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

Admis la susţinere
Şefă departament:
Tîrșu Valentina, conf. univ., dr
_____
„____”_____ 2024

ASIGURAREA SECURITĂȚII TRANSFERULUI DOCUMENTELOR ELECTRONICE CLASIFICATE CA SECRET DE STAT

Teză de master

Student: **Robu Dorin, grupa SISRC-221M**
Conducător: **Cerbu Olga, conf. univ., dr.**

Chişinău, 2024

ADNOTARE

Autorul: Robu Dorin gr SISRC-221M

Tema: Asigurarea securității transferului documentelor electronice clasificate ca secret de stat.

Structura lucrării: constă din pagini de titlu, aviz, rezumat, introducere, 4 capitole, concluzii și bibliografie.

Cuvinte cheie: secret de stat, securitatea națională, securitatea informațională, trafic de date, criptografia, comunicarea în sistemele secrete, PKI.

Problematica studiului: Analiza mijloacelor de construire a rețelelor și tunelurilor de comunicații informaționale sigure .

Scopul lucrării: Este de a identifica algoritmi criptografice simetrici și asimetrici cu structura deschisă, de a le testa stabilitatea criptografică atât separat, cât și ca o soluție complexă la criptarea pe mai multe niveluri, precum și de a analiza mijloacele de construire a rețelelor și tunelurilor de comunicații informaționale sigure.

Obiectivele:

1. Analiza și clasificare documentelor secrete de stat.
2. Studierea metodelor de protecție a informațiilor.
3. Dezvoltarea unui sistem informatic de transmitere a datelor secrete de stat.
4. Dezvoltarea unui sistem de informații securizat.
5. Examinarea Arhitectura sistemului de informații.
6. Testarea pentru intruziuni și interceptări.

Metode aplicate: Au fost utilizate metodele de cercetare bibliografică, analiză, sinteză, proiectare și testare.

Rezultatele obținute: A fost elaborat, un sistem informațional pentru criptarea end-to-end a documentelor digitale de o importanță deosebită (documente al căror conținut este clasificat ca secrete de stat), a fost construită o infrastructură de rețea sigură bazată pe soluții open source.La fel materialele din teza pot sta la baza dezvoltării unor lucrări de cercetare suplimentare, manuale și cursuri de specialitate.

ANNOTATION

Author: Dorin Robu, SISRC-221M .

Topic: Securing the Transfer of Electronic Documents Classified as State Secrets.

Work Structure: The work consists of a title page, abstract, introduction, four chapters, conclusions, and bibliography.

Keywords: state secret, national security, information security, data traffic, cryptography, communication in secret systems, PKI.

Research Problem: Analysis of the means of building secure information communication networks and tunnels.

Purpose of the Work: The purpose of this work is to identify open-source symmetric and asymmetric cryptographic algorithms, to test their cryptographic stability both separately and as a complex solution to multilevel encryption, and to analyze the means of building secure information communication networks and tunnels.

Objectives:

1. Analysis and classification of classified state documents..

2. Study of information protection methods.

3.Development of an information system for transmitting classified state data.

4.Develop a secure information system.

5.Examine the architecture of the information system.

6.Test for intrusions and interceptions.

Methods Applied: Bibliographic research, analysis, synthesis, design, and testing methods were used.

Results Obtained: An information system for end-to-end encryption of digital documents of particular importance (documents whose content is classified as state secrets) was developed, and a secure network infrastructure based on open source solutions was built. Additionally, the materials in the thesis can form the basis for the development of additional research papers, manuals, and specialized courses.

CUPRINS

INTRODUCERE

Scopul secretului de stat este de a crea condiții pentru funcționarea statului în ansamblu, precum și a organizațiilor strategice individuale, prevenind amenințările la adresa securității, protejând interesele legale de divulgare, pierdere, scurgere, distorsionare și distrugere a informațiilor de serviciu, asigurând în cadrul activității de producție toate subdiviziunile organizației.

Asigurarea securității traficului documentelor digitale care conțin informații clasificate ca secret de stat este un proces complex și dificil, care necesită o abordare integrată. Pe lângă metodele și tehnicile de criptare, sunt necesare și măsuri de securitate fizică, precum și proceduri de lucru bine definite și implementate.

Principiile privind mijloacele de organizare și protecție a acestui proces sunt stabilite de organele legislative și executive, care au o responsabilitate majoră în asigurarea securității statului. Aceste principii sunt foarte scrupuloase și sunt concepute pentru a proteja informațiile clasificate de divulgare, pierdere, scurgere, distorsionare și distrugere.

Cu toate acestea, în era informaționalizării, aceste principii devin din ce în ce mai dificil de implementat. Tehnologiile moderne de comunicare și stocare a datelor fac mai ușor pentru cei rău intenționați să acceseze și să fure informații clasificate.

Inovații necesare:

Pentru a face față acestor provocări, este necesar să se investească în inovații în domeniul securității informaționale. Aceste inovații ar trebui să vizeze atât îmbunătățirea metodelor și tehnicilor de criptare, cât și dezvoltarea de noi măsuri de securitate fizică și proceduri de lucru.

Câteva exemple de inovații posibile

Utilizarea inteligenței artificiale pentru a detecta și preveni atacurile cibernetice.

Dezvoltarea de noi algoritmi de criptare care sunt mai rezistenți la atacurile moderne.

Implementarea de sisteme de securitate fizică mai sofisticate, cum ar fi camere de supraveghere cu inteligență artificială.

Creșterea gradului de conștientizare a angajaților cu privire la riscurile de securitate informațională.

De exemplu, metoda de protecție a datelor în procesul de transmitere prin intermediul rețelelor de comunicații utilizând criptare simetrică este foarte învechită, deoarece necesită transmiterea separată a cheilor de criptare prin alte canale de comunicare securizate, iar aceste canale, la rândul lor, necesită protecție. În cazul utilizării canalelor de transmitere a cheilor simetrice de criptare prin intermediul schimbului direct de la mână la mână, așa cum se întâmplă în spațiul post-sovietic, acest lucru este extrem de dificil.

Astfel, obiectul cercetării constă în elementele și factorii de asigurare a securității secretului de stat în procesul de transmitere prin intermediul rețelelor de comunicații. Și studiul potențialului metodelor asimetrice de criptare pentru organizarea acestui proces. Metodele de cercetare utilizate în lucrare sunt cercetarea bibliografică, analiza, sinteza, proiectarea și testarea.

Valoarea teoretică a lucrări constă în dezvoltarea tendințelor de dezvoltare a software-ului de calitate, a sistemelor informaționale și a infrastructurii de rețea, bazate doar pe soluții cu cod sursă deschis.

Valoarea aplicată a lucrări constă în rezultatul metodei complexe de criptare dezvoltate, precum și în produsul final acceptat în exploatare de către instituții a Statului. În același timp, materialele lucrării pot servi ca bază pentru dezvoltarea unor lucrări științifice ulterioare, manuale didactice, ghiduri și cursuri specializate.

Scopul lucrării de masterat este de a dezvolta un sistem informațional pentru asigurarea traficului sigur al documentelor care conțin secret de stat. Acest sistem ar trebui să ofere următoarele beneficii:

Siguranță: Sistemul ar trebui să fie capabil să protejeze datele de divulgare, pierdere, scurgere, distorsionare și distrugere.

Eficiență: Sistemul ar trebui să fie ușor de utilizat și să nu introducă întârzieri semnificative în transmiterea documentelor.

Costuri reduse: Sistemul ar trebui să fie bazat pe algoritmi cu sursă deschisă, pentru a reduce costurile de dezvoltare și implementare.

Pentru a atinge scopul stabilit în lucrare, este necesar să rezolvați următoarele obiective:

1. Analiza și clasificare documentelor secrete de stat.

2. Studierea metodelor de protecție a informațiilor.

3. Dezvoltarea unui sistem informatic de transmitere a datelor secrete de stat.

4. Dezvoltarea unui sistem de informații securizat.

5. Examinarea Arhitectura sistemului de informații.

6. Testarea pentru intruziuni și interceptări.

Cerințe pe care sistemul trebuie să le îndeplinească:

- Metode de criptare:

Sistemul ar trebui să utilizeze metode de criptare moderne, care sunt rezistente la atacurile moderne.

- Distribuție a cheilor:

Sistemul ar trebui să ofere un mod sigur și convenabil de a distribui cheile de criptare către utilizatorii autorizați.

- Arhitectură de rețea:

Sistemul ar trebui să fie bazat pe o arhitectură de rețea sigură, care să protejeze datele de acces neautorizat.

- Inovații posibile

În plus față de aspectele menționate mai sus, lucrarea de masterat ar putea explora și următoarele inovații:

- Utilizarea inteligenței artificiale pentru a detecta și preveni atacurile cibernetice.

Dezvoltarea de noi algoritmi de criptare care sunt mai rezistenți la atacurile moderne.

Implementarea de tehnologii de securitate fizică, cum ar fi camere de supraveghere cu inteligență artificială.

BIBLIOGRAFIE

1. HOTĂRÎRE Guvernului RM Nr. 1176 din 22-12-2010 pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în cadrul autorităților publice și al altor persoane juridice.

2. PARLAMENTUL Republicii Moldova, LEGE Nr. 245 din 27-11-2008 cu privire la secretul de stat.

3. PARLAMENTUL Republicii Moldova, LEGE Nr. 91 din 27-06-2014 privind semnătura electronică și documentul electronic.

4. Dinu Ţurcanu, Natalia Spinu, Serghei Popovici, Tatiana Ţurcanu. Cybersecurity of the Republic of Moldova: a retrospective for the period 2015-2020. Journal of Social Sciences, Vol. IV, no. 1 (2021), pp. 74 – 83.

5. Dinu Ţurcanu, Serghei Popovici, Tatiana Ţurcanu. Digital signature: advantages, challenges and strategies, Journal of Social Sciences, Vol. III, no. 4 (2020), pp. 62 - 72.

6. ISO 15489-1 Information and documentation — Records management, 2001.

7. ISO/IEC 27003 Information technology — Security techniques — Information security management systems — Guidance, 2017.

8. Aho, Alfred V., Hopcroft, John E., Ullman, Jeffrey D. (1979). "The Design and Analysis of Computer Algorithms." Moscow: Mir Publishers.

9. Singh, Simon. (2006). "The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography." Moscow: Ast, Astrel Publishers.

10. Bauer, Friedrich L. (2007). "Decrypted Secrets: Methods and Principles of Cryptology." Moscow: Mir Publishers.

11. Schneier, Bruce. (2003). "Applied Cryptography: Protocols, Algorithms, and Source Code in C." Moscow: Triumph Publishers.

12. Mao, Wenbo. (2015). "Modern Cryptography: Theory and Practice." Moscow: Williams Publishers.

13. Alferov, A.P., Zubov, A.Yu., Kuzmin, A.S., Cheremushkin, A.V. (2001). "Fundamentals of Cryptography." Moscow: Helios ARV Publishers.

14. Michael DiBernardo et al. (2011). "The Architecture of Open-Source Applications." Available online: http://aosabook.org/en/index.html (accessed on 17.01.2021).

15. Shannon, Claude Elwood. (1949). "Communication Theory of Secrecy Systems."

16. McConnell, Steve. (1996). "Rapid Development."

17. Fowler, Martin. (2002). "Patterns of Enterprise Application Architecture."

18. Zgadzai, I.S., Dubrovin, N.Kh., Safiullin, O.E. (2012). "Information Technology in Jurisprudence." Moscow: Academy Publishers.

19. Gavrilov, M.V., Klimov, V.A. (2013). "Informatics and Information Technologies."

20. Gavrilov, M.V., Sprozheczkaya, N.V. (2006). "Informatics."

21. Shaporev, S.D. (2008). "Informatics. Theoretical Course and Practical Classes." St. Petersburg: BHV-Petersburg Publishers.

22. Bird, Jim. (2016). "DevOpsSec."

23. Linn, Ryan, Andress, Jason. (2017). "Coding for Penetration Testers: Building Better Tools."

24. Marsh, Nicholas. (2015). "Nmap Cookbook: The Fat-Free Guide to Network Security Scanning."

25. Sutton, Michael. (2019). "Fuzzing: Brute Force Vulnerability Discovery."

26. Schneier, Bruce. (2003). "Applied Cryptography: Protocols, Algorithms, and Source Code in C."

27. Panasenko, V.S. (2009). "Encryption Algorithms: A Special Handbook."

28. Kudryashov, B.D. (2016). "Fundamentals of Coding Theory."
29. Clarke, Richard. (2015). "The Fifth Domain."
30. Pasad, Prahar. (2017). "Mastering Modern Web Penetration Testing."
31. McPhee, Michael. (2016). "Mastering Kali Linux for Web Penetration Testing."