mai ține cont de granițele naționale și implică eforturi comune, în sensul identificării și evaluării oricăror puncte vulnerabile ale acestora. Ca atare, protecția infrastructurilor critice – element determinant pentru menținerea stării de stabilitate și securitate – impune amplificarea preocupărilor principalilor actori internaționali (state și organizații internaționale) de elaborare și armonizare a unor strategii în domeniu.

Acestea trebuie să permită identificarea și avertizarea timpurie a riscurilor, concomitent cu adoptarea și inițierea oportună a deciziilor/demersurilor de intervenție preventivă și contracarare. Infrastructurile critice au reprezentat, din totdeauna, cel mai sensibil și cel mai vulnerabil domeniu al oricărui sistem și proces. Sensibilitatea acestora decurge din rolul lor deosebit pe care îl dețin în cadrul structurii.

Oricât de bine ar fi protejate, infrastructurile critice vor avea întotdeauna un grad de vulnerabilitate ridicat, întrucât, de regulă, sunt primele vizate atunci când se urmărește destabilizarea și chiar distrugerea unui sistem sau unui proces sau atunci când se produce o situație de urgență.

Identificarea, optimizarea și securizarea infrastructurilor critice reprezintă o prioritatea indiscutabilă pentru structurile care au rolul de protecție, prevenire și gestionare a situațiilor de urgență sau dezastrelor de orice natură.

Infrastructurile critice nu sunt și nu devin critice, doar la atacuri sau din cauza atacurilor, ci și din alte cauze, unele dintre acestea greu de depistat și de analizat, altele mai ușor de recunoscut prin crearea unor scenarii privind analiza riscurilor.

De aceea, analiza problematicii infrastructurilor critice trebuie să țină seama de toate dimensiunile și implicațiile stabilității și funcționalității sistemelor și proceselor, precum și de înlănțuirile cauzale care pot genera sau influența dinamica lor.

Infrastructura critică este legată de tot ceea ce susține viabilitatea unei societăți, începând cu administrația, instituțiile economico-financiare, serviciile publice, de asistență socială și de sănătate, comunitățile de informații, armată și terminând cu rezervele de hrană, transportul, comunicațiile, apă și energie, educația și cercetarea sau mass-media.

Protecția infrastructurilor critice reprezintă un domeniu care se dorește a fi foarte bine investigat, monitorizat, analizat, evaluat, prognozat şi ameliorat. Atât Uniunea Europeană cât și Statele Unite ale

Americii sau alte state, alianțe, structuri de securitate internaționale, regionale își intensifică eforturile pentru a identifica, supraveghea, optimiza şi proteja infrastructurile critice/vitale ale țărilor, societăților, rețelelor și ale lumii.

Obiectivul general al lucrării este cercetarea asupra domeniului asigurării protecției infrastructurii critice la nivel național. Obiectivele specifice ale cercetării sunt: definirea conceptului de protecție a infrastructurilor critice; stabilirea unui grad acceptabil al rezilienței – sub aspect conceptual, teoretic, precum și în privința implicațiilor sociale, noutăților de abordare în privința ordinii publice și siguranței naționale; analiza și evaluarea multi-risc privind producerea unor situații de urgență.

Ca metode de cercetare, am utilizat metoda observației, studiul documentelor actelor normative, procedurilor, legislației internaționale, analiza de conținut, metodele comparative și cazuistice, metodele de prezentare statistică și grafică, studiul de caz sau analiza situațională. Culegerea informațiilor și colectarea datelor de lucru s-a realizat prin folosirea statisticilor planurilor operative, analizelor de risc, procedurilor operaționale.

Motivația alegerii acestei teme este generată de stadiul de cunoaștere limitat în domeniul pe care demersul științific îl urmărește. Cercetarea în domeniul pe care îl propun se află încă la început, deoarece chiar această abordare este nouă. Conceptele de bază sunt în continuare dezbătute, astfel sintagma infrastructură critică este definită atât din punct de vedere militar, cât și economic, social ori academic.

Astfel, pe lângă adâncirea unor aspecte teoretice, tema lucrării oferă posibilitatea dezvoltării unor considerații cu aplicabilitate practică de interes pentru cei ce activează în aceste domenii, în contact direct cu unitățile de intervenție și suport.

BIBLIOGRAFIE

1. Congressional Budget Office – *Report on Public Works Infrastructure*: Policy Considerations of the 1980s, 1983. Disponibil: https://www.cbo.gov/sites/default/files/98th-congress-1983-1984/reports/doc20-entire.pdf, Accesat la 10.09.2021.
2. Ordinul executiv al Președintelui SUA nr. 13010 privind protecția infrastructurilor critice, Disponibil: https://irp.fas.org/offdocs/eo13010.htm, Accesat la 08.09.2021.
3. The National Strategy to Secure Cyberspace, february 2003, pag. VII, Disponibil: https://www.energy.gov/sites/prod/files/National%20Strategy%20to%20Secure%20Cyberspace.pdf, Accesat la 11.09.2021.
4. DEDIU, George, MANAFU, Alexandru, „*Protecția infrastructurilor critice – o nouă provocare*" în „*Provocări la adresa securității și strategiei la începutul secolului XXI*", Sesiunea de comunicări științificce cu participare internațională – 14-15 aprilie 2005, Editura Universității Naționale de Apărare, București, 2005, ISBN 973-663-182-6;
5. ALEXANDRESCU, Grigore, VĂDUVA, Gheorghe, „Infrastructuri critice: Pericole, ameninţări la adresa acestora: Sisteme de protecţie", Editura Universităţii Naţionale de Apărare „Carol I", Bucureşti: 2006, ISBN 973-663-412-4;
6. About Critical Infrastructure, Public Safety Canada, Disponibil: https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx, Accesat la 16 septembrie 2021
7. National Strategy for Critical Infrastructure, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/srtg-crtcl-nfrstrctr-eng.pdf, ISBN: 978-1-100-11248-0
8. National infrastructure protection plan (NIPP) 2013: Partnering for critical infrastructure security and resilience, Disponibil: https://www.cisa.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf, Accesat la 14.09.2021.
9. Critical infrastructure sectors, Disponibil: https://www.cisa.gov/critical-infrastructure-sectors, Accesat la 14.09.2021.
10. Critical Infrastructure Protection in Germany. Federal Office for Information Security Disponibil: https://www.kritis.bund.de/SubSites/Kritis/EN/introduction/introduction_node.html, Accesat la 15.09.2021;
11. Green paper on an european programme for critical infrastructure protection (presented by the Commission) COM (2005) 576 final, Bruxelles, Belgium, 17 november 2005, Disponibil: https://eur-

lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN, Accesat la 16.09.2021

12. European programme for critical infrastructure protection, COM2006-786, Disponibil: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52006DC0786&from=EN, Accesat la 17.09.2021.
13. Directiva 2008/114/CE a Consiliului din 8 decembrie 2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora, accesat la 27.09.2021 Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32008L0114&from=RO, Accesat la 18.09.2021
14. Hotărâre nr. 36 din 18 decembrie 2001 privind adoptarea Strategiei de securitate naţională a României, publicată în Monitorul Oficial nr. 822/20, dec. 2001. Disponibil: http://www.cdep.ro/pls/legis/legis_pck.htp_act_text?idt=31060, Accesat la 18.09.2021.
15. Ordonanța de Urgență a Guvernului României nr. 98 din 3 noiembrie 2010 privind identificarea, desemnarea și protecția infrastructurilor critice, publicată în Monitorul Oficial al României nr. 757 din 12 noiembrie 2010, Disponibil: http://legislatie.just.ro/Public/DetaliiDocument/123547, Accesat la 18.09.2021;
16. Regulamentul privind protecția antiteroristă a infrastructurii critice, aprobat prin Hotărârea Guvernului nr. 701 din 11.07.2018, publicat la 27.07.2018 în Monitorul Oficial nr. 277-284, art. 773.
17. Proiectul de lege privind protejarea obiectelor de infrastructură esențială pentru asigurarea securității naționale și a ordinii publice, Disponibil: http://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/5019/language/ro-RO/Default.aspx, Accesat la 18.09.2021.
18. RINALDI S., PEERENBOOM, J., KELLY T. Identifying, understanding, analysing critical infrastructure interdependencies. In: *IEEE Control Systems Magazine*, vol. 21, pp. 11-25, 2001. ISSN: 1066-033X;
19. ALCARAZ, C., LOPEZ J. Analysis of requirements for critical control systems. In: *International Journal of Critical Infrastructure Protection*, Elsevier, vol. 2, pp.137-145, 2012. ISSN: 1874-5482;
20. HARRISON, K., WHITE G., A taxonomy of cyber events affecting communities. In: 44th Hawaii International Conference on System Sciences (HICSS), IEEE, 2011. ISBN: 978-1-4244-9618-1
21. ZHU B., JOSEPH A., SASTRY S. A taxonomy of cyber attacks on SCADA systems. In: *4th International Conference on Cyber*, Physical and Social Computing, 2011. ISBN: 978-1-4577-1976-9

22. SURESH, K., KIRUBASHANKAR, R., KRISHNAMURTHY K. Research of Internet based supervisory control and information system. In: *International Conference on Recent Trends in Information Technology (ICRTIT)*, pp. 1180-1185, 2011. ISBN: 978-1-4577-0588-5
23. ADNAN, S., MARINKOVIC, V., CICO, Z., KARAVDIC E., DELIC N. Web based multilayered distributed SCADA/HMI system in refinery application. In: *Computer Standard Interfaces*, vol. 31, pp. 599-612, 2009. ISSN: 0920-5489
24. JAIN, M., JAIN, A., SRINIVAS M., A web-based expert system shell for fault diagnosis and control of power system equipment. In: *International Conference Condition Monitoring and Diagnosis (CMD)*, pp. 1310-1313, 2008. ISBN: 978-1-4244-1621-9
25. RIMAL, B., LUMB, I., A taxonomy and survey of cloud computing systems [online]. In: *Fifth International Joint Conference on INC, IMS and IDC*, pp. 44-51, 2009 [citat 11.10.2021]. ISBN: 978-0-7695-3769-6/09 Disponibil: https://cdn.manesht.ir/4198___Intro.2[1].pdf
26. ALCARAZ, C., LOPEZ, J., A security analysis for wireless sensor mesh networks in highly critical systems. In: IEEE Transactions on Systems, Man, Cybernetics, Part C: Applications and Reviews, vol. 40, pp. 419-428, 2010, ISSN 1094-6977.
27. KARNOUSKOS, S., The cooperative Internet of Things enabled Smart Grid. In: *14th IEEE International Symposium on Consumer Electronics*, pp. 16, 2010.
28. ALCARAZ, C., FERNANDEZ-GAGO, C., LOPEZ, J., An early warning system based on reputation for energy control systems. In: *IEEE Transactions on Smart Grid*, vol. 2, pp. 827-834, 2011. ISSN: 1949-3053
29. ALCARAZ, C., ROMAN, R., NAJERA P., LOPEZ, J., Security of industrial sensor network-based remote substations in the context of the Internet of things. In: *Ad Hoc Networks*, Elsevier, vol. 11(3), pp. 1091-1104, 2013. ISSN: 1570-8705.
30. CEN/CENELECT/ETSI Cyber Security Coordination Group: "White Paper No. 01 – Recommendations for a Strategy on European Cyber Security Standardisation", 2014
31. Department of Homeland Security: "Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritization, and Protection", 2003
32. ORGANIZAȚIA MONDIALĂ DE STANDARDIZARE. Standardul IEC/ISO 27001:2018 Tehnologia informației - Tehnici de securitate - Sisteme de management al securității informațiilor – Cerințe. Aprobat: 2018-02, accesat la 22.09.2021, Disponibil: https://akela.mendelu.cz/~lidak/IPI/ISO_IEC_27000_2018.pdf

33. ORGANIZAȚIA MONDIALĂ DE STANDARDIZARE. Standardul ISO / IEC 15408:2009 - Tehnologia informației - Tehnici de securitate - Criterii de evaluare pentru securitatea IT, Aprobat: 2009-12, Localizare: UE.
34. INSTITUTUL NAȚIONAL DE STANDARDIZARE ȘI TEHNOLOGIE. Publicația specială NIST 800-53 - Controale de securitate și confidențialitate pentru sisteme de informație și organizații. Aprobat: 2020-09-23, Localizare: SUA.
35. INSTITUTUL NAȚIONAL DE STANDARDIZARE ȘI TEHNOLOGIE. Raport intern sau interinstanțial (IR) NIST 7628 - Ghid pentru securitatea cibernetică a rețelelor inteligente. Aprobat: 2014-09. Localizare: SUA.
36. NERC: North American Electric Reliability Corporation [citat 11.10.2021], Disponbil: https://www.nerc.com/pa/Stand/Pages/AllReliabilityStandards.aspx?jurisdiction=United%20States
37. ANSI/ISA-62443. Securitate pentru sisteme de automatizare și control industrial. Aprobat: 2009-07. Localizare: SUA. Accesat la 01.10.2021, Disponibil: http://www.icsdefender.ir/files/scadadefender-ir/paygahdanesh/standards/ISA-62443-2-1-Public.pdf
38. IEC 62351 - Managementul sistemelor de alimentare și schimbul de informații asociate - Securitatea datelor și comunicațiilor. Aprobat: 2007-05-15. Localizare: UE.
39. SCHLEGEL, R., OBERMEIER, S., SCHNEIDER, J., A security evaluation of IEC 62351. In: *Journal of Information Security and Applications 34* [online], pp. 197–204, 2017 [citat 01.10.2021]. Disponibil: https://www.researchgate.net/publication/303914771_A_security_evaluation_of_IEC_62351
40. STROBEL, M., WIEDERMANN, N., ECKERT, C., Novel weaknesses in IEC 62351 protected Smart Grid control systems. In: *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 266–270. IEEE (2016). ISBN: 978-1-5090-4075-9.
41. YOUSSEF, T.A., HARIRI, M.E., BUGAY, N., MOHAMMED, O.A.: IEC 61850: Technology Standards and Cyber-Security Threats. In: *2016 IEEE 16th International Conference on Environment and Electrical Engineering (EEEIC)*, 2016. ISBN: 978-1-5090-2320-2.
42. WRIGHT, J.G., WOLTHUSEN, S.D., Limitations of IEC62351-3's public key management. In: *2016 IEEE 24th International Conference on Network Protocols (ICNP)*, pp. 1–6, IEEE, 2016. ISBN: 978-1-5090-3281-5.
43. HAN, W., XIAO, Y., Non-Technical Loss Fraud in Advanced Metering Infrastructure in Smart Grid. In: International Conference on Cloud Computing and Security (ICCCS) 2016: Cloud Computing and Security, pp. 163–172. Springer, Cham, 2016. ISBN: 978-3-319-48674-1

44. RRUSHI, J.L., FARHANGI, H., NIKOLIC, R., HOWEY, C., CARMICHAEL, K., PALIZBAN, A., By-design vulnerabilities in the ANSI C12.22 protocol specification. In: *Proceedings of the 30th Annual ACM Symposium on Applied Computing – SAC '15*, pp. 2231–2236. ACM Press, New York, SUA, 2015.
45. MCKAY, B., Lessons to Learn for U.S. Electric Grid Critical Infrastructure Protection: Organizational Challenges for Utilities in Identification of Critical Assets and Adequate Security Measures. In: *2011 44th Hawaii International Conference on System Sciences*, pp. 1–9. IEEE, 2011. ISBN:978-1-4244-9618-1.
46. LEE, S., PARK, Y., LIM, H., SHON, T.: Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology. In: *2014 International Conference on IT Convergence and Security (ICITCS)*, pp. 1–4. IEEE, 2014. ISBN: 978-1-4799-6541-0
47. CHAN, A.C., JIANYING, ZHOU: On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628. In: *IEEE Communications Magazine 51(1)*, pp. 58–65, 2013. ISSN: 0163-6804.
48. LESZCZYNA R., „Cybersecurity in the Electricity Sector. Managing Critical Infrastructure", Editura Springer. Gdansk, Polonia: 2019, 213 p. ISBN: 978-3-030-19538-0
49. LANGER, L., SMITH, P., HUTLE, M. Smart grid cybersecurity risk assessment. In: 2015 *International Symposium on Smart Electric Distribution Systems and Technologies (EDST)*, pp. 475-482. IEEE (2015). ISBN: 978-1-4799-7736-9
50. GUPTA, B., B., AKHTAR, T. A survey on smart power grid: frameworks, tools, security issues, and solutions. In: *Annals of Telecommunications*, vol. 72, no. 9, pp. 517–549, 2017 [online]. Disponibil: https://doi.org/10.1007/s12243-017-0605-4;
51. GENGE, B., SIATERLIS, C., Analysis of the effects of distributed denial-of-service attacks on MPLS networks. In: *International Journal of Critical Infrastructure Protection 6(2)*, pp. 87–95, 2013. ISSN: 1874-5482
52. WEERATHUNGA, P.E., CIORACA, A., The importance of testing Smart Grid IEDs against security vulnerabilities. In: *2016 69th Annual Conference for Protective Relay Engineers (CPRE)*, pp. 1–21. IEEE (2016). ISSN: 2474-9753.
53. BRANDSETTER, T., KNORR, K., ROSENBAUM, U., A Manufacturer-Specific Security Assessment Methodology for Critical Infrastructure Components. In: *Fourth Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, ICCIP, 2010*, Washington, SUA, 15-17 martie 2010, pp. 229–244. Springer, Berlin, Heidelberg, 2010. ISBN: 978-3-642-16806-2

54. DONDOSSOLA, G., DECONNICK, G., GARONNE, F., BEITOLLAHI, H., Testbeds for Assessing Critical Scenarios in Power Control Systems. pp. 223–234. Springer, Berlin, Heidelberg (2009). ISBN: 978-3-642-03552-4
55. WERMANN, A.G., BORTOLOZZO, M.C., GERMANO DA SILVA, E., SCHAEFFER-FILHO, A., GASPARY, L.P., BARCELLOS, M., ASTORIA: A framework for attack simulation and evaluation in smart grids. In: *NOMS 2016 – 2016 IEEE/IFIP Network Operations and Management Symposium*, pp. 273–280. IEEE, 2016. ISBN: 978-1-5090-0223-8
56. ALCARAZ C., ZEADALLY S., Critical Infrastructure Protection: Requirements and Challenges for the 21st Century. In: *International Journal of Critical Infrastructure Protection (IJCIP)*, vol. 8, Elsevier Science, pp. 53-66, Publicat: 2015-01 [online]. [citat 16.10.2021] Disponibil: https://www.researchgate.net/publication/272391570_Critical_infrastructure_protection_Requirements_and_challenges_for_the_21st_century
57. LESZCZYNA, R., FOVINO, I. N., MASERA, M.: Approach to security assessment of critical infrastructures' information systems. In: *IET Information Security 5(3)*, pp. 135-144, septembrie 2011. ISSN: 1751-8709.
58. FOVINO, I. N., MASERA, M.: InSAW-Industrial Security Assessment Workbench. In: *2008 First International Conference on Infrastructure Systems and Services: Building Networks for a Brighter Future (INFRA)*, pp. 1–5, IEEE, 2008. ISBN: 978-1-4244-6887-4
59. VARUTTAMASENI, A., BARI, R. A., YOUNGBLOOD, R.: Construction of a Cyber Attack Model for Nuclear Power Plants, In: *2017 ANS Annual Conference*, 10 p., San Francisco, SUA, Publicat: 2017-06 [online]. [citat 02.11.2021] Disponibil: https://www.bnl.gov/isd/documents/94595.pdf.
60. AHN, W., CHUNG, M., MIN, B. G., SEO, J.: Development of Cyber-Attack Scenarios for Nuclear Power Plants Using Scenario Graphs. In: *International Journal of Distributed Sensor Networks*, 12 p., Korea, Publicat: 2015-09 [online]. [citat 02.11.2021] Disponibil: https://journals.sagepub.com/doi/pdf/10.1155/2015/836258.
61. BEEK, C., DUNTON, T., GROBMAN, S., KARLTON, M., MINIHANE, N., PALM, C., PETERSON, E., SAMARI, R., SCHMUGAR, C., SIMS, R., SOMMER, D., SUN, B.: McAfee Labs Threats Report: June 2018. Tech. rep., McAfee (2018).
62. LESZCZYNA, R., NAI FOVINO, I., MASERA, M.: Simulating malware with MAlSim. In: *Journal in Computer Virology. 6*. pp. 65-75, 2008 [online]. [citat 05.11.2021] Disponibil: https://www.researchgate.net/publication/226129222_Simulating_malware_with_MAlSim.
63. Leszczyna, R.: Evaluation of Agent Platforms. Tech. rep., European Commission, Joint Research Centre, Institute for the Protection and security of the Citizen, Ispra, Italy (2004).