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

Admis la susținere:
Șef departament:
Fiodorov Ion, conf. univ., dr.
"___" _____20__

PROTECȚIA COMPONENTELOR TIC DIN CADRUL INFRASTRUCTURILOR CRITICE NAȚIONALE

Teză de master

Student:_____MOGHILDA Sergiu
Conducător :_____PUTERE Alexandru
lect. univ

Chișinău – 2022

ADNOTARE

la teza de master cu tema **„Protecția componentelor TIC din cadrul infrastructurilor critice naționale", elaborată de Moghilda Sergiu, Chișinău, 2022.**

Lucrarea de față are drept scop analiza infrastructurii critice naționale a Republicii Moldova în raport cu cadrul de reglementare și practicile internaționale în domeniul identificării, desemnării și protecției infrastructurilor critice precum și crearea unui model de organizare și protecție a componentelor TIC din cadrul infrastructurilor critice naționale.

Această lucrare poate servi drept ghid pentru implementarea și managementul securității componentelor TIC din cadrul IC. În teză sunt prezentate şi analizate date teoretice privind importanţa, metodele și bunele practici ale altor țări de implementare a securității informaţionale şi cibernetice în mediul infrastructurilor critice de diferite nivele şi apartenenţe.

De asemenea, este caracterizată evoluţia riscurilor, enumerate vulnerabilitățile şi ameninţările pentru IC.

Se impune alinierea cadrului normativ național privind protecția infrastructurilor critice la practicile internaționale din domeniu. Studiile au demonstrat un vid legislativ precum și necesitatea implementării unor astfel de modele de protecție și management al securității infrastructurilor critice la nivel naţional.

Teza de master cuprinde introducere, trei capitole, concluzii, bibliografie și referințe. Volumul lucrării este de 65 de pagini text de bază, 5 tabele şi 6 figuri.

În teză au fost utilizate cuvinte-cheie: infrastructuri critice; infrastructuri informaționale critice; atacuri cibernetice; cadre de reglementare; securitate cibernetică; securitatea informațiilor;

ANNOTATION

to the master's thesis on "Protection of ICT components in national critical infrastructures", developed by Moghilda Sergiu, Chisinau, 2022.

This paper aims to analyze the national critical infrastructures of the Republic of Moldova in relation to the international regulatory framework and practices in the field of identification, designation and protection of critical infrastructures and to create a model of organization and protection of ICT components used within national critical infrastructures.

This paper can serve as a guide for the implementation and security management of ICT components within the IC. The thesis presents and analyzes theoretical data relying the importance and methods of implementing information and cyber security in the environment of critical infrastructures of different levels and affiliations.

The evolution of risks, vulnerabilities and threats to CI are also characterized.

It is necessary to align the national regulatory framework on critical infrastructure protection with international practices in the field. Studies have shown the need to implement such models for the protection and management of critical infrastructure security at the national level.

The master's thesis includes an introduction, three chapters, conclusions, bibliography and references. The volume of the paper is 65 pages of basic text, 5 tables and 6 figures.

Keywords were used in the thesis, such as: critical infrastructures; critical information infrastructure; cyber attacks; regulatory frameworks; cyber security; information security;

CUPRINS

INTODUCERE

Actualitatea temei cercetate. Infrastructurile critice constituie o parte indispensabilă a vieții moderne. Acestea sunt considerate drept indicator al bunăstării sociale și al dezvoltării economice. Protecția infrastructurilor critice care susțin toate aspectele vieții reprezintă un imperativ în ceea ce privește asigurarea ordinii și securității publice. În acest context, prin această lucrare îmi propun să studiez evoluțiile din lume în ceea ce privește definirea și protecția infrastructurilor informaționale critice. Studiul a fost realizat pe o bază teoretică prin efectuarea unei revizuiri a literaturii. În studiu, în primul rând, sunt examinate conceptele de infrastructură critică (CI) și infrastructură critică informațională (ICI), iar apoi sunt explicate domeniul de aplicare al infrastructurilor critice, cadrele de reglementare ale SUA și UE privind protecția ICI. De asemenea, sunt examinate atacurile cibernetice de rezonanță în adresa ICI. În final, sunt făcute recomandări pentru definirea și protecția ICI a Republicii Moldova.

Alegerea temei acestei cercetări se justifică cel puțin prin două motive. În primul rând, tehnologia informației și comunicațiile (TIC), în special Internetul, s-au dezvoltat rapid în ultimele decenii și s-au răspândit în întreaga lume. Odată cu această dezvoltare și rapida răspândire, metodele clasice de lucru, de gândire, chiar de a produce, de a face afaceri au început să se schimbe, iar viața treptat s-a plasat într-un mediu din ce în ce mai digital, mobil și online.

Aceste evoluții oferă multe beneficii, în special economisirea forței de muncă, a resurselor și a timpului. Cu toate acestea, domeniile TIC oferă, de asemenea, oportunități persoanelor cu intenții rele, cum ar fi accesul neautorizat la sistemele informaționale, deteriorarea sistemelor, accesul la informații personale, furtul, modificarea și ștergerea acestor informații prin utilizarea instrumentelor bazate pe TIC, cum ar fi viruși, viermi, troieni, spam, atacuri de tip distribuited denial-of-service (DDoS), computere zombie și rețele botnet. Aceste provocări scot în evidență al doilea motiv și în special introduc noțiunea de securitate cibernetică, care în cele din urmă rămâne a fi una dintre problemele importante ale comunității globale.

Pe lângă dependența tot mai mare a statelor de sistemele informaționale, introducerea lor în întreaga sferă a vieții umane contribuie la dezvoltarea infracțiunilor informatice și a atacurilor informatice asupra infrastructurilor informaționale critice. În plus, acest lucru duce la apariția de noi conflicte la nivel internațional, inclusiv apariția unor astfel de amenințări precum atacurile cibernetice internaționale, războiul informațional etc.

Apariția amenințărilor cibernetice a devenit principalul motiv pentru care practic toate statele moderne de stat au început să perceapă securitatea informațiilor drept element al securității naționale. O atenție deosebită este acordată asigurării securității cibernetice a infrastructurilor critice care prezintă o

importanță deosebită pentru economia și securitatea statului (industria nucleară, instalații militaro-industriale, sectorul bancar etc.).

Gradul de studiere a temei. Analiza teoretico-științifică efectuată în baza studierii literaturii de specialitate pentru subiectul abordat atestă că problema asigurării securității cibernetice și/sau informaționale a componentelor TIC din cadrul infrastructurilor critice este foarte relevantă la nivel global, național, departamental, întrucît efectele atacurilor cibernetice reușite pot cauza prejudicii considerabile financiare, fizice, umane sau de altă natură. De asemenea, penetrarea sistemelor informatice aferente infrastructurii critice ale Republicii Moldova poate oferi control neautorizat asupra acestor sisteme, și în consecință, afectarea proceselor economice, sociale, politice, informaționale, militare etc.

Scopul şi sarcinile tezei. Scopul lucrării constă în scrutarea celor mai bune practici pentru protecția infrastructurilor critice informaționale, întru identificarea elementelor slabe exploatate în atacuri cibernetice asupra ICI și a oferi recomandări și concluzii cu referire la implementarea unor mecanisme de protecție a ICI.

Baza ştiinţifica-metodologică. Metodologia folosită a presupus, în primul rând, evaluarea conceptului de infrastructură critică și analiza principalelor amenințări şi vulnerabilități. În cadrul studiului au fost aplicate şi îmbinat ansamblul de metode teoretice, care au făcut posibilă cercetarea mecanismelor de protecție și implementare a arhitecturilor de rețea întru realizarea schimbului instant de date dintre componentele esențiale ale IC.

Metoda analizei de conținut și cea comparativă a cadrului normativ în domeniu au servit la cercetarea practicilor internaționale și evidenţierea trăsăturilor distincte ale acestora cu cadrul de reglementare a protecției infrastructurilor critice existent în Republicii Moldova

Sinteza a fost utilizată pentru a scoate în prim-plan din multitudinea de abordări teoretice și practice - conceptele, procedurile, cerințele și politicile cele mai eficiente la etapa actuală.

Elemente de inovaţie ştiinţifică constau în abordarea protecției infrastructurilor critice prin prisma principalelor ameninţări, vulnerabilităţi şi cadrului normativ de proiectare, implementare și utilizare a componentelor TIC, acestea ar putea servi drept o foaie de parcurs pentru actualizarea cadrului de reglementare național.

Teza constă din introducere, adnotare, trei capitole, concluzii (în total 71 pagini).

Primul capitol include conceptul de infrastructură critică, evoluția definițiilor infrastructurilor critice, diferența între infrastructuriă critică și infrastructură critică informațională și domeniile de aplicare

a IC, măsuri organizatorice și operaționale și, nu în ultimul rînd, cerințe de protecție a infrastructurilor critice informaționale.

Capitolul doi conține abordarea cadrului de reglementare (internaționale și naționale) în domeniul protecției infrastructurilor critice, starea actuală a lucrurilor cu referire la IC.

Cu referire la capitolul trei, acesta prevede provocările și cerințele de protecție a infrastructurilor critice informaționale, noțiunea de reziliență a sistemelor, soluții și recomandări de aliniere a proceselor la standardele organizaționale și operaționale pentru sistemele critice de control.

BIBLIOGRAFIE

Manuale, monografii, cărţi, broşuri şi articole

[1] European Commission, *Critical Infrastructure Protection in the fight against terrorism*, 2004.

[2] Serviciul Român de Informaţii, Protecţia infrastructurii critice. https://www.sri.ro/upload/BrosuraProtectiaInfrastructurilorCritice.pdf

[3] European Commission (2005) COM 576 final, Green paper on a European Programme for critical infrastructure protection, Brussels, 17.11.2005. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52005DC0576&from=EN.

[4]https://publications.jrc.ec.europa.eu/repository/handle/JRC70046

[5]https://www.researchgate.net/publication/312040936_PROTECTIA_INFRASTRUCTURILOR_CRITICE_MODELAREA_BAZATA_PE_OBIECT_rezumat_teza_de_doctorat_Critical_Infrastructures_Protection_-_Object-Oriented_Modelling_-_Executive_summary_PhD_Thes

[6] .https://cssas.unap.ro/ro/pdf_studii/infrastructuri_critice.pdf

[7] https://www.ipn.md/ro/protectia-infrastructurii-critice-o-noua-prioritate-a-republicii-moldova-7978_1082768.html

[8] https://radiochisinau.md/protectia-infrastructurii-critice-o-noua-prioritate-a-r-moldova-comentariu-de-valeriu-turcanu-si-iulian-rusu

[9] http://ipre.md/2021/07/02/protectia-infrastructurii-critice-o-noua-prioritate-a-republicii-moldova-comentariu-de-valeriu-turcanu-si-iulian-rusu-ipn-md/

[10] https://multimedia.parlament.md/parlamentul-a-votat-crearea-comisiei-pentru-infrastructura-esentiala-in-componenta-guvernului/

[11] https://www.legis.md/cautare/rezultate/23321

[12] TEAM, S. A.: sKyWIper (a.k.a. Flame a.k.a. Flamer): A complex malware for targeted attacks. Budapest, Hungary: Laboratory of Cryp tography and System Security (CrySyS Lab), 2012.

[13] HAGEROTT, M.: Stuxnet and the vital role of critical infrastructure operators and engineers. International Journal of Critical Infrastructure Protection, vol. 7(4), 2014, pp. 244-246

[14] MACKENZIE, H.: How Dragonfly Hackers and RAT Malware Threaten ICS Security. Belden, Indianapolis, Indiana: Industrial Security Blog, 2014.

[15] FRANCIS, R.; BEKERA, B.: A metric and frameworks for resilience analysis of engineered and infrastructure systems. Reliability Engineering and System Safety 121, 2014, pp. 90-103.

[16] ZOBEL, C. W.: Representing perceived tradeoffs in defining disaster resilience. Decision Support Systems, 2011, pp. 394-403

[17] FISHER, R.; BASSETT, G.; BUEHRING, W.; COLLINS, M.; DICKINSON, D.E. ş.a.:Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program. Chicago: Argonne National Laboratory, Decision and Information Sciences Division, 2010.

[18] DHS, Public Law 107-296, Homeland Securty ACT of 2002, http://www.dhs.gov

[19] C. Alcaraz and S. Zeadally, Critical Control System Protection in the 21st Century, IEEE Computer, vol. 46(4), pp. 74-83, 2013.

[20] C. Alcaraz, G. Fernandez and F. Carvajal, Security aspects of SCADA and DCS environments, Advances in Critical Infrastructure Protection: Information Infrastructure Models, Analysis, Defense, Springer, 120149, 2011.

[21] R. McClanahan, SCADA and IP: Is network convergence really here?, IEEE Industry Applications Magazine, vol. 9, pp. 29-36, 2009.

[22] NIST, NIST framework and roadmap for Smart Grid interoperability standards, release 2.0., NIST Special Publication 1108R2, 2012.

[23] C. Alcaraz and. J. Lopez, Analysis of requirements for critical control systems, International Journal of Critical Infrastructure Protection, Elsevier, vol. 2, pp. 137-145, 2012.

[24] E. Knapp, Network security, Securing Critical Infrastructure Networks for Smart Grid, SCADA, Other Industrial Control Systems, Syngress Book, Elsevier, 2011.

[25] CloudCERT, Testbed framework to exercise critical infrastructure protection, 2012, http://cloudcert.european-project.eu.

[26] B. Rimal and I. Lumb, A taxonomy and survey of cloud computing systems, Fifth International Joint Conference on INC, IMS and IDC, pp. 4451, 2009.

[27] P. Parikh, S. Kanabar and S. Sidhu, Opportunities and challenges of wireless communication technologies for Smart Grid applications, IEEE Conference on Power and Energy Society General Meeting, pp. 1-7, 2010.

[28] MiWi, Microchip MiWi P2P wireless protocol, http://www.microchip.com.

[29] IEEE, IEEE standard for information technology telecommunications and information exchange between systems-local and metropolitan area networks, IEEE 802.15.4d-2009, http://standards.ieee.org.

[30] HART, HART Communication Foundation, http://wirelesshart.hartcomm.org/.

[31] R. Roman, P. Najera and J. Lopez, Securing the Internet of Things, IEEE Computer, vol. 44, pp. 51-58, 2011.

[32] C. Alcaraz and J. Lopez, A security analysis for wireless sensor mesh networks in highly critical systems, IEEE Transactions on Systems, Man, Cybernetics, Part C: Applications and Reviews, vol. 40, pp. 419-428, 2010.

[33] ARPA, President Obama Announces $3.4 Billion Investment to Spur Transition to Smart Energy Grid, The White House, Office of the Press Secretary, 2009.

[34] S. Rinaldi, Modeling and simulating critical infrastructures and their interdependencies, 37th Annual Conference on Hawaii International System Sciences, 2004.
[35] IEEE, A compilation of IEEE standard computer glossaries, IEEE Standard Computer Dictionary, 1991.
[36] Z. Zheng and J. Lopez, An adaptive QoS aware fault tolerance strategy for web services, Empirical Software Engineering Journal, vol. 15, pp. 323-345, 2010.
[37] C. Alcaraz, C. Fernandez-Gago, and J. Lopez, An early warning system based on reputation for energy control systems, IEEE Transactions on Smart Grid, vol. 2, pp. 827-834, 2011.
[38] DHS, Catalog of control systems security: Recommendations for standards developers, http://www.us-cert.gov.
[39] NIST, Information security, NIST Special Publication 800-53, Revision 3, 2009.
[40] NIST, Guidelines for Smart Grid cyber security: Vol. 1, Smart Grid cyber security strategy, architecture, high-level requirements, NISTIR 7628, The Smart Grid Interoperability Panel Cyber Security Working Group, 2010.
[41] IEC62351, Power systems management and associated information exchange data and communications security, Part1-8, http://www.iec.ch/, retrieved on October 2014.
[42] ISA, Security for industrial automation and control systems, Security technologies for industrial automation and control systems, ISA-TR62443-3-1 (99.03.01), http://isa99.isa.org.
[43] ISO 27002:2005, Codul de practică al managementului securității informațiilor;
[44] ISO 27001:2005, Sistemul de management al securității informațiilor – Cerințe;
[45] ISO, Information technology-security techniques-security assessment of operational systems, /IEC TR 19791:2006, draft revision ISO/IEC JTC 1/SC 27 Final text for ISO/IEC TR, ITTF.
[46] ISO, Tecnolog´ıa de la informaci´on t´ecnicas de seguridad c´odigo para la pr´actica de la gesti´on de la seguridad de la informaci´on, 2005, ISO/IEC 17779.
[47] IEEE, P1402 Standard for physical security of electric power substations, IEEE 1402, 2000.
[48] API-1164: Pipeline SCADA Security, American Petroleum Institute, API, 2004.
[49] NISCC, NISCC good practice guide on firewall deployment for SCADA and process control networks, Technical report, British Columbia Institute of Technology (BCIT), National Infrastructure Security Coordination Centre, 2005.
[50] H. Psaier and S. Dustdar, A survey on self-healing systems: Approaches and systems, Computing, SpringerWien, vol. 91, pp. 43-73, 2011.
[51] T. Rigole and G. Deconinck, A survey on modelling and simulation of interdependent critical infrastructures, 3er IEEE Beneluz Your Researchers Symposium in Electrical Power Engineering, 2006.

[52] G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis and R. Cepeda, Privacy for smart Meters: Towards undetectable appliance load signatures, First IEEE International Conference on Smart Grid Communications (SmartGridComm)., pp. 232-237, 2010.
[53] SELFMAN, Self management for large-scale distributed systems based on structured overlay networks and components, EU FP6 Information Society Technologies, EU FP6 Information Society Technologies, http://www.ist-selfman.org.
[54] A. Josang, R. Ismail and C. Boyd, A survey of trust and reputation systems for online service provision, Decision Support Systems, vol. 43, pp. 618644, 2007.
[55] B. Zhu, A. Joseph and S. Sastry, A taxonomy of cyber attacks on SCADA systems, 4th International Conference on Cyber, Physical and Social Computing, 2011.
[56] S, Pai, Transactional confidentiality in sensor networks, IEEE Security& Privacy, vol. 6, pp. 28-35, 2008.