MINISTRY OF EDUCATION AND RESEARCH OF THE REPUBLIC OF MOLDOVA

Technical University of Moldova

Faculty of Computers, Informatics, and Microelectronics

Department of Software Engineering and Automation

Approved for defense
Department head:
Ion FIODOROV, phd, associate professor

„___" _____ 2026

Security Implications of API Gateway Patterns in Distributed Systems

Master's Project

Student: _____ **Moisei Liviu, SI-241M**

Coordinator: _____ **Țurcanu Dinu, Conf. Univ. Dr.**

Consultant: _____ **Cojocaru Svetlana, university assistant**

Chisinau, 2026

REZUMAT

Această lucrare prezintă o metodologie comprehensivă de evaluare a securității gateway-urilor API pentru microservicii, concentrându-se pe modelele de integrare în arhitecturi distribuite. Cercetarea abordează provocarea critică a securizării implementărilor de gateway-uri API care servesc drept punct principal de intrare pentru sistemele bazate pe microservicii.

Studiul dezvoltă un cadru sistematic de evaluare care combină analiza modelelor arhitecturale, modelarea amenințărilor utilizând metodologia STRIDE și evaluarea controalelor de securitate bazată pe ghidurile OWASP. O analiză comparativă a framework-urilor proeminente, inclusiv Spring Cloud Gateway, Kong Gateway și Google Apigee, identifică caracteristicile cheie de securitate în ceea ce privește autentificarea, autorizarea, limitarea ratei și mecanismele de protecție a datelor.

Metodologia introduce o abordare bazată pe modele care categorizează implementările de gateway în trei modele arhitecturale principale: Gateway simplu, Backend for Frontend (BFF) și Gateway aggregation. Fiecare model este analizat în raport cu proprietățile inerente de securitate, suprafețele de vulnerabilitate și strategiile de atenuare. Cadrul oferă criterii de suport decizional pentru selectarea modelelor în funcție de cerințele organizaționale de securitate, complexitatea operațională și considerentele de scalabilitate.

Validarea practică demonstrează eficacitatea metodologiei prin studii de caz reale, dezvăluind lacune critice de securitate în implementările comune și furnizând recomandări acționabile pentru îmbunătățirea securității. Cercetarea contribuie atât la fundamentarea teoretică, prin caracteristici formalizate ale modelelor, cât și la instrumente practice, inclusiv matrice de evaluare a amenințărilor, liste de verificare a configurațiilor și cadre de metrici de securitate.

Rezultatele indică faptul că proiectarea securității conștientă de modele îmbunătățește semnificativ postura de securitate a arhitecturilor de microservicii, menținând în același timp eficiența operațională. Metodologia propusă permite organizațiilor să ia decizii arhitecturale informate care echilibrează cerințele de securitate cu obiectivele funcționale și de performanță.

Cuvinte-cheie: Gateway API, securitatea microserviciilor, modele de integrare, modelarea amenințărilor, STRIDE, evaluarea securității.

ABSTRACT

This thesis presents a comprehensive security assessment methodology for microservices API gateways, focusing on integration patterns in distributed architectures. The research addresses the critical challenge of securing API gateway implementations that serve as the primary entry point for microservices-based systems.

The study develops a systematic evaluation framework that combines architectural pattern analysis, threat modeling using STRIDE methodology, and security control assessment based on OWASP guidelines. A comparative analysis of prominent frameworks including Spring Cloud Gateway, Kong Gateway, and Google Apigee identifies key security characteristics across authentication, authorization, rate limiting, and data protection mechanisms.

The methodology introduces a pattern-based approach that categorizes gateway implementations into three primary architectural patterns: Simple Gateway, Backend for Frontend (BFF), and Gateway Aggregation. Each pattern is analyzed for inherent security properties, vulnerability surfaces, and mitigation strategies. The framework provides decision support criteria for pattern selection based on organizational security requirements, operational complexity, and scalability considerations.

Practical validation demonstrates the methodology's effectiveness through real-world case studies, revealing critical security gaps in common implementations and providing actionable recommendations for security enhancement. The research contributes both theoretical foundations through formalized pattern characteristics and practical tools including threat assessment matrices, configuration checklists, and security metric frameworks.

Results indicate that pattern-aware security design significantly improves the security posture of microservices architectures while maintaining operational efficiency. The proposed methodology enables organizations to make informed architectural decisions that balance security requirements with functional and performance objectives.

Keywords: API Gateway, Microservices Security, Integration Patterns, Threat Modeling, STRIDE, Security Assessment

CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS AND DEFINITIONS

- **ABAC** – Attribute-Based Access Control;
- **API** – Application Programming Interface;
- **BFF** – Backend for Frontend;
- **DDD** – Domain-Driven Design;
- **DoS** – Denial of Service;
- **HTTP** – HyperText Transfer Protocol;
- **HTTPS** – HyperText Transfer Protocol Secure;
- **JSON** – JavaScript Object Notation;
- **JWE** – JSON Web Encryption;
- **JWS** – JSON Web Signature;
- **JWT** – JSON Web Token;
- **mTLS** – Mutual Transport Layer Security;
- **NIST** – National Institute of Standards and Technology;
- **OAuth** – Open Authorization;
- **OWASP** – Open Web Application Security Project;
- **PKCE** – Proof Key for Code Exchange;
- **RBAC** – Role-Based Access Control;
- **REST** – Representational State Transfer;
- **STRIDE** – Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege;
- **TLS** – Transport Layer Security.

INTRODUCTION

The shift from monolithic to microservices-based architectures has fundamentally transformed how distributed systems are designed and operated. API gateways have emerged as critical infrastructure components, serving as the primary entry point mediating access between external clients and internal microservices. Recent surveys indicate that the majority of organizations implementing microservices architectures deploy API gateway patterns to manage cross-cutting concerns including authentication, authorization, rate limiting, and request routing [1, 2].

However, API gateways occupy a security-critical position in distributed system architectures. As centralized entry points processing all external traffic, they concentrate both security enforcement capabilities and security risks. A single vulnerability in gateway configuration or implementation can compromise entire backend infrastructures, potentially exposing sensitive data across multiple services or enabling unauthorized access to protected resources. The security implications of API gateway deployments extend beyond individual vulnerability instances to encompass architectural characteristics that fundamentally influence threat landscapes and attack surfaces.

Organizations implementing API gateways face three primary patterns documented in microservices literature: Gateway Routing (simple request forwarding), Gateway Aggregation (response composition from multiple services), and Backend for Frontend (client-specific gateway instances) [1, 2]. While extensive literature addresses functional characteristics, performance trade-offs, and operational considerations of these patterns, systematic approaches to security assessment remain underdeveloped. Existing security guidance tends toward generic API security best practices without addressing how architectural characteristics inherent to gateway patterns influence security posture.

Beyond pattern selection, organizations must make numerous implementation-level decisions affecting gateway security: authorization architecture choices (gateway-only, defense-in-depth, or backend-only), backend communication security mechanisms (HTTP, HTTPS, or mutual TLS), response data handling approaches (pass-through, filtered, or composed), and rate limiting strategies (IP-based, user-based, or absent). These decisions interact with pattern-level architectural characteristics to determine the overall security posture of gateway deployments.

Current practice often treats security assessment in ad-hoc manner, evaluating individual security controls without systematic methodology for identifying which threats are relevant to specific gateway configurations or how architectural and implementation choices influence vulnerability to different attack types. This gap between architectural decision-making and security assessment motivates the development of systematic, characteristic-based security evaluation approaches.

The fundamental problem addressed by this research is the absence of systematic methodologies for assessing API gateway security based on architectural and implementation characteristics. Organizations select gateway patterns and make configuration decisions without adequate frameworks for understanding security implications, leading to deployments that may be vulnerable to threats not adequately considered during design.

This research addresses the following primary research questions:

BIBLIOGRAPHY

[1] S. Newman, *Building Microservices: Designing Fine-Grained Systems*, 2nd ed. O'Reilly Media, 2021.

[2] C. Richardson, *Microservices Patterns: With Examples in Java*. Manning Publications, 2018.

[3] A. S. Tanenbaum and M. van Steen, *Distributed Systems: Principles and Paradigms*, 3rd ed. Pearson, 2017.

[4] K. Indrasiri and P. Siriwardena, *Design Patterns for Cloud Native Applications: Patterns in Practice Using APIs, Data, Events, and Streams*. O'Reilly Media, 2021.

[5] N. Madden, *API Security in Action*. Manning Publications, 2020.

[6] J. Richer and A. Sanso, *OAuth 2 in Action*. Manning Publications, 2017.

[7] A. Shostack, *Threat Modeling: Designing for Security*. Wiley, 2014.

[8] C. Contas¸el, R. Rughinis¸, D. C. Trancă, and D. T¸urcanu, "Enhancing e-health cybersecurity and resilience: Shifting from monolithic to microservices architecture," *U.P.B. Scientific Bulletin, Series C*, vol. 87, no. 1, 2025. [Online]. Available: https://www.scientificbulletin.pub.ro/rev_docs_arhiva/rez142_992799.pdf

[9] E. Evans, *Domain-Driven Design: Tackling Complexity in the Heart of Software*. Addison-Wesley, 2003.

[10] M. T. Nygard, *Release It!: Design and Deploy Production-Ready Software*, 2nd ed. Pragmatic Bookshelf, 2018.

[11] M. Fowler, *Patterns of Enterprise Application Architecture*. Addison-Wesley, 2002.

[12] J. Geewax, *API Design Patterns*. Manning Publications, 2021.

[13] B. Beyer, C. Jones, J. Petoff, H. Adkins, P. Blankinship, P. Lewandowski, and A. Oprea, *Building Secure and Reliable Systems: Best Practices for Designing, Implementing, and Maintaining Systems*. O'Reilly Media, 2020.

[14] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, NIST Special Publication 800-207, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

[15] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," IETF, RFC 7519, 2015. [Online]. Available: https://tools.ietf.org/html/rfc7519

[16] D. Hardt, "The OAuth 2.0 Authorization Framework," IETF, RFC 6749, 2012. [Online]. Available: https://tools.ietf.org/html/rfc6749

[17] E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.3," IETF, RFC 8446, 2018. [Online]. Available: https://tools.ietf.org/html/rfc8446

[18] D. F. Ferraiolo, R. Sandhu, S. Gavrila, D. R. Kuhn, and R. Chandramouli, "Proposed nist standard for role-based access control," *ACM Transactions on Information and System Security (TISSEC)*, vol. 4, no. 3, pp. 224–274, 2001.

[19] V. C. Hu, D. Ferraiolo, R. Kuhn, A. R. Friedman, A. J. Lang, M. M. Cogdell, A. Schnitzer, K. Sandlin, R. Miller, and K. Scarfone, "Guide to Attribute Based Access Control (ABAC) Definition and Considerations," National Institute of Standards and Technology, NIST Special Publication 800-162, 2014. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-162.pdf

[20] P. Siriwardena and N. Dias, *Microservices Security in Action*. Manning Publications, 2020.

[21] M. J. Hossain, M. R. Arefin, K. M. Alam, and S. Ahmed, "Security analysis of microservices architecture through api gateway," in *Proceedings of the 2021 International Conference on Information and Communication Technology for Sustainable Development (ICICT4SD)*. IEEE, 2021, pp. 373–377.

[22] OWASP Foundation, "OWASP API Security Top 10 - 2023," 2023, accessed: 2024-11-05. [Online]. Available: https://owasp.org/API-Security/editions/2023/en/0x11-t10/

[23] ——, "Application Security Verification Standard (ASVS) Version 4.0.3," OWASP Foundation, Tech. Rep., 2021. [Online]. Available: https://owasp.org/www-project-application-security-verification-standard/

[24] D. Winograd, K. Scarfone, and A. Singhal, "Guide to Secure Web Services," National Institute of Standards and Technology, NIST Special Publication 800-95, 2007. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-95.pdf

[25] T. Yarygina and A. H. Bagge, "Overcoming security challenges in microservice architectures," in *2018*

IEEE Symposium on Service-Oriented System Engineering (SOSE). IEEE, 2018, pp. 11–20.
[26] Joint Task Force, "Security and Privacy Controls for Information Systems and Organizations," National Institute of Standards and Technology, NIST Special Publication 800-53, Revision 5, 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[27] M. Jones, A. Nadalin, B. Campbell, J. Bradley, and C. Mortimore, "OAuth 2.0 Token Exchange," IETF, RFC 8693, 2020. [Online]. Available: https://tools.ietf.org/html/rfc8693
[28] K. Scarfone, M. Souppaya, and P. Hoffman, "Guide to General Server Security," National Institute of Standards and Technology, NIST Special Publication 800-123, 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf
[29] N. Dragoni, S. Giallorenzo, A. L. Lafuente, M. Mazzara, F. Montesi, R. Mustafin, and L. Safina, "Microservices: Yesterday, today, and tomorrow," in *Present and Ulterior Software Engineering*. Springer, 2017, pp. 195–216.
[30] P. A. Grassi, J. L. Fenton, E. M. Newton, R. A. Perlner, A. R. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker, Y.-Y. Choong, K. K. Greene, and M. F. Theofanos, "Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology, NIST Special Publication 800-63B, 2017. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf
[31] L. Peca, S. Cojocaru, M. Dumitraşcu, and D. Ţurcanu, "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.
[32] 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.
[33] 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, Chişinău. Chişinău: „Tehnica-UTM", 2024, Editia 13, pp. 120-121. ISBN (pdf) 978-9975-64-480-8 (PDF).
[34] BOLUN, Ion, COJOCARU, Svetlana. A Differentiated Beneficiary Cybersecurity Approach. In: *Electronics, Communications and Computing*, Ed. 12, 20-21 octombrie 2022, Chişinău. Chișinău: „Tehnica-UTM", 2023, Editia 12, pp. 115-118. ISBN (pdf) 978-9975-45-898-6 (PDF).
[35] DUCA, Ludmila, COJUHARI, Irina, CIORBĂ, Dumitru, COJOCARU, Svetlana. Limbaje formale şi automate finite: Ghid pentru lecţiile practice. Universitatea Tehnică a Moldovei, Facultatea Calculatoare, Informatică şi Microelectronică, Departamentul Ingineria Software şi Automatică. Chişinău: Tehnica-UTM, 2024. 128 p. ISBN 978-9975-64-381-8.
[36] 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
[37] Ţurcanu, D., Peca, L., Prisacaru, A., & Ţurcanu, 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
[38] PECA, Ludmila, ŢURCANU, 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.
[39] 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.
[40] 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
[41] 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.

[42] 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.

[43] PLĂMĂDEALĂ, Maxim, BALAMATIUC, Eduard, NEGAI, Marin, FIȘTIC, 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).

[44] 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, Chișinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 188-189. ISBN (pdf) 978-9975-64-480-8 (PDF).

[45] 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.

[46] 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.

[47] 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.

[48] 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.

[49] 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.

[50] 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.

[51] 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

[52] POȘTARU, GHEORGHE; STOICEV, PETRU; POȘTARU, 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.

[53] 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

[54] POȘTARU, ANDREI. Экспериментальный метод и программные средства для исследования динамического поведе ния 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

[55] ISTRATI, Daniela. *Metode de optimizare şi interfețe în organizarea sistemelor de producție*. 2023. PhD Thesis. Universitatea Tehnică a Moldovei. https://repository.utm.md/handle/5014/25886.

[56] 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, Chişinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 178-179. ISBN (pdf) 978-9975-64-480-8 (PDF).

[57] 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, Chişinău. Chișinău: „Tehnica-UTM", 2024, Editia 13, pp. 169-170. ISBN (pdf) 978-9975-64-480-8 (PDF).

[58] ISTRATI, Daniela. A Brief Overview of Intelligent Interfaces in Production Systems. In: *Electronics, Communications and Computing*, Ed. 12, 20-21 octombrie 2022, Chişinău. Chișinău: „Tehnica-UTM", 2023, Editia 12, pp. 158-161. ISBN (pdf) 978-9975-45-898-6 (PDF).

[59] 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

[60] ISTRATI, Daniela. Influența factorilor fundamentali în sistemele de producție. In: *Conferința tehnico-ştiinţifică a studenţilor, masteranzilor şi doctoranzilor*, 29-31 martie 2022, Chişinău. 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).

[61] BRANIȘTE, Rodica, ISTRATI, Daniela, GOGOI, Elena. La qualite de l'eau : metodes et modeles numerique de recherche. In: *Conferința tehnico-ştiinţifică a studenţilor, masteranzilor şi doctoranzilor*, 29-31 martie 2022, Chişinău. 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)..

[62] 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