MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Calculatoare, Informatică şi Microelectronică
Departamentul Ingineria Software și Automatică

Admis la susţinere
Şef departament:
FIODOROV Ion dr., conf.univ.
_____
„___” _____ 2026

ANALIZA ȘI DEZVOLTAREA COMPONENTELOR CLIENT ALE SISTEMULUI DE AUTENTIFICARE CU DOI FACTORI

Proiect de master

Student: _____ **Negrea Irina, TI-241M**

Coordonator: _____ **Ludmila Peca, lect. univ.**

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

Chişinău, 2026

REZUMAT

Lucrarea de față abordează problematica autentificării cu doi factori (2FA) în aplicațiile moderne, cu accent pe analiza, dezvoltarea și testarea componentelor client, precum și pe integrarea acestora într-un sistem sigur. Scopul principal al tezei este de a analiza teoriile și soluțiile existente, de a propune un model de sistem 2FA adaptat nevoilor actuale și de a demonstra aplicabilitatea practică a soluțiilor propuse.

În capitolul 1, „Fundamentarea teoretică a autentificării cu doi factori (2FA)", s-au prezentat noțiuni generale privind securitatea aplicațiilor și importanța protecției datelor utilizatorilor. Au fost analizate metodele și mecanismele de autentificare a utilizatorilor, incluzând parole, token-uri hardware, coduri unice și autentificare biometrică. De asemenea, s-au descris principiile autentificării multifactor, avantajele implementării 2FA și protocoalele și tehnologiile uzuale utilizate pentru aceasta, precum TOTP, HOTP, OAuth 2.0 și OpenID Connect. În final, s-au discutat avantajele și dezavantajele 2FA, subliniind necesitatea unei implementări corecte și adaptate contextului aplicației.

În capitolul 2, „Analiza soluțiilor existente și definirea cerințelor sistemului propus", s-au analizat sistemele de autentificare 2FA disponibile în prezent, evaluând funcționalitatea, securitatea și compatibilitatea acestora cu diferite tipuri de aplicații. Au fost identificate limitările și vulnerabilitățile principale, cum ar fi dependența de SMS, riscul de phishing sau integrarea dificilă în aplicațiile existente. Pe baza acestei analize, s-au stabilit cerințele funcționale și non-funcționale ale sistemului propus, incluzând criterii de securitate, performanță și experiență a utilizatorului. De asemenea, s-au evaluat tehnologiile și arhitectura necesare pentru implementarea unui sistem sigur și eficient.

În capitolul 3, „Analiza și proiectarea componentelor client pentru sistemul 2FA", s-au definit componentele principale ale clientului, propunând soluții originale pentru autentificarea adaptivă, generarea și validarea codurilor 2FA cu feedback vizual, precum și notificările inteligente și sugestiile în timp real. S-au proiectat interfețele și fluxurile de autentificare, incluzând tabele explicative și diagrame ilustrative care arată modul de interacțiune între module și integrarea cu backend-ul. În plus, s-au prezentat tehnologiile și instrumentele utilizate pentru dezvoltarea componentelor client, precum JavaScript și React.js, și s-au explicat motivele alegerii acestora, subliniind compatibilitatea, flexibilitatea și ușurința de integrare.

În capitolul 4, „Dezvoltarea și testarea componentelor client", s-au detaliat etapele de implementare a modulelor de autentificare, integrarea interfeței cu fluxurile funcționale, precum și testarea funcțională și de securitate a componentelor client. Au fost prezentate exemple de cod analizate și dezvoltate parțial, cu explicații despre modul de generare și validare a codurilor 2FA și feedback-ul oferit utilizatorului. S-a realizat o analiză a rezultatelor testelor pentru identificarea posibilităților de optimizare, iar concluziile subliniază valoarea practică a soluției și perspectivele implementării acesteia în medii reale. Această etapă demonstrează modul în care teoria și proiectarea sunt aplicate în practică pentru crearea unui sistem intuitiv, adică, lucrarea dată combină analiza teoretică cu propunerile și implementările practice.

ABSTRACT

This thesis addresses the issue of two-factor authentication (2FA) in modern applications, focusing on the analysis, development, and testing of client components, as well as their integration into a secure system. The main objective of the thesis is to analyze existing theories and solutions, propose a 2FA system model adapted to current needs, and demonstrate the practical applicability of the proposed solutions.

In chapter 1, "Theoretical Foundations of Two-Factor Authentication (2FA)," general concepts regarding application security and the importance of protecting user data are presented. The methods and mechanisms of user authentication, including passwords, hardware tokens, one-time codes, and biometric authentication, were analyzed. Furthermore, the principles of multi-factor authentication, the advantages of implementing 2FA, and the commonly used protocols and technologies, such as TOTP, HOTP, OAuth 2.0, and OpenID Connect, were described. Finally, the advantages and disadvantages of 2FA were discussed, emphasizing the need for correct implementation adapted to the application context.

In chapter 2, "Analysis of Existing Solutions and Definition of the Proposed System Requirements," current 2FA authentication systems were analyzed, evaluating their functionality, security, and compatibility with various types of applications. Key limitations and vulnerabilities were identified, such as SMS dependency, phishing risks, or difficult integration into existing applications. Based on this analysis, the functional and non-functional requirements of the proposed system were established, including security, performance, and user experience criteria. Additionally, the technologies and architecture necessary for implementing a secure and efficient system were assessed.

In chapter 3, "Analysis and Design of Client Components for the 2FA System," the main client components were defined, proposing original solutions for adaptive authentication, generation and validation of 2FA codes with visual feedback, and intelligent notifications with real-time suggestions. User interfaces and authentication flows were designed, including explanatory tables and illustrative diagrams showing the interaction between modules and integration with the backend. Moreover, the technologies and tools used for developing the client components, such as JavaScript and React.js, were presented, explaining the reasons for their selection, highlighting compatibility, flexibility, and ease of integration.

In chapter 4, "Development and Testing of Client Components," the stages of implementing authentication modules, integrating the interface with functional flows, and testing the functional and security aspects of the client components were detailed. Examples of partially developed and analyzed code were presented, with explanations on generating and validating 2FA codes and providing user feedback. An analysis of test results was conducted to identify optimization opportunities, and the conclusions emphasize the practical value of the solution and its implementation prospects in real environments. This phase clearly demonstrates how theoretical concepts and system design principles are applied in practice to create an intuitive and user-friendly system. In other words, this thesis effectively combines thorough theoretical analysis with concrete practical proposals and implementations.

CUPRINS

ABREVIERI ȘI DEFINIȚII

2FA – autentificare cu doi factori.

MFA – autentificare multi-factor.

Atacuri de tip phishing – tentative de fraudă prin care atacatorii încearcă să obțină informații confidențiale de la utilizatori, prin intermediul mesajelor sau site-urilor false.

Malware – software rău intenționat conceput să afecteze sau să compromită sistemele informatice.

Injecții SQL – tehnică de atac asupra bazelor de date prin inserarea de cod SQL malițios într-o interogare.

TOTP – Time-based One-Time Password, parolă unică generată pe baza timpului.

HOTP – HMAC-based One-Time Password, parolă unică generată pe baza unui contor.

OTP – One-Time Password, parolă utilizată o singură dată.

RFC 4226 – standard care definește algoritmul HOTP.

RFC 6238 – standard care definește algoritmul TOTP.

OAuth 2.0 – protocol de autorizare care permite aplicațiilor să obțină acces limitat la conturile utilizatorilor fără a solicita parola acestora.

Twilio Verify – serviciu API care permite trimiterea de coduri de autentificare prin SMS, voce sau aplicații mobile.

Firebase Authentication – platformă Google pentru autentificarea utilizatorilor în aplicații web și mobile.

FIDO2/WebAuthn – standarde pentru autentificare securizată, fără parolă, folosind chei publice și dispozitive hardware.

React.js – bibliotecă JavaScript pentru construirea interfețelor de utilizator interactive.

API-uri RESTful – interfețe de programare care respectă principiile arhitecturii REST pentru comunicarea între client și server.

GraphQL – limbaj de interogare pentru API-uri, care permite solicitarea exactă a datelor necesare.

HMAC-SHA1 – algoritm criptografic utilizat pentru verificarea integrității și autenticității datelor.

Elastic Stack (ELK) – set de instrumente pentru colectarea, stocarea, analizarea și vizualizarea datelor (Elasticsearch, Logstash, Kibana).

Redux – bibliotecă JavaScript pentru gestionarea stării aplicațiilor.

Axios – bibliotecă JavaScript pentru efectuarea cererilor HTTP din aplicații web.

GDPR – Regulamentul General privind Protecția Datelor, care stabilește reguli pentru colectarea și prelucrarea datelor cu caracter personal în UE.

Token-urile hardware – dispozitive fizice care generează coduri de autentificare unice pentru a asigura securitatea conturilor.

Brute force - este o metodă de atac informatic prin care un atacator încearcă sistematic și repetat toate combinațiile posibile de parole, coduri sau chei de autentificare până când obține acces neautorizat la un cont sau sistem.

INTRODUCERE

În ultimele decenii, odată cu dezvoltarea rapidă a tehnologiilor informaționale și creșterea utilizării internetului, securitatea datelor în mediul online a devenit un aspect esențial pentru protejarea informațiilor personale și a activităților desfășurate în aplicațiile. Atacurile cibernetice, furtul de identitate, phishing-ul și accesul neautorizat reprezintă amenințări constante pentru organizații și utilizatori individuali, generând pierderi financiare semnificative și afectând încrederea în serviciile digitale. În acest context, autentificarea utilizatorilor devine un element cheie în asigurarea securității aplicațiilor, fiind necesară implementarea unor mecanisme de protecție complexe și eficiente.

Autentificarea tradițională bazată doar pe parolă prezintă numeroase vulnerabilități, întrucât parolele pot fi ușor compromise prin atacuri de tip phishing, keylogging sau brute-force. În consecință, autentificarea cu doi factori (2FA) a apărut ca o soluție fiabilă, care adaugă un strat suplimentar de securitate. Aceasta presupune combinarea a două metode distincte de verificare a identității utilizatorului, cum ar fi un element pe care utilizatorul îl cunoaște (parolă, PIN), un element pe care îl deține (token hardware, aplicație mobilă de autentificare, cod SMS) sau un element biometric (amprentă, recunoaștere facială). Implementarea corectă a unui sistem 2FA reduce semnificativ riscul accesului neautorizat, chiar și în cazul compromiterii parolei, și contribuie la protejarea datelor sensibile.

Tema lucrării de față se concentrează pe analiza, proiectarea și dezvoltarea unui sistem de autentificare cu doi factori pentru aplicații, combinând analiza teoretică a conceptelor de securitate cu realizarea unui prototip practic. Lucrarea are scopul de a demonstra modul în care tehnologiile moderne pot fi utilizate pentru a crea un sistem sigur, scalabil și ușor de utilizat, care să respecte atât cerințele de securitate, cât și experiența optimă a utilizatorului. Sistemele de autentificare 2FA nu sunt doar o tendință tehnologică, ci o necesitate în contextul actual. Numeroase organizații internaționale, instituții financiare și platforme online au adoptat autentificarea multifactor pentru protejarea conturilor utilizatorilor și pentru prevenirea accesului neautorizat. În plus, reglementările privind protecția datelor cu caracter personal, cum ar fi GDPR în Uniunea Europeană, impun implementarea unor măsuri de securitate adecvate, iar autentificarea cu doi factori reprezintă o soluție corespunzătoare și recomandată.

Structura lucrării reflectă un parcurs logic de la fundamentarea teoretică până la implementarea practică a sistemului. Capitolul 1 prezintă aspectele teoretice privind securitatea aplicațiilor web și autentificarea utilizatorilor, subliniind principiile autentificării cu doi factori și avantajele acesteia. Capitolul 2 se axează pe analiza soluțiilor existente și definirea cerințelor sistemului, evidențiind limitele sistemelor curente și necesitățile specifice unui sistem eficient de autentificare 2FA. Capitolul 3 tratează proiectarea sistemului, incluzând arhitectura, fluxurile de date și modelarea componentelor, iar Capitolul 4 descrie procesul de implementare și testarea prototipului, analizând rezultatele obținute și eficiența soluției. Această lucrare contribuie la aprofundarea cunoștințelor în domeniul securității aplicațiilor web și oferă un exemplu concret de aplicare a autentificării cu doi factori.

BIBLIOGRAFIE

1. „Autentificare prin doi factori | ESET HOME”. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://help.eset.com/home_eset/ro-RO/two_factor_authentication.html
2. „What Is a Cyberattack? | IBM”. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://www.ibm.com/think/topics/cyber-attack
3. „Malware Attacks”, CyberArk. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://www.cyberark.com/what-is/malware/
4. „Autentificare prin doi factori | ESET Business Account”. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://help.eset.com/eba/ro-RO/two_factor_authentication.html
5. G. Constantin, „Autentificarea Multi-Factor (MFA) și Autentificarea cu Doi Factori (2FA) - Gelusi.RO - Consultanta IT”. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://www.gelusi.ro/consultanta-it/autentificarea-multi-factor-mfa-si-autentificarea-cu-doi-factori-2fa/
6. M. Shirvanian și S. Agrawal, „2D-2FA: A New Dimension in Two-Factor Authentication”, 29 octombrie 2021, *arXiv*: arXiv:2110.15872. doi: 10.48550/arXiv.2110.15872.
7. „Sistemul UE Login de autentificare cu factor unic sau cu doi factori: care este diferența și cum se poate modifica? - EURES (EURopean Employment Services)”. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://eures.europa.eu/eures-services/help-and-support/eu-login-single-or-two-factor-authentication-what-difference-and-how-change_ro
8. „STISC atenționează asupra importanței implementării Autentificării cu Doi Factori (2FA)”, Serviciul Tehnologia Informației și Securitate Cibernetică. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://stisc.gov.md/ro/comunicate-de-presa/stisc-atentioneaza-asupra-importantei-implementarii-autentificarii-cu-doi
9. „What is phishing? | Phishing attack prevention”. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://www.cloudflare.com/learning/access-management/phishing-attack/
10. C. Iosub, „Ghid: autentificarea în doi pași (2FA)”, CyberSkill - Educatie in Securitate Cibernetica. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://www.cyberskill.ro/ghid-autentificarea-doi-pasi-2fa/
11. „Ce este autentificarea pe două niveluri (2FA)? | Microsoft Security”. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://www.microsoft.com/ro-ro/security/business/security-101/what-is-two-factor-authentication-2fa
12. A. P. SRL, „Activarea autentificării securizate (cu doi factori) pe contul de client Hostico (Two Factor Authentication - 2FA)”, Hostico. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://hostico.ro/docs/activarea-autentificarii-securizate-cu-doi-factori-pe-contul-de-client-hostico-two-factor-authentication-2fa/
13. R. Nastase, „Atacuri Cibernetice: 5 Exemple de metode de Hacking”, RamonNastase.ro. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://ramonnastase.ro/blog/exemple-de-atacuri-cibernetice-metode-de-hacking-din-internet/
14. VirtualBoard, „Ce este Diagrama de Flux? - Caracteristici și simboluri”, VirtualBoard. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://virtualboard.ro/rezolvarea-problemelor/ce-este-diagrama-de-flux-caracteristici-si-simboluri/
15. Y. Sun, S. Zhu, Y. Zhao, și P. Sun, „Let Your Camera See for You: A Novel Two-Factor Authentication Method against Real-Time Phishing Attacks”, 1 septembrie 2021, *arXiv*: arXiv:2109.00132. doi: 10.48550/arXiv.2109.00132.
16. C. este autentificarea în doi pași? G. complet pentru securitatea multi-factor PostNext implementare și cele mai bune practici |., „Ce este autentificarea în doi pași? Ghid complet pentru securitatea multi-factor, implementare și cele mai bune practici”, PostNext. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://postnext.io/ro-ro/glossary/two-factor-authentication
17. „Ce Este un Atac Cibernetic? | Simulare Sigură & Legală”. Data accesării: 27 noiembrie 2025. [Online]. Disponibil la: https://www.cyberarena.ro/ce-este-un-atac-cibernetic/

18. „Blocking Brute Force Attacks | OWASP Foundation”. Data accesării: 22 decembrie 2025. [Online]. Disponibil la: https://owasp.org/www-community/controls/Blocking_Brute_Force_Attacks
19. L. Peca, S. Cojocaru, M. Dumitrașcu, and D. Țurcanu, “EVALUATION OF CYBERSECURITY TRAINING PERCEPTIONS, ADOPTED PRACTICES AND STRATEGIC DIRECTIONS FOR CAPACITY BUILDING”, *J. Eng. Sci.*, vol. 32, no. 3, pp. 75–90, Nov. 2025.
20. ISTRATI, Daniela. *Metode de optimizare și interfețe în organizarea sistemelor de producție*. 2023. PhD Thesis. Universitatea Tehnică a Moldovei. https://repository.utm.md/handle/5014/25886.
21. O. Mangos, V. Rachier, S. Cojocaru, G. Bunescu and C. Rusu, "Web Platform for Wind Potential Assessment in the Republic of Moldova," *2025 International Conference on Electromechanical and Energy Systems (SIELMEN)*, Iasi, Romania, 2025, pp. 308-313, doi: 10.1109/SIELMEN67352.2025.11260662.
22. COJOCARU, Svetlana, PECA, Ludmila. Challenges and solutions on the use of Artificial Intelligence in Internet of Things network security. In: *Electronics, Communications and Computing: IC ECCO 2024*, Ed. 13, 17-18 octombrie 2024, Chișinău. Chișinău: „Tehnica-UTM”, 2024, Editia 13, pp. 120-121. ISBN (pdf) 978-9975-64-480-8 (PDF).
23. BOLUN, Ion, COJOCARU, Svetlana. A Differentiated Beneficiary Cybersecurity Approach. In: *Electronics, Communications and Computing*, Ed. 12, 20-21 octombrie 2022, Chișinău. Chișinău: „Tehnica-UTM”, 2023, Editia 12, pp. 115-118. ISBN (pdf) 978-9975-45-898-6 (PDF).
24. BRANIȘTE, Rodica, ISTRATI, Daniela, GOGOI, Elena. La qualite de l’eau : metodes et modeles numerique de recherche. In: *Conferința tehnico-științifică a studenților, masteranzilor și doctoranzilor*, 29-31 martie 2022, Chișinău. Chișinău, Republica Moldova: „Tehnica-UTM”, 2022, Vol.1, pp. 432-436. ISBN 978-9975-45-828-3.. ISBN (pdf) 978-9975-45-829-0 (Vol. I) (PDF)..
25. DUCA, Ludmila, COJUHARI, Irina, CIORBĂ, Dumitru, COJOCARU, Svetlana. Limbaje formale și automate finite: Ghid pentru lecțiile practice. Universitatea Tehnică a Moldovei, Facultatea Calculatoare, Informatică și Microelectronică, Departamentul Ingineria Software și Automatică. Chișinău: Tehnica-UTM, 2024. 128 p. ISBN 978-9975-64-381-8.
26. PECA, Ludmila, TSURCANU, Dinu. Reducing cyber risk through a human–centred approach. In: *Journal of Engineering Science*, 2025, vol. 32, nr. 1, pp. 18-31. ISSN 2587-3474. DOI: https://doi.org/10.52326/jes.utm.2025.32(1).02
27. Țurcanu, D., Peca, L., Prisacaru, A., & Țurcanu, T. (2025). CYBER SECURITY PROFESSIONAL DEVELOPMENT WITHIN CYBERCOR. *JOURNAL OF ENGINEERING SCIENCE*, *32*(2), 87–98. https://doi.org/10.52326/jes.utm.2025.32(2).08
28. PECA, Ludmila, ȚURCANU, Dinu. Network security: Practical examples solved to be introduced in network security. [Practical Guide]. Fac. of Computers, Informatics and Microelectronics, Dep. Software Engineering and Automatics: Tehnica UTM, 2023, 243 p. ISBN 978-9975-45-941-9.
29. POȘTARU, ANDREI. Экспериментальный метод и программные средства для исследования динамического пове дения трибосистем скольжения. In: Электронная обработка материалов, 2024, vol. 60, nr. 2, pp. 74-86. ISSN 0013-5739. DOI: https://doi.org/10.52577/eom.2024.60.2.74 https://ibn.idsi.md/ro/vizualizare_articol/206975
30. M. Chiper, D. Stanescu, T. Becheru and L. Peca, "Adversarial Attacks for Scripts," *2025 24th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Chisinau, Moldova, Republic of, 2025, pp. 1-7, doi: 10.1109/RoEduNet68395.2025.11208410.
31. ISTRATI, Daniela. Influența factorilor fundamentali în sistemele de producție. In: *Conferința tehnico-științifică a studenților, masteranzilor și doctoranzilor*, 29-31 martie 2022, Chișinău. Chișinău, Republica Moldova: „Tehnica-UTM”, 2022, Vol.1, pp. 442-445. ISBN 978-9975-45-828-3.. ISBN (pdf) 978-9975-45-829-0 (Vol. I) (PDF).

32. Leahu, A., Andrievschi-Bagrin, V., Ciorbă, D., Fiodorov, I. (2025). On Dynamic Probabilistic Models in Network Reliability. In: Hoskova-Mayerova, S., Flaut, C., Flaut, D., Rackova, P. (eds) Changes and Innovations in Social Systems. Studies in Systems, Decision and Control, vol 505. Springer, Cham. https://doi.org/10.1007/978-3-031-43506-5_5
33. POŞTARU, GHEORGHE; STOICEV, PETRU; POŞTARU, ANDREI; BODNARIUC, ION; BUGA, ALEXANDRU; PLATON, ANDREI. Determination of the tribotechnical characteristics of the materials used for precessional transmissions design. In: Acta Technica Napocensis - Series: Applied Mathematics, Mechanics, and Engineering, 2024, vol. 67, supl. nr. 2, pp. 577-584. ISSN 1221-5872.
34. S. -F. Ion, C. Carabas, N. Ţăpuş and D. Ciorbă, "Enhancing Blockchain Performance via Unikraft: A Case Study of Implementation and Scalability Analysis on MultiversX," *2024 23rd RoEduNet Conference: Networking in Education and Research (RoEduNet)*, Bucharest, Romania, 2024, pp. 1-8, doi: 10.1109/RoEduNet64292.2024.10722595.
35. ISTRATI, Daniela, CALMÎCOV, Igor, MORARU, Vasile, ZAPOROJAN, Sergiu. Interfaces dans l'organisation des systemes de production. In: *Intellectus*, 2023, nr. 2, pp. 145-154. ISSN 1810-7079. DOI: https://doi.org/10.56329/1810-7087.23.2.16
36. L. Alexei, R. Maria, D. Ciorbă and F. Ion, "Geometric distributions MinMax and MaxMin modified as lifetime distributions and statistical estimators for them," *2025 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom)*, Chisinau, Moldova, Republic of, 2025, pp. 1-5, doi: 10.1109/BlackSeaCom65655.2025.11193904.
37. PLĂMĂDEALĂ, Maxim, BALAMATIUC, Eduard, NEGAI, Marin, FIŞTIC, Cristofor, CIORBĂ, Dumitru. Enhancing machine learning model performance through data augmentation techniques across varied dataset sizes. In: *Conferinţa tehnico-ştiinţifică a studenţilor, masteranzilor şi doctoranzilor*, 27-29 martie 2024, Chișinău. Chișinău, Republica Moldova: „Tehnica-UTM", 2024, Vol.2, pp. 855-860. ISBN 978 9975-64-460-0. ISBN (pdf) 978-9975-64-458-7 (Vol.2).
38. DUCA, Ludmila, ZAPOROJAN, Sergiu, ISTRATI, Daniela, MUNTEAN, Nicolae. Effectiveness of Artificial Intelligence Integration in ERP Systems for Fitness Centers. In: *Electronics, Communications and Computing: IC ECCO 2024*, Ed. 13, 17-18 octombrie 2024, Chişinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 188-189. ISBN (pdf) 978-9975-64-480-8 (PDF).
39. ALEXEI, Arina. SYSTEMIC SECURITY FRAMEWORK FOR HEI'S. In: Scientific and Practical Cyber Security Journal (SPCSJ), Vol 8(2), 2024, pp. 59–67. ISSN 2587-4667.
40. Arina, Alexei, Ion Bolun, and Anatolie Alexei. "Cybersecurity challenges in healthcare: mitigating risks in a rapidly evolving digital landscape." Bulletin of Electrical Engineering and Informatics 14.6 (2025): 4867-4875.
41. BOLUN, I, ALEXEI, A. Aspecte de securizare a rețelelor și sistemelor informatice biomedicale. In: ECONOMICA, vol.4, numărul 160, 2024, pag.60-75. DOI: 10.53486/econ.2024.130.060.
42. Alexei, A., Moraru, V., & Alexei, A. (2025). SECURING MOLDOVAN SMALL AND MEDIUM-SIZED BUSINESSES: STRATEGIES BASED ON IT INFRASTRUCTURE DOMAINS. In: JOURNAL OF ENGINEERING SCIENCE, 32(2), 75–86. https://doi.org/10.52326/jes.utm.2025.32(2).07.
43. ISTRATI, Daniela. Temperature capture and image processing system: a case study .... In: *Journal of Engineering Science*, 2022, vol. 29, nr. 2, pp. 108-115. ISSN 2587-3474. DOI: https://doi.org/10.52326/jes.utm.2022.29(2).10
44. ALEXEI, A., PLATON, N., BOLUN, I., ALEXEI, An. Smart and digital healthcare. Advanced technologies and security issues. In: CEEeGov: Central and Eastern European eDem and eGov Days, Budapest, Hungary, September 2024. ACM, New York, NY, USA, 7 Pages. DOI: https://doi.org/10.1145/3670243.3673857.
45. Alexei, A., Alexei, A. (2025). Towards More Protected Medical Data: Assessing the Security of Web and Email Infrastructures in SMEs in the Republic of Moldova. In: Sontea, V., Tiginyanu, I., Railean, S. (eds) 7th International Conference on Nanotechnologies and Biomedical Engineering.

ICNBME 2025. IFMBE Proceedings, vol 135. Springer, Cham. https://doi.org/10.1007/978-3-032-06497-4_31.
46. POȘTARU, ANDREI. Experimental Method and Software Instruments for Sliding Tribosystem Dynamic Behavior Research. In: Surface Engineering and Applied Electrochemistry. 2024, vol. 60, Issue 5, pp 706-716, ISSN: 1068-3755 DOI: https://doi.org/10.3103/S1068375524700297
47. BOSTAN, ION; STOICEV, PETRU; POȘTARU, GHEORGHE; BUGA, ALEXANDRU; BODNARIUC, ION; POȘTARU, ANDREI; PLATON, ANDREI. Particularities of tribological behavior of the contact elements of the precessional gear, made of metallic and plastic materials. In: International Journal of Modern Manufacturing Technologies, 2023, vol. 15, pp. 16-27. ISSN 2067-3604. DOI: https://doi.org/10.54684/ijmmt.2023.15.3.16 https://ibn.idsi.md/ro/vizualizare_articol/194562
48. ISTRATI, Daniela, CALMÎCOV, Igor, MORARU, Vasile, ZAPOROJAN, Sergiu. Development of an Employee Scheduling Application Under Consecutive Days-off Constraints. In: *Electronics, Communications and Computing: IC ECCO 2024*, Ed. 13, 17-18 octombrie 2024, Chișinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 178-179. ISBN (pdf) 978-9975-64-480-8 (PDF).
49. DUCA, Ludmila, ZAPOROJAN, Sergiu, ISTRATI, Daniela. ERP system implementation in companies. In: *Electronics, Communications and Computing: IC ECCO 2024*, Ed. 13, 17-18 octombrie 2024, Chișinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 169-170. ISBN (pdf) 978-9975-64-480-8 (PDF).
50. ISTRATI, Daniela. A Brief Overview of Intelligent Interfaces in Production Systems. In: *Electronics, Communications and Computing*, Ed. 12, 20-21 octombrie 2022, Chișinău. Chișinău: „Tehnica-UTM", 2023, Editia 12, pp. 158-161. ISBN (pdf) 978-9975-45-898-6 (PDF).