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

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

_____

„____” _____2025

Elaborarea sistemelor de securitate cibernetică a rețelelor militare optimizate prin metode criptografice

Teză de master

Student: **Olari Mihail, SISRC-231M**

Conducător: **Dorogan Andrei, dr.,conf.univ.**

Chişinău, 2025

Adnotare

Olari Mihail „Elaborarea sistemelor de securitate cibernetică a rețelelor militare optimizate prin metode criptografice” or. Chișinău, 2025.

Teza cuprinde: introducere, 3 compartimente, concluzii şi recomandări, bibliografia de 30 titluri şi este perfectată pe 54 pagini, din care 44 pagini partea de bază, inclusiv 13 figuri, 2 tabele şi 4 diagrame.

Cuvintele cheie: militar, cibernetic, CERTES, securitate, criptografie, metode, AES, strategic, rețele, cibernetică avansată, integritate informațională, protecție criptografică, infrastructură militară, segregare rețele, criptare adaptivă, reziliență cibernetică.

Scopul şi obiectivele lucrării: Dezvoltarea infrastructurii informaționale prin delimitarea fizică a rețelelor informaționale, în unitățile militare/instituții, pentru asigurarea și organizarea comunicațiilor sigure și protejate (securizate) a fluxului de informații și documente clasificate (atribuite la secret de stat), dintre organul superior de conducere și instituțiile subordonate, precum și îmbunătățirea securității cibernetice.

Asigurarea scopului propus presupune realizarea obiectivelor precum: elaborarea unor soluții de securitate cibernetică adaptate cerințelor operaționale ale rețelelor militare, optimizarea rețelelor militare existente prin implementarea metodelor avansate de criptografie, creșterea rezilienței cibernetice prin integrarea tehnologiilor de monitorizare în timp real și soluțiilor criptografice.

Această lucrare reprezintă un studiu ce ține de analiza și optimizarea securității cibernetice a rețelelor militare, axându-se pe implementarea metodelor criptografice avansate pentru protecția comunicațiilor clasificate. Scopul principal al tezei constă în dezvoltarea unor soluții care să asigure confidențialitatea, integritatea și disponibilitatea informațiilor militare, prin aplicarea unor metode criptografice robuste și a unei delimitări logice și fizice a rețelelor.

Un rol deosebit în lucrare îl ocupă partea teoretică, unde sunt descrise aspectele generale ale criptografiei, noțiunile fundamentale de securitate cibernetică, analiza amenințărilor specifice rețelelor militare, precum și tehnologiile existente pentru apărarea acestora.

În partea practică a tezei este proiectat și implementat un sistem de securitate bazat pe metode criptografice, utilizând algoritmi precum AES și RSA. Soluția propusă include delimitarea fizică și logică a rețelelor informaționale militare și integrarea dispozitivelor de criptare pentru a proteja fluxurile de date sensibile. De asemenea, se realizează o evaluare economică a soluției implementate, subliniind fezabilitatea acesteia în contextul necesităților operaționale ale Armatei Naționale. Lucrarea contribuie semnificativ la îmbunătățirea rezilienței cibernetice și propune un model ce poate fi aplicat gradual, reducând impactul financiar asupra infrastructurilor militare existente deoarece Ministerul Apărarii dispune de proprii specialiști care în comun cu reprezenții companiilor ce furnizează soluțiile, execută o parte din lucrări/misiuni care sunt remunerate conform salarizării.

Annotation

Olari Mihail, „Development of cyber security systems for military networks optimized using cryptographic methods", Chișinău, 2025.

The thesis includes: an introduction, three chapters, conclusions and recommendations, a bibliography with 30 references, and is presented over 54 pages, of which 44 pages constitute the main content, including 13 figures, 2 tables, and 4 diagrams.

Keywords: military, cybernetic, CERTES, security, cryptography, methods, AES, strategic, networks, advanced cybersecurity, informational integrity, cryptographic protection, military infrastructure, network segregation, adaptive encryption, cyber resilience.

Purpose and objectives of the work: The aim is to develop informational infrastructure through the physical segregation of informational networks within military units/institutions to ensure secure and protected communication of classified information and documents (state secrets) between higher command authorities and subordinate institutions, as well as to enhance cybersecurity.

Achieving the proposed goal entails the following objectives: developing cybersecurity solutions tailored to the operational requirements of military networks, optimizing existing military networks by implementing advanced cryptographic methods, increasing cyber resilience through the integration of real-time monitoring technologies and cryptographic solutions.

This thesis represents a study focused on the analysis and optimization of cybersecurity for military networks, emphasizing the implementation of advanced cryptographic methods for protecting classified communications. The primary goal of the thesis is to develop solutions that ensure the confidentiality, integrity, and availability of military information by applying robust cryptographic methods and implementing logical and physical network segregation.

A significant portion of the work is dedicated to the theoretical framework, where general aspects of cryptography, fundamental concepts of cybersecurity, analysis of specific threats to military networks, and existing defense technologies are approached.

The practical part of the thesis includes the design and implementation of a security system based on cryptographic methods, utilizing algorithms such as AES and RSA. The proposed solution incorporates physical and logical segregation of military informational networks and the integration of encryption devices to secure sensitive data flows. Additionally, an economic evaluation of the implemented solution is conducted, highlighting its feasibility in meeting the operational needs of the National Army. This research significantly contributes to improving cyber resilience and proposes a scalable model that can be gradually implemented, reducing the financial impact on existing military infrastructures. This is achieved since the Ministry of Defense employs its own specialists who, together with solution providers, perform part of the tasks/missions, remunerated according to the existing salary framework.

Cuprins

Introducere

În contextul evoluției accelerate a tehnologiilor informaționale, protecția cibernetică a devenit un domeniu esențial pentru securitatea națională și globală. Rețelele militare, prin natura lor, reprezintă ținte critice pentru atacurile cibernetice, având în vedere rolul lor fundamental în asigurarea schimbului de informații clasificate și coordonării operațiunilor strategice. Creșterea complexității și frecvenței atacurilor cibernetice subliniază necesitatea adoptării unor soluții inovatoare și robuste de securitate.

Această teză are ca obiectiv principal proiectarea unui sistem optimizat de securitate cibernetică pentru rețelele militare, utilizând metode avansate de criptografie. Scopul lucrării constă în dezvoltarea unei infrastructuri care să asigure confidențialitatea, integritatea și disponibilitatea informațiilor clasificate, protejând fluxurile critice de comunicații împotriva amenințărilor interne și externe.

Lucrarea este structurată în trei capitole care acoperă aspectele teoretice, practice și economice ale soluțiilor propuse.

Capitolul 1 oferă fundamentele teoretice ale securității cibernetice, prezentând noțiunile esențiale de criptografie, amenințările și vulnerabilitățile specifice rețelelor militare, precum și tehnologiile și metodologiile de apărare cibernetică. Această bază teoretică este necesară pentru a înțelege provocările și cerințele actuale ale securității informațiilor în rețelele militare.

Capitolul 2 se concentrează pe proiectarea unui sistem de securitate cibernetică optimizat prin utilizarea criptografiei. Sunt detaliate arhitectura propusă, metodele criptografice aplicabile și implementarea măsurilor de protecție, evidențiind soluțiile inovatoare care răspund cerințelor specifice ale rețelelor militare.

Capitolul 3 analizează aspectele economice ale soluției propuse, incluzând costurile de implementare și întreținere, performanța sistemului în prevenirea și detectarea atacurilor, precum și adaptabilitatea acestuia la nevoile rețelelor militare. De asemenea, se subliniază necesitatea unor cheltuieli suplimentare pentru a asigura o protecție completă.

În final, lucrarea formulează concluzii și propuneri bazate pe analiza efectuată, oferind recomandări pentru implementarea și utilizarea sistemului de securitate cibernetică în infrastructurile militare.

Această lucrare nu doar că explorează soluțiile tehnice și economice pentru protecția rețelelor militare, dar contribuie și la înțelegerea profundă a provocărilor și oportunităților în domeniul securității cibernetice. Rezultatele obținute pot servi drept fundament pentru dezvoltarea unor strategii naționale de apărare cibernetică, adaptate unui peisaj tehnologic în continuă schimbare. De asemena planul elaborat de delimitare fizică a rețelelor existente și instalarea unor soluții de criptare în arhitectura rețelelor Armatei Naționale, ar putea fi implimentate etapizat, astfel fără a simți efortul financiar enorm al instituției de apărare.

Bibliografie

1. William Stallings, Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson, 2016; p. 384-386, p. 392, 404, 410.
2. Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Education, 2013; p.512-514;
3. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, Wiley, 2015; p. 220, 315, 340
4. NIST, Specification for the Advanced Encryption Standard (AES), FIPS PUB 197; p.7, p. 10.
5. Document PDF: Quantum-Resistant Algorithms; p. 4, 8,
6. Raport Microsoft, *Cyberattacks in Ukraine*, 2022.
7. Alfred J. Menezes, Handbook of Applied Cryptography, CRC Press, 2018; p. 230-280.
8. Douglas R. Stinson, Cryptography: Theory and Practice, CRC Press, 2019; p. 120-165.
9. NIST. "Specification for the Advanced Encryption Standard (AES)". FIPS PUB 197. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf accesat la pagina 7.
10. William Stallings. "Cryptography and Network Security: Principles and Practice". Sixth Edition, Pearson, 2013.
11. Bruce Schneier. "Applied Cryptography: Protocols, Algorithms, and Source Code in C". Second Edition, Wiley, 1996.
12. https://certesnetworks.com/encryption-appliances/
13. https://www.army.md/img/userfiles/info/aquizition/plan_2024_1205.pdf
14. Behrouz A. Forouzan, Cryptography and Network Security, McGraw-Hill Education, 2013; p. 512-514.
15. Alfred J. Menezes, Handbook of Applied Cryptography, CRC Press, 2018; p. 230-280.
16. Rafail Ostrovsky și William E. Skeith III, A Survey of Cryptographic Protocols for Secure Multi-Party Computation, Springer, 2020.
17. NIST Special Publication 800-77, Guide to IPsec VPNs, 2021; p. 15-45.
18. Kathy Wainaina, Network Security for Military Communications, Wiley, 2019; p. 88-124.
19. Microsoft Cybersecurity Field Manual, VPNs and Secure Data Transmission Strategies, 2020.
20. Cisco Systems, VPN Solutions for Secure Military Communications, 2022.
21. https://www.legis.md/cautare/getResults?doc_id=135512&lang=ro
22. Certes Networks – Certes Networks Encryption Solutions. Descrierea soluțiilor Layer 4 pentru rețele militare și dispozitivele CEP (CryptoFlow Enforcement Points).

23. Thales Group – High-Speed Network Encryption Solutions. Detalii despre encryptoarele CN4010, CN6140 și platforma Security Management Center (SMC).

24. NIST Special Publication 800-77 – Guide to IPsec VPNs, 2021. Ghid tehnic pentru utilizarea criptografiei în VPN-uri.

25. ENISA (European Union Agency for Cybersecurity) – ENISA Publications. Ghiduri pentru implementarea standardelor de securitate cibernetică în infrastructuri critice.

26. Cisco Systems – VPN and Network Security Solutions. Soluții de criptare și securitate pentru rețele militare.

27. Microsoft Security – Cybersecurity Best Practices. Recomandări pentru securizarea rețelelor militare și managementul cheilor.

28. Journal of Cybersecurity (Oxford Academic). Articole despre criptografia avansată și reziliența cibernetică aplicată în rețelele militare.

29. IEEE Transactions on Information Forensics and Security. Cercetări despre implementarea soluțiilor criptografice în rețele distribuite.

30. OpenSSL Documentation – OpenSSL Resources. Referințe tehnice pentru utilizarea protocoalelor criptografice în aplicații militare.