MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică şi Telecomunicaţii
Departamentul Telecomunicaţii și Sisteme Electronice

Admis la susţinere
Şefă departament:
Valentina Tîrșu, dr.conf.univ.

20 ianuarie 2025

Utilizarea listelor de control al accesului în scopul impunerii politicilor de securitate în cadrul reţelelor informaţionale

Teză de master

Student: **Caraulan Nicu, grupa SISRC-231M**

Conducător: **Dinu ȚURCANU,**
dr. în șt. inginerești
conferențiar universitar

Chișinău, 2025

REZUMAT

La teza de master

Tema „Utilizarea listelor de control al accesului în scopul impunerii politicilor de securitate în cadrul rețelelor informaționale”

Actualitatea și importanța temei. În contextul evoluției tehnologice și al creșterii constante a volumului de informații gestionate în mediul digital, securitatea rețelelor informaționale a devenit o prioritate majoră pentru organizațiile din întreaga lume. Tema „Utilizarea listelor de control al accesului” în scopul impunerii politicilor de securitate în cadrul rețelelor informaționale” este extrem de actuală și relevantă, având în vedere că amenințările cibernetice sunt tot mai sofisticate și că protejarea resurselor informatice devine un obiectiv central în cadrul oricărei strategii de securitate IT. În ultima perioadă, atacurile informatice au evoluat atât în complexitate, cât și în frecvență. Hackerii folosesc metode din ce în ce mai avansate pentru a exploata vulnerabilitățile rețelelor și pentru a accesa date sensibile sau pentru a provoca daune organizațiilor. Breșele de securitate pot duce la pierderi semnificative, nu doar financiare, ci și reputaționale, iar în anumite cazuri, pot afecta chiar continuitatea activității unei organizații. În acest context, ACL devin un instrument esențial pentru protejarea datelor, prin limitarea accesului la informații doar pentru persoanele autorizate, de aceea considerăm tema data actuală și important pentru a fi cercetată.

Scopul și obiectivele tezei - este de a cerceta aspectele teoretice și practice privind utilizarea listelor de control al accesului în implementarea și aplicarea politicilor de securitate în cadrul rețelelor informaționale, având în vedere provocările actuale ale securității cibernetice. Această lucrare își propune să explice modul în care ACL pot fi utilizate pentru a asigura un control eficient al accesului la resursele rețelelor informatice, protejând astfel datele sensibile și prevenind accesul neautorizat, într-un context de amenințări cibernetice tot mai sofisticate.

Valoarea teoretică a tezei. Cercetarea efectuată contribuie la îmbunătățirea doctrinei privind utilizarea listelor de control al accesului.

Valoarea aplicativă a tezei rezidă în recomandările elaborate care pot fi implimentate cu success în practică privind utilizarea listelor de control al accesului în scopul impunerii politicilor de Securitate în cadrul rețelelor informaționale.

SUMMARY

In the master's thesis

Topic " The use of access control lists for enforcing security policies within information networks"

Timeliness and importance of the topic. In the context of technological evolution and the constant increase in the volume of information managed in the digital environment, the security of information networks has become a major priority for organizations around the world. The topic "Using access control lists" to enforce security policies in information networks" is extremely current and relevant, considering that cyber threats are becoming more sophisticated and that protecting information resources is becoming a central objective in any IT security strategy. Recently, computer attacks have evolved both in complexity and frequency. Hackers are using increasingly advanced methods to exploit network vulnerabilities and access sensitive data or cause damage to organizations. Security breaches can lead to significant losses, not only financial, but also reputational, and in some cases, can even affect the continuity of an organization's business. In this context, ACLs become an essential tool for data protection, by limiting access to information only to authorized persons, that is why we consider the topic current and important to be researched.

The purpose and objectives of the thesis - is to research the theoretical and practical aspects regarding the use of access control lists in the implementation and enforcement of security policies within information networks, considering the current challenges of cyber security. This paper aims to explain how ACLs can be used to ensure effective access control to computer network resources, thus protecting sensitive data and preventing unauthorized access, in a context of increasingly sophisticated cyber threats.

The theoretical value of the thesis. The research conducted contributes to the improvement of the doctrine regarding the use of access control lists.

The applicative value of the thesis resides in the elaborated recommendations that can be successfully implemented in practice regarding the use of access control lists for the purpose of imposing Security policies within information networks.

CUPRINS

INTRODUCERE

Actualitatea și importanța temei. În cadrul prezentei teze ne-am propus să abordăm o temă de actualitate – contabilitatea operațiunilor de plată în bănci și perfecționarea acesteia. Odată cu digitalizarea masivă a datelor și cu expansiunea rapidă a tehnologiilor precum cloud computing, Internet of Things (IoT) și rețelele software-defined, organizațiile se confruntă cu o creștere considerabilă a complexității infrastructurilor IT. În acest peisaj digital în continuă schimbare, atacurile cibernetice devin din ce în ce mai sofisticate și mai greu de detectat. Breșele de securitate, accesul neautorizat la informații sensibile, dar și atacurile de tip ransomware, reprezintă riscuri grave care pot afecta activitatea organizațiilor, reputația acestora și integritatea datelor. În acest context, listelor de control al accesului (ACL) devin un instrument esențial pentru asigurarea unei protecții eficiente a rețelelor informatice. ACL permit implementarea unor politici precise de control al accesului, restricționând accesul doar la utilizatorii autorizați și protejând astfel resursele critice ale organizației. ACL sunt folosite pentru a gestiona accesul la date, aplicații și sisteme, prevenind astfel vulnerabilitățile ce pot apărea dintr-un management ineficient al accesului. Astăzi, organizațiile dispun de rețele complexe, care pot include atât infrastructuri fizice, cât și soluții cloud sau resurse distribuite. Tehnologiile emergente, cum ar fi rețelele software-defined și virtualizarea, permit o flexibilitate mai mare, dar impun și o complexitate mai mare în gestionarea accesului. ACL sunt esențiale pentru a aplica politici de securitate într-un mod dinamic, în timp real, adaptat la schimbările infrastructurii IT. De exemplu, ACL pot fi folosite pentru a reglementa accesul în timp real la resursele cloud, pentru a limita accesul pe bază de locație geografică sau de tip de dispozitiv, protejând astfel organizațiile de riscurile asociate cu accesul din surse externe sau necontrolate. Tema „Utilizarea Listelor de Control al Accesului în scopul impunerii politicilor de securitate în cadrul rețelelor informaționale” este deosebit de actuală și importantă în contextul creșterii complexității rețelelor informatice, al evoluției atacurilor cibernetice și al reglementărilor din domeniul protecției datelor. ACL reprezintă un instrument cheie pentru asigurarea unui control eficient al accesului, protejând astfel infrastructurile IT și contribuind la implementarea celor mai bune practici de securitate. Într-un peisaj digital în continuă schimbare, utilizarea ACL ajută organizațiile să se protejeze de riscuri, să asigure conformitatea cu reglementările și să apere integritatea și confidențialitatea datelor sensibile.

Scopul și obiectivele tezei - este de a analiza și de a demonstra importanța listelor de control al accesului ca instrument esențial pentru implementarea politicilor de securitate într-un mediu de rețea informatizată, protejând astfel resursele organizației și prevenind accesul neautorizat. Teza își propune să explice cum ACL contribuie la securizarea infrastructurii IT, la reducerea riscurilor de securitate și la protejarea datelor sensibile, oferind soluții pentru un control precis și eficient al accesului la resursele rețelei.

Obiectivele tezei:

1. Prezentarea noțiunilor privind securitatea informațiilor;
2. Prezentarea conceptului și managementul politicilor de securitate în cadrul rețelelor informaționale;
3. Prezentarea aspectelor teoretice privind utilizarea listelor de control al accesului în scopul impunerii politicilor de securitate în cadrul rețelelor informaționale;
4. Desfășurarea unui studiu practic, utilizarea listelor de control al accesului în scopul impunerii politicilor de securitate în cadrul rețelelor informaționale;
5. Prezentarea concluziilor și elaborarea recomandărilor.

Baza ştiinţifico-metodologică a cercetării – a constituit doctrina, publicațiile, monografiile ce prezintă informații teoretice relevante privind utilizarea listelor de control al accesului, în scopul impunerii politiclor de securitate în cadrul rețelelor informaționale, tema fiind cercetată de autorii: Cărăuş Iurie, Cerbu Olga, Rusnac A., Burtescu, E., Udroiu M., Popa C. etc.

Metodologia cercetării - cercetarea ştiinţifică, studiul monografiilor, revistelor de specialitate, realizarea vastelor cercetări privind domeniul vizat. În ceea ce priveşte metodologia, în procesul elaborării lucrării, am selectat materialul doctrinar, folosindu-mă de metodele consacrate ale cercetării ştiinţifice:

- metoda logică a fost folosită în vederea sintezei punctelor de vedere ale autorilor menţionaţi cu privire la tema investigată, precum şi în expunerea concluziilor proprii;
- metoda informatică privind aplicabilitatea în practică a listelor de control al accesului în scopul impunerii politicilor de securitate în cadrul rețelelor informaționale.

Sumarul compartimentelor tezei. Scopul şi sarcinile cercetării au prefigurat structura lucrării, care constă din introducere, trei capitole, concluzii şi lista surselor bibliografice.

În primul capitol **„ASPECTE TEORETICE PRIVIND UTILIZAREA LISTELOR DE CONTROL AL ACCESULUI ÎN SCOPUL IMPUNERII POLITICILOR DE SECURITATE ÎN CADRUL REȚELELOR INFORMAȚIONALE”**, sunt analizate noțiunile privind securitatea informațiilor, este cercetat conceptul și managementul politicilor de securitate în cadrul rețelelor informaționale și controlul accesului.

Capitolul II **„UTILIZAREA LISTELOR DE CONTROL AL ACCESULUI ÎN SCOPUL IMPUNERII POLITICILOR DE SECURITATE ÎN CADRUL REȚELELOR INFORMAȚIONALE”**, sunt prezentate tipurile de control al accesului, sunt analizate aspectele privind autentificarea, autorizarea și auditarea, managementul parolelor etc.

Capitolul III **„ STUDIU PRACTIC - UTILIZAREA LISTELOR DE CONTROL AL ACCESULUI ÎN SCOPUL IMPUNERII POLITICILOR DE SECURITATE ÎN CADRUL REȚELELOR INFORMAȚIONALE”**, prezintă formele combinate de control al accesului privind securitatea în cadrul rețelelor informaționale, sunt analizate politicile de securitate în cadrul rețelelor informaționale în cadrul entității analizate și sunt prezentate direcțiile de optimizare în utilizarea listelor de control al accesului în scopul impunerii politicilor de securitate în cadrul rețelelor informaționale în cadrul entității supuse studiului.

În **concluzii și recomandări,** sunt elaborate concluziile și recomandările prezentate asupra temei cercetate, sun elaborate recomandări care pot fi aplicate cu succes în practică și care ar contribui la securitatea rețelelor informaționale.

BIBLIOGRAFIE

Acte normative

1.Legea privind securitatea cibernetică nr. 48 din 16.03.2023. În: Monitorul Oficial nr. 151-153 din 28.04.2023

2. Strategia securității informaționale a Republicii Moldova pentru anii 2019–2024. În: Monitorul Oficial nr. 13-21 art. 80 din 18.01.2019

3. Hotărârea Guvernului Republicii Moldova cu privire la aprobarea Concepţiei Sistemului informaţional geografic cu destinaţie specială al Serviciului de Informaţii şi Securitate nr. 972 din 01.09.2004. În: Monitorul Oficial al Republicii Moldova nr. 171 din 17.09.2004.

4. Legea privind aprobarea Concepţiei securităţii informaţionale Republicii Moldova nr. 299 din 21.12.2017. Monitorul Oficial al Republicii Moldova nr. 48-57 din 16.02.2018.

Cărți, monografii, Articole Științifice

5. PECA, L., ȚURCANU, D. Network security: Practical examples solved to be introduced in network security. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chişinău: Tehnica-UTM, 2023. – 243 p. ISBN 978-9975-45-941-9. http://repository.utm.md/

6. PECA, L., ȚURCANU, D. Computer networks: Practical examples solved to be introduced in computer networks. Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department Software Engineering and Automatics. – Chişinău: Tehnica-UTM, 2022. – 188 p. ISBN 978-9975-45-812-2. http://repository.utm.md/

7. ȚURCANU, D., SPINU, N., POPOVICI, S., ȚURCANU, T. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. In: Journal of Social Sciences. 2021, IV (1), pp. 74–83. https://doi.org/10.52326/jss.

8. ȚURCANU, D., POPOVICI, S., ȚURCANU, T. Digital signature: advantages, challenges and strategies. In: Journal of Social Sciences. 2020, III (4), pp. 62–72. https://doi.org/10.5281/

9. CĂCIULESCU, A.R., RUGHINIȘ, R., ȚURCANU, D., RADOVICI, A. Mapping Cyber-Financial Risk Profiles: Implications for European Cybersecurity and Financial Literacy. In: Risks. 2024, 12(12), 200. https://doi.org/10.3390/

10. VULPE, S.-N., RUGHINIȘ, R., ȚURCANU, D., ROSNER, D. AI and cybersecurity: a risk society perspective. In: Frontiers in Computer Science. Volume 6-2024. https://doi.org/10.3389/fcomp.

11. BRAN, E., RUGHINIȘ, R., ȚURCANU, D., RADOVICI, A. AI Leads, Cybersecurity Follows: Unveiling Research Priorities in SDG-Relevant Technologies Across Nations. In: Sustainability. 2024, 16(20), 8886. https://doi.org/10.3390/

12. BRAN, E., RUGHINIȘ, R., ȚURCANU, D., NADOLEANU, G. Technical Innovations and Social Implications: Mapping Global Research Focus in AI, Blockchain, Cybersecurity, and Privacy. In: Computers. 2024, 13(10), 254. https://doi.org/10.3390/

13. BRAN, E., RUGHINIȘ, R., ȚURCANU, D., STĂICULESCU, A. Decoding National Innovation Capacities: A Comparative Analysis of Publication Patterns in Cybersecurity, Privacy, and Blockchain. In: Applied Sciences. 2024, 2024, 14(16), 7086. https://doi.org/10.3390/

14. GRIGORESCU, O., BOTEZATU, L., MUTU, A., ȚURCANU, D. Contextual Remediations Prioritization System Designed to Implement Theoretical Principles of CVSS V4. In: University Politehnica of Bucharest scientific bulletin series C-Electrical Engineering and Computer Science. 2024, Volume 86, Issue 3, Page 121-138. https://www.scientificbulletin.upb.ro/rev_docs_arhiva/rez833_656075.pdf

15. BĂLUȚĂ, A., SOARE, R. M., RUGHINIȘ, R., ȚURCANU, D. GeckoNet - Self-Healing SDN Framework. In: 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet). 19-20 September, 2024, Bucharest, Romania. https://doi.org/10.1109/

19. TÎRȘU V., SAVA L. *Integrating elasticsearch and kibana in ict management processes for economic efficiency in multimedia content administration***.** In: The scientific heritage. Economic Sciences., Vol.1 № 142 (142), 2024, p.15-20 . Budapest, Hungary. ISSN 9215 — 0365, Cosmos Impact Factor - 3.336 SJIF Impact Factor - 5.78 DOI: , Categoria B+. Disponibil: http://www.scientific-heritage.com/ru/arhiv/

20. SAVA L., TÎRȘU V., PLĂMĂDEALĂ C. *Performance evaluation of microtik routers according to electromagnetic compatibility testing standards.* În: Electrotehnica, Electronica, Automatica, vol.72/4, p.57-61. Romania, Sibiu: ISSN: 2392-828X, categoria B+. Disponibil: https://eea-journal.ro/articles-and-issues/current-issues/

22. TÎRȘU, V. Programare : Ghid metodic pentru lucrări de laborator. Chișinău: Ed. “Tehnica-UTM”, 2022, pag.130, ISBN 978-9975-45-861-0. Disponibil: https://library.utm.md/items/?biblionumber=2619626

23. Anderson R. – Security Engineering : A Guide to Building Dependable Distributed Systems, NY 2001

24. Hallberg Bruce. Reţele de calculatoare. Ghidul începătorului. Editura „Rosetti Educaţional," Bucureşti, 2006.

25. Burtescu, E., Securitatea bazelor de date distribute, Catedra de Informatică Economică, ASE,

referat doctorat, 2002.

26. Bragaru T., Briceag V., Malcocui V., Galaicu V. Securitatea informaţiei vis a –vis de securitatea informațională. USM

27. Bellamy BJ. Vulnerability Identification and Remediation Through Best Security Practices, SANS Institute, 2002

28. Buraga Corneliu. Reţele de calculatoare – introducere în securitate. Universitatea „Al. I. Cuza," Iasi, 2007.

29. C. Alberts and A. Dorofee, Managing Information Security Risks: The OCTAVE Approach, New York: Addison Wesley, 2003

30. Cărăuş Iurie, Cerbu Olga. Securitatea tranzacţiilor electronice. USM, Chişinău, 2009.

31. D. Oprea, Protecția și securitatea informațiilor. Ed. II, București: Ed. Polirom, 2007

32. D. Zaharie, Proiectarea obiectuală a sistemelor informaticeEditura DualTech, 2003.

33. Diver S., Information Security Policy. A Development Guide for Large and Small Companies, SANS Institute, 2007.

34. Flowerday S., Information security policy development and implementation, Journal Computers and Security archive, vol. 61, Issue C, August 2016

35. Grime R. Implementing Vulnerability Scanning in a Large Organisation, SANS Institute, June 2003.

36. Habracken Joe. Reţele de calculatoare pentru începători. Editura „All," Bucureşti, 2022.

37. Held Gil, Hundley Kent. Arhitecturi de securitate. Editura „Teora," Bucureşti, 2003.

38. Ioan-Cosmin Mihai. Securitatea informaţiilor. Editura „Sitech," Galaţi, 2022.

39. Ioan-Cosmin Mihai. Securitatea sistemului informatic. Editura Universităţii „Dunărea de Jos," Galaţi, 2007.

40. Julia H. Allen et al., Improving the Security of Networked Systems, CrossTalk, 2000.

41. J. Habraken, „Reţele de calculatoare pentru începători”, Editura BIC ALL, 2002.

42. Mircea F. V. Tehnologii de securitate alternative pentru aplicaţii în reţea. Universitatea Tehnică din Cluj Napoca, 2009.

43. McClure Stuart, „Securitatea reţelelor”, Editura Teora, 2002.

44. Mihai Ioan-Cosmin; „Securitatea sistemului informatic”, ISBN Galați, Ed. Dunărea de Jos, 2023.

45. Năstase, F., Securitatea afacerilor electronice, Curs- Informatică Economică, ASE, 2020.

46. Neeraj, S., Perniu L., Chong,R. ş.a. Baze de date-Fundamente, 2010

47. Patriciu Victor-Valeriu, Pietroşanu-Ene Monica, Bica Ion, Cristea Costel-Securitatea informatică în UNIX şi INTERNET, Editura Tehnică, 2018.

48. Patriciu Victor-Valeriu, Pietroşanu-Ene Monica, Bica Ion, Priescu Justin-Semnături electronice şi securitate informatică. Aspecte criptografice, tehnice, juridice şi de standardizare, Editura BIC ALL, 2006.

49. Petersen R. Security Breaches: Notification, Treatment and Prevention, EDUCAUSE review, 2005.

50. Ramón J. Hontanon. Securitatea reţelelor. Editura „Teora,” Bucureşti, 2003.

51. R. Daniel Zatu, „Reţele de calculatoare în era Internet”, Editura Economică, 2002.

52. Rusnac A. Aspecte ale teoriei securităţii, Chişinău, 2005.

53. Stanciu V., Tinca A. Securitatea informației. Principii și bune practici. Ediția a doua, 2015.

54. S. Bellovin and W. Cheswich, Firewalls and Internet Security, MA: Addison- Wesley Publishing Co., 2007.

55. Thomas T., Primii paşi în securitatea reţelelor, Corint, Bucureşti, 2005.

56. Udroiu M., Popa C. Securitatea informaţiilor în societatea informațională. Editura Universitară, 2010.

57. Vasilescu Andrei, Rachieru Dan, Vasile Irina, Filip Luminiţa, Vasilescu Elena-Ghid de aplicare a recomandărilor europene referitoare la confidenţialitatea comunicaţiilor, INSCC, decembrie 2015.

58. Walters N. Into the Breach: Security Breaches and Identity Theft, AARP Public Policy Institute, July 2006.

59. Wiener, N. Cybernetics; or control and communication in the animal and the machine. John Wiley, 2022.

60. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. — М.:Книжный мир, 2009. — 352 с.