**Ministerul Educației și Cercetării al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Electronică și Telecomunicații**

**Departamentul Telecomunicații şi Sisteme Electronice**

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

**----------**
**„___” _____ 2025**

# Proiectarea sistemelor de acces securizat utilizând tehnici avansate de execuție

## Teză de master

**Student:** _____ **Dimitrov Vladislav,** SISRC-231M

**Conducător:** _____ **DOROGAN Andrei,** lec.univ., dr.

**Chişinău, 2025**

# REZUMAT

**Tema:** Proiectarea sistemelor de acces securizat utilizând tehnici avansate de execuție .

**Structura lucrării:** Introducere, Capitolul 1: Practica de documentare. Capitolul 2: Investigarea și Implementarea Soluțiilor Avansate pentru Sisteme de Acces Securizat. Capitolul 3: Analiza economică.

**Cuvintele cheie**: Securitate, Trusted Platform Modules (TPM), Autentificarea multi-factor (MFA), Criptografia avansată, Controlul de acces bazat pe roluri (RBAC).

**Scopul lucrării:** Proiectarea sistemelor de acces securizat, utilizând aceste tehnologii avansate, colaborează cu rolul strategic al administratorului de sistem pentru a crea o infrastructură IT robustă și sigură.

**Obiectivele:**

1. **Crearea unei infrastructuri securizate pentru accesul la resurse critice**
   - Proiectarea unui sistem bazat pe servere dedicate și module TPM pentru a garanta confidențialitatea, integritatea și disponibilitatea datelor sensibile.
2. **Implementarea autentificării avansate multi-factor (MFA)**
   - Dezvoltarea unui mecanism de autentificare sigur utilizând combinarea codurilor OTP, biometriei și modulelor hardware pentru prevenirea accesului neautorizat.
3. **Integrarea criptografiei moderne pentru protecția datelor**
   - Utilizarea algoritmilor AES-256 și a tehnologiilor enclave hardware pentru criptarea datelor sensibile și reducerea vulnerabilităților.
4. **Optimizarea performanței aplicațiilor critice**
   - Configurarea serverelor dedicate pentru timpi de procesare reduși și eficiență ridicată în gestionarea volumelor mari de date.
5. **Dezvoltarea unei soluții scalabile și conforme cu reglementările internaționale**
   - Asigurarea compatibilității cu standarde precum GDPR, PCI DSS și HIPAA, pentru adoptarea soluției în diverse sectoare.
6. **Monitorizarea și analiza activităților utilizatorilor**
   - Crearea unui mecanism de audit și supraveghere pentru detectarea comportamentelor suspecte și prevenirea incidentelor de securitate.
7. **Evaluarea impactului economic și a raportului cost-beneficiu al soluției**
   - Analizarea investiției și a beneficiilor asociate pentru a demonstra fezabilitatea financiară a implementării soluției propuse.

**Metodele aplicate:** Java, Fernet cryptography, Django, Pytop , platforma Kubernetes, metoda criptării, securizării . Precum și controalele de acces bazate pe roluri (RBAC).

**Rezultatele obținute:** Obținerea unui sistem de acces securizat utilizând tehnici avansate de execuție implică implementarea unor mecanisme robuste (MFA), criptare, (RBAC). Acest proces include utilizarea enclavelor hardware și a modulelor de platformă securizată (TPM).

## SUMMARY

**Title:** Designing Secure Access Systems Using Advanced Execution Techniques.

**Structure :** Introduction, Chapter 1: Documentation Practice, Chapter 2: Investigation and Implementation of Advanced Solutions for Secure Access Systems, Chapter 3: Economic Analysis

**Keywords:** Security, Trusted Platform Modules (TPM), Multi-Factor Authentication (MFA), Advanced Cryptography, Role-Based Access Control (RBAC)

**Target:** To design secure access systems using advanced technologies, collaborating with the strategic role of the system administrator to create a robust and secure IT infrastructure.

**Objectives:**

1. **Creating a secure infrastructure for accessing critical resources**
    - Design a system based on dedicated servers and TPM modules to ensure the confidentiality, integrity, and availability of sensitive data.
2. **Implementing advanced multi-factor authentication (MFA)**
    - Develop a secure authentication mechanism using a combination of OTP codes, biometrics, and hardware modules to prevent unauthorized access.
3. **Integrating modern cryptography for data protection**
    - Utilize AES-256 algorithms and hardware enclave technologies to encrypt sensitive data and reduce vulnerabilities.
4. **Optimizing the performance of critical applications**
    - Configure dedicated servers for reduced processing times and high efficiency in managing large data volumes.
5. **Developing a scalable solution compliant with international regulations**
    - Ensure compatibility with standards like GDPR, PCI DSS, and HIPAA for adoption in various sectors.
6. **Monitoring and analyzing user activities**
    - Create an audit and supervision mechanism to detect suspicious behaviors and prevent security incidents.
7. **Evaluating the economic impact and cost-benefit ratio of the solution**
    - Analyze the investment and associated benefits to demonstrate the financial feasibility of implementing the proposed solution.

**Applied Methods:** Java, Fernet cryptography, Django, PyOTP, Kubernetes platform, encryption, security method. As well as role-based access controls (RBAC).

**Results Achieved:** Achieving a secure access system using advanced execution techniques involves implementing robust mechanisms (MFA), encryption, (RBAC). This process includes the use of hardware enclaves and secure platform modules (TPM).

**CUPRINS**

# INTRODUCERE

Importanța Securității Cibernetice - este crucială pentru protejarea resurselor digitale și a informațiilor sensibile, care sunt din ce în ce mai vulnerabile la atacuri. Măsurile de securitate previn furtul de date confidențiale și contribuie la integritatea organizațiilor, menținând totodată încrederea consumatorilor. Riscurile criminalității cibernetice sunt alarmante, afectând atât companiile mari, cât și utilizatorii obișnuiți care folosesc servicii cloud. Tehnicile de atac, cum ar fi phishing-ul și ransomware-ul și atacuri DDoS, devin tot mai sofisticate, iar neglijența utilizatorilor amplifică aceste riscuri. Organizațiile sunt ținte principale pentru atacatori datorită valorii datelor pe care le dețin.

**Proiectarea sistemelor de acces securizat -** se concentrează pe protejarea resurselor și datelor sensibile împotriva accesului neautorizat, folosind tehnologii avansate de autentificare, criptare și control de acces. Aceste sisteme utilizează tehnici moderne precum autentificarea multi-factor (MFA), criptografia avansată, controlul de acces bazat pe roluri (RBAC) și execuția în medii securizate, cum ar fi enclavările hardware și Trusted Platform Modules (TPM). Rolul unui **Administrator de sistem (System Administrator) -** este esențial în implementarea și întreținerea acestor sisteme securizate. Administratorii de sistem gestionează infrastructura IT și sunt responsabili de configurarea și monitorizarea soluțiilor de acces, instalarea și întreținerea hardware-ului și software-ului, gestionarea conturilor de utilizator și permisiunilor, precum și monitorizarea securității rețelelor și sistemelor. De asemenea, aceștia asigură că sistemele sunt conforme cu politicile de securitate și gestionează incidentele de securitate prin aplicarea de patch-uri și soluții de recuperare după dezastre. Integrarea tehnicilor avansate de execuție și a tehnologiilor emergente precum Inteligența Artificială (AI), învățarea automată (ML) și blockchain ajută la detectarea anomaliilor și a comportamentelor suspecte, reducând astfel riscul atacurilor cibernetice.

În această lucrare, o să explorez cum proiectarea sistemelor de acces securizat, utilizând aceste tehnologii avansate, colaborează cu rolul strategic al administratorului de sistem pentru a crea o infrastructură IT robustă și sigură. Cu drept scop de a dezvolta și implimenta un sistem de acces securizat în domeniul IT de progres.

**BIBLIOGRAFIE**


1. https://www.sans.org
2. https://www.nist.gov/cyberframework
3. https://owasp.org
4. Bellare, M., & Rogaway, P., *"Optimal Asymmetric Encryption – How to Encrypt with RSA,"* Advances in Cryptology.
5. Ferraiolo, D.F., Kuhn, R., *"Role-Based Access Control,"* 15th National Computer Security Conference.
6. Rivest, R.L., Shamir, A., & Adleman, L., *"A Method for Obtaining Digital Signatures and Public-Key Cryptosystems"*.
7. IBM Security, *"Cost of a Data Breach Report 2024"*.
8. Cybersecurity Ventures, *"Cybercrime Report 2024"*.
9. Trellix Endpoint Security.
10. Kubernetes Documentation.
11. *TPM (Trusted Platform Module) Specifications***,** TCG (Trusted Computing Group).
12. 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/
13. PECA, L., ȚURCANU, D. Reducing cyber risk through a human-centered approach. In: The 13th International Conference on Electronics, Communications and Computing. IC ECCO-2024, 17-18 October, 2024, Chisinau, Republic of Moldova. http://repository.utm.md/bitstream/handle/5014/28769/Int-Conf-ECCO-2024-Abstract-Book-p111-112.pdf?sequence=1&isAllowed=y
14. 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/
15. ȚURCANU, D., PRISĂCARU, A., PECA, L., ȚURCANU, T. Cyber security professional development within CYBERCOR. In: The 13th International Conference on Electronics, Communications and Computing. IC ECCO-2024, 17-18 October, 2024, Chisinau, Republic of Moldova.

http://repository.utm.md/bitstream/handle/5014/28823/Int-Conf-ECCO-2024-Abstract-Book-p212-213.pdf?sequence=1&isAllowed=y

16. 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.utm.2021.4(1).10
17. 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
18. Sava, L., Vortolomei, D. Organizarea şi analiza activităţii economice în domeniul telecomunicaţiilor. Note de curs, Chişinău, Editura UTM, 2022, ISBN: 978-9975-45-805-4.