

**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 dr., conf.univ.**

„\_\_\_\_\_” \_\_\_\_\_ 2025

# **SECURIZAREA TRANZACȚIILOR ELECTRONICE ÎN SISTEMELE INFORMATICE DE VÂNZĂRI**

**Teză de master**

**Student: Comanac Artiom, SI-231M**

**Coordonator: Bulai Rodica, lect. univ.**

**Consultant: Cojocaru Svetlana, asist.univ.**

**Chișinău, 2025**

## CUPRINS

<b>INTRODUCERE</b> .....	<b>7</b>
<b>1 ANALIZA DOMENIULUI DE STUDIU</b> .....	<b>8</b>
1.1 Analiza sistemelor informatice pentru înregistrarea operațiunilor de casa.....	9
1.2 Tipuri de tranzacții electronice în sistemele informatice de vânzări .....	10
1.3 Analiza comunicării cu serviciul guvernamental în baza sistemelor existente.....	12
1.4 Amenințări în procesul efectuării tranzacțiilor electronice.....	14
1.5 Reglementări normative în securitatea tranzacțiilor electronice.....	17
1.6 Cerințe de securitate pentru sistemele informatice de vânzări.....	19
<b>2 SECURIZAREA TRANZACȚIILOR ELECTRONICE</b> .....	<b>22</b>
2.1 Tehnici și metode existente de securizare a tranzacțiilor electronice .....	22
2.2 Metode de autentificare în procesul comunicării cu serviciile guvernamentale .....	25
2.3 Utilizarea mecanismelor de criptare și semnare a tranzacțiilor electronice.....	26
2.3.1 Modul criptografic fizic – Smart-card / SIM .....	28
2.3.2 Modul criptografic electronic cu utilizarea certificatelor .....	29
2.4 Metode de securizare a canalului de comunicare.....	30
2.5 Mecanisme de protecție a datelor operațiunilor de vânzări .....	31
<b>3 INTEGRAREA METODELOR DE SECURITATE IN SISTEMUL INFORMATIC</b> .....	<b>33</b>
3.1 Modelul securității informatice în sistemul informatic.....	34
3.2 Tehnologii și mecanisme de securitate utilizate .....	37
3.3 Implementarea și integrarea modulului criptografic .....	40
3.4 Autentificarea tranzacțiilor electronice în procesul de comunicare cu sistemul guvernamental .....	44
3.5 Implementarea mecanismului de protecție a datelor sensibile.....	46
3.6 Implementarea și integrarea mecanismelor WORM.....	49
3.7 Analiza și testarea securității sistemului informatic și asigurarea conformității cu legislația .....	51
<b>4 RECOMANDĂRI DE SECURITATE PENTRU SISTEMELE INFORMATICE CARE GESTIONEAZĂ TRANZACȚIILE ELECTRONICE</b> .....	<b>55</b>
4.1 Securitatea datelor personale ale clienților în tranzacțiile electronice .....	56
4.2 Criptarea și semnarea tranzacțiilor electronice .....	58
4.3 Securitatea canalului de comunicare.....	60
4.4 Conformitatea cu cerințele ISO și legislația Republicii Moldova .....	61
<b>CONCLUZII</b> .....	<b>63</b>
<b>BIBLIOGRAFIE</b> .....	<b>65</b>

## INTRODUCERE

Cu dezvoltarea comerțului electronic și fizic, precum și cu răspândirea tehnologiilor digitale în societatea modernă, sistemele informaționale de înregistrare a vânzărilor devin o parte integrantă a vieții de zi cu zi. Noile norme legislative prevăd trecerea de la sistemele tradiționale de înregistrare a vânzărilor, precum casele de marcat, la cele noi, care înregistrează tranzacțiile în timp real și transmit datele către serviciile de stat. Totuși, odată cu această tranziție către noi metode de înregistrare a vânzărilor bazate pe tehnologii informaționale, riscul și amenințările de compromitere a acestor sisteme cresc. Amenințările la adresa securității, cum ar fi fraudă, furtul de date personale, accesul neautorizat și modificarea informațiilor, precum și diverse atacuri, devin din ce în ce mai complexe și sofisticate, necesitând implementarea unor metode moderne și eficiente de protecție, care să fie actualizate în mod constant și să țină cont de evoluția rapidă a metodelor de atac asupra acestor sisteme.

Securitatea în procesul de înregistrare și transmitere a tranzacțiilor electronice în sistemele informaționale de vânzări este o sarcină critică, deoarece în prezent acestea constituie un sistem obligatoriu pentru agenții economici, menit să înlocuiască sistemele vechi. Orice întrerupere în funcționarea acestora poate duce la pierderi financiare, afectarea reputației companiei, precum și la probleme legale, întrucât transmiterea întârziată sau distorsionată a tranzacțiilor electronice către serverele administrației fiscale și ale serviciilor de tehnologia informației din domeniul financiar reprezintă o încălcare a legii și poate duce la blocarea activității economice.

Scopul principal al acestei lucrări este de a analiza amenințările existente la adresa securității tranzacțiilor electronice, metodele de protecție a tranzacțiilor în sistemele informaționale moderne de vânzare, precum și cerințele actelor normative și legislative care reglementează bazele și cerințele pentru sistemele informaționale de înregistrare a vânzărilor. Este necesar să se identifice limitările și cerințele legate de securitatea informațiilor impuse de legislație, deoarece crearea sistemului și protecția tranzacțiilor trebuie să țină cont de toate aspectele.

În cadrul acestei lucrări, vor fi analizate riscurile probabile și actuale pentru tranzacțiile electronice în general și pentru sistemele de înregistrare a vânzărilor, precum și posibilitățile de asigurare a securității pe baza cerințelor legislației și standardelor internaționale în domeniul tehnologiilor informaționale și al securității.

## BIBLIOGRAFIE

- [1] „Regulamentul privind schimbul de date dintre echipamentele de casă și de control și Sistemul Informațional Automatizat «Monitorizarea Electronică a Vânzărilor»”. Anexa nr. 1 la Decizia CIECC Nr. 26-11/1-19/01-2021 din 10.06.2021, 10 iunie 2021.
- [2] „HOTĂRÂRE Nr. 55 din 05-02-2020 cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat «Monitorizarea electronică a vânzărilor»”. 5 februarie 2020. Data accesării: 14 octombrie 2024. [Online]. Disponibil la: [https://www.legis.md/cautare/getResults?doc\\_id=120392&lang=ro](https://www.legis.md/cautare/getResults?doc_id=120392&lang=ro)
- [3] „ORDIN Nr. 632 din 18-12-2020 privind aprobarea Regulamentului cu privire la modul de evidență și sigilare a echipamentelor de casă și de control”. 18 decembrie 2020. Data accesării: 10 noiembrie 2024. [Online]. Disponibil la: [https://www.legis.md/cautare/getResults?doc\\_id=145477&lang=ro](https://www.legis.md/cautare/getResults?doc_id=145477&lang=ro)
- [4] „Platforma Guvernamentală de Interoperabilitate”, Agenția de Guvernare Electronică. Data accesării: 10 noiembrie 2024. [Online]. Disponibil la: <https://egov.md/ro/content/platforma-guvernamentala-de-interoperabilitate>
- [5] Loreto Damasco Jr, „Safeguarding Transactional Data: A Comprehensive Investigation of VPN Integration in Point-of-Sale Systems for Enhanced Security and Connectivity”, Eximia, dec. 2023, Data accesării: 1 decembrie 2024. [Online]. Disponibil la: [https://www.academia.edu/122822446/Safeguarding\\_Transactional\\_Data\\_A\\_Comprehensive\\_Inv estigation\\_of\\_VPN\\_Integration\\_in\\_Point\\_of\\_Sale\\_Systems\\_for\\_Enhanced\\_Security\\_and\\_Connec tivity](https://www.academia.edu/122822446/Safeguarding_Transactional_Data_A_Comprehensive_Inv estigation_of_VPN_Integration_in_Point_of_Sale_Systems_for_Enhanced_Security_and_Connec tivity)
- [6] Steven A. Harrast, „Robotic process automation in accounting systems - Harrast - 2020 - Journal of Corporate Accounting & Finance - Wiley Online Library”, iun. 2020, Data accesării: 1 decembrie 2024. [Online]. Disponibil la: <https://onlinelibrary.wiley.com/doi/abs/10.1002/jcaf.22457>
- [7] „Preventing Man in the Middle Attack Network Projects”, Network Simulation Tools. Data accesării: 6 octombrie 2024. [Online]. Disponibil la: <https://networksimulationtools.com/man-in-the-middle-attack-network-projects/>
- [8] „Decizie Nr. 26-11/1-19/01 din 10-06-2021”. Data accesării: 3 octombrie 2024. [Online]. Disponibil la: [https://www.legis.md/cautare/getResults?doc\\_id=141182&lang=ro#](https://www.legis.md/cautare/getResults?doc_id=141182&lang=ro#)
- [9] Ziyad R. Alashhab, Mohammed Anbar, Manmeet Mahinderjit Singh, Iznan H. Hasbullah, Prateek Jain and Taief Alaa Al-Amiedy, „Distributed Denial of Service Attacks against Cloud Computing Environment: Survey, Issues, Challenges and Coherent Taxonomy”, dec. 2022, Data accesării: 2 decembrie 2024. [Online]. Disponibil la: <https://www.mdpi.com/2076-3417/12/23/12441>

- [10] Razieh Nokhbeh Zaeem, K. Suzanne Barber, „The Effect of the GDPR on Privacy Policies: Recent Progress and Future Promise: ACM Transactions on Management Information Systems: Vol 12, No 1”, dec. 2020, Data accesării: 3 decembrie 2024. [Online]. Disponibil la: <https://dl.acm.org/doi/abs/10.1145/3389685>
- [11] „Cerințele tehnice față de echipamentele de casă și de control”. Anexa nr. 1 la Decizia CIECC nr. 26-11/1-19/02-2020 din 20 octombrie 2020, 20 octombrie 2020.
- [12] Darapureddy Devendra Kumar, Jerripothula Desai Mukharzee, Chirla Vijay Durga Reddy, Shinu M. Rajagopal, „Safe and Secure Communication Using SSL/TLS | IEEE Conference Publication | IEEE Xplore”, apr. 2024, Data accesării: 1 decembrie 2024. [Online]. Disponibil la: <https://ieeexplore.ieee.org/abstract/document/10497224>
- [13] R. Singh, „Auditing a POS System”, în *Modernizing Enterprise IT Audit Governance and Management Practices*, IGI Global Scientific Publishing, 2023, pp. 211–237. doi: 10.4018/978-1-6684-8766-2.ch008.
- [14] R. Bulai și N. Snegur, „Model de securitare a aplicațiilor mobile în baza analizei STRIDE”, 9 th International Conference on Microelectronics and Computer Science, Chisinau, Republic of Moldova, October 19-21, 2017, 2017, doi: 978-9975-4264-8-0.
- [15] „What is Transport Layer Security (TLS)?”. Data accesării: 14 octombrie 2024. [Online]. Disponibil la: <https://www.wallarm.com/what/what-is-transport-layer-security>
- [16] Y. Li și Q. Liu, „A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments”, *Energy Reports*, vol. 7, pp. 8176–8186, nov. 2021, doi: 10.1016/j.egy.2021.08.126.
- [17] R. Awadallah și A. Samsudin, „Using Blockchain in Cloud Computing to Enhance Relational Database Security”, *IEEE Access*, vol. 9, pp. 137353–137366, 2021, doi: 10.1109/ACCESS.2021.3117733.
- [18] „Regulamentul privind certificarea echipamentelor de casă și de control”. Anexa nr. 2 la Decizia CIECC Nr. 26-11/1-19/01-2021 din 10.06.2021, 10 iunie 2021.
- [19] „Regulamentul privind funcționarea Centrului de certificare a echipamentelor de casă și de control”. Anexa nr. 3 la Decizia CIECC Nr. 26-11/1-19/01-2021 din 10.06.2021, 10 iunie 2021.
- [20] A. Comanac, „Generarea de cod cu ajutorul inteligenței artificiale: riscuri și beneficii”, Conferința tehnico-științifică a studenților, masteranzilor și doctoranzilor / Technical Scientific Conference of Undergraduate, Master and PhD Students: Chișinău, vol. 1, mar. 2024, doi: 978 9975-64-459-4.