ASEM
Academia de Studii Economice din Moldova

TEORIE &POLITICI ECONOMICE ASEM

PROCEEDINGS

of International Conference

ECONOMIC SECURITY

in the context of systemic transformations

3rd EDITION

CHIȘINĂU, 2024

Academy of Economic Studies of Moldova

Department of Economic Theory and Policy

PROCEEDINGS

of International Conference,
3rd Edition, December 07-08, 2023, Chișinău, Moldova

”ECONOMIC SECURITY IN THE CONTEXT OF SYSTEMIC TRANSFORMATIONS”

Chișinău, 2024

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chişinău, Moldova

CZU: 082=135.1=111=161.1

E 15

DESCRIEREA CIP A CAMEREI NAŢIONALE A CĂRŢII DIN REPUBLICA MOLDOVA

"Economic Security in the Context of Systemic Transformations", international conference (3 ; 2023 ; Chişinău). Proceedings of International Conference "Economic Security in the Context of Systemic Transformations", 3rd Edition, December 7-8 2023, Chişinău / drafting committee: Tatiana Bucos [et al.]. – Chişinău : SEP ASEM, 2024. – 271 p. : fig., tab.

Cerinţe de sistem: PDF Reader.

Antetit.: Academy of Economic Studies of Moldova, Department of Economic Theory and Policy. – Texte : lb. rom., engl., rusă. – Rez.: lb. engl. – Referinţe bibliogr. la sfârşitul art.

ISBN 978-9975-167-43-7 (PDF).

082=135.1=111=161.1

E 15

ISBN 978-9975-167-43-7 (PDF).

DOI: https://doi.org/10.53486/escst2023

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chișinău, Moldova

Proceedings of Scientific Articles Presented at the International Conference on 'Economic Security in the Context of Systemic Transformations', 3rd Edition (December 07-08, 2023)

DRAFTING COMMITTEE

**The editors are not responsible for the content of published scientific papers or for the opinions of the authors presented in this collection of articles.*

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chișinău, Moldova

CONTENTS:

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chișinău, Moldova

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chişinău, Moldova

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chișinău, Moldova

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chişinău, Moldova

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

IMPACTUL PLATFORMIZĂRII ECONOMIEI ASUPRA „EXODULUI DE CREIERE”

THE IMPACT OF ECONOMY PLATFORMIZATION ON THE PHENOMENON OF 'BRAIN DRAIN'

Tatiana BUCOS

PhD, Associate professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0001-6448-6001
E-mail:bucos.tatiana@ase.md

Abstract: *This article delves into the impact of the economy's platformization on the 'virtual brain drain' within the Industry 4.0 revolution. It explores the transformation of economic and business systems through digital platforms, transitioning from traditional brain drain to a virtual one. The study highlights the role of these platforms in transforming data management, reshaping economic sectors, and influencing consumer behavior. The paper examines the evolution of remote work from a pre-internet niche to widespread adoption, particularly accelerated by the COVID-19 pandemic. It discusses the critical role of online platforms in structuring remote work, including communication, project management, and data security.*
At its core, the research focuses on the 'virtual brain drain', where skilled professionals work remotely for international companies without emigrating, particularly prevalent in IT, programming, and digital marketing. This differs from traditional brain drain due to its virtual nature. The article addresses the challenges of remote work, such as cultural and legal differences, time zone challenges, and data security. It notes the adaptation of human resource management strategies, emphasizing collaborative technology and virtual recruitment. In conclusion, the paper reflects on the labor market's significant changes due to the virtual brain drain, altering talent attraction, retention, and management in a digitized, global work environment, providing insights into the evolving workforce dynamics in a platform-dominated economy.

Keywords: *platform economy, virtual brain drain, digitalization, remote work.*

UDC: *004.77:334.72*

JEL Classification: *J21, O33, M12, F22.*

INTRODUCERE

În contextul actual, marcat de o accelerare fără precedent a digitalizării și platformizării economice, asistăm la o transformare radicală a modalităților tradiționale de muncă. Aceast articol își propune să exploreze impactul pe care platformizarea economiei îl are asupra fenomenului de exod al creierelor, un aspect deosebit de relevant în era post-pandemie COVID-19. Pandemia a catalizat o schimbare majoră în percepția și adopția muncii la distanță, făcând-o nu doar o necesitate temporară, ci o componentă permanentă a peisajului muncii globale. Prin urmare, acest studiu se concentrează asupra modului în care platformele digitale, care facilitează munca la distanță, au contribuit la emergența unui nou tip de migrație profesională: exodul de creiere virtual.

Articolul are drept scop analiza impactul platformelor digitale asupra economiei, în special asupra pietei muncii, o atenție deosebită fiind dedicată fenomenului 'exodului de creiere'. Obiectivele includ înțelegerea dinamicii acestei migrații virtuale de talente și implicațiile sale pentru piața globală a muncii, precum și identificarea provocărilor și oportunităților pe care le prezintă atât pentru indivizi cât și pentru organizații.

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

IMPACTUL PLATFORMELOR ASUPRA ECONOMIEI

Termenul de platformizare a economiei este unul recent aparut în limbajul științific, dar care atrage atenția a tot mai mulți cercetători, grație impactului pe care îl au platformele digitale asupra proceselor economice și sociale. După cum menționează Kenney&Zysman (2016), platformele digitale generează transformări profunde sistemului economic prin modul în care facilitează interacțiunile între diferiți subiecți economici, modul în care aceștia lucrează și crează valoare [1]. Pe lângă modificările profunde la nivel de sistem, platformele digitale provoacă schimbări esențiale în lumea afacerilor, Choudary (2015) menționând că modelele de afaceri bazate pe platforme schimbă paradigma tradițională de business, permițând crearea de valoare prin gestiunea rețelelor și ecosistemelor [2]. În același context, în raportul Deloite, ”The rise of the platform economy”, publicat în anul 2019, se menționează că „lumea trece printr-o nouă revoluție economică, perturbând economia, afacerile, piețele muncii și viața noastră de zi cu zi într-un mod neîntâlnit de la revoluția industrială... în centrul aflându-se ascensiunea economiei bazate pe platforme.”[3].

Revoluția menționată în raportul Deloite, cunoscută și sub denumirea „Industria 4.0” schimbă esențial lumea afacerilor, ca urmare a transformărilor legate de:

- *digitalizarea și automatizarea avansată:* utilizarea tehnologiilor digitale, cum ar fi inteligența artificială (IA), big data și analiza de date, pentru a automatiza și optimiza procesele industriale și de afaceri;
- *conectivitatea extinsă:* conectarea dispozitivelor și echipamentelor din industrie la internet (IoT) permite comunicare între ele, respectiv, monitorizarea în timp real, analiza datelor și luarea deciziilor bazate pe date pentru a optimiza operațiunile;
- *personalizarea masivă:* capacitatea de a produce bunuri personalizate în masă, adaptate nevoilor individuale ale clienților, fără a crește semnificativ costurile;
- *colaborarea om-mașină:* integrarea resursei umane cu tehnologiile pentru a îmbunătăți calitatea și eficiența muncii.

Poziționarea platformelor digitale în centrul revoluției industriale 4.0, este determinată de rolul crucial ce revine platformelor în partajarea accesului la tehnologiile esențiale care fac posibile schimbările menționate mai sus (vezi tabelul 1).

Tabelul 1. Contribuția platformelor digitale la schimbările caracteristice revoluției industriale 4.0.

Schimbare Caracteristică Industriei 4.0	Exemplu de platforme digitale	Anul lansării / Utilizatori	Servicii oferite
Digitalizarea și Automatizarea Avansată	IBM Watson	Lansat în 2013. Peste 30.000 de clienți.	Furnizează servicii de inteligență artificială și analiză de date pentru optimizarea proceselor industriale.
Conectivitate Extinsă	Siemens MindSphere	Lansat în 2016. Peste 1,7 milioane de dispozitive conectate.	Permite conectarea echipamentelor industriale pentru monitorizarea și optimizarea performanței.
Personalizare Masivă	Amazon Web Services (AWS)	Lansat în 2006; Peste 2,3 milioane de clienți.	Oferă servicii de cloud computing și analiză de date pentru colectarea și analiza datelor.
Colaborarea Om-Mașină	Microsoft Azure	Lansat în 2010; Peste 722 milioane clienți.	Furnizează instrumente și servicii pentru dezvoltarea de aplicații AI.

Sursă: Elaborat de autor

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

Platformele furnizează infrastructura și instrumentele necesare pentru digitalizare, conectivitate extinsă, personalizare masivă și colaborare om-mașină, permițând astfel companiilor să adopte cu succes inovații tehnologice și să îmbunătățească semnificativ procesele lor de producție și operațiunile generale.

Prin facilitarea accesului la tehnologii avansate, platformele permit afacerilor realizarea cu cheltuieli reduse diverse sarcini de business. În acest scop, afacerile pot apela la o divesitate mare de platfrome digitale ce permit realizarea unor sarcini concrete (vezi tabelul 2).

Tabelul 2. Unele tipuri de platforme digitale

Tipuri de platforme digitale	Exemple de platforme	Operațiuni de afaceri posibile
Platforme de comerț electronic	Amazon, eBay, Shopify	Vânzare și achiziție de produse online.
Platforme de freelancing	Upwork, Freelancer, Fiverr	Angajarea de profesioniști pentru proiecte.
Platforme de socializare	Facebook, Instagram, LinkedIn	Marketing, gestionarea relațiilor cu clienții.
Platforme de analiză de date	Tableau, Google Analytics, Power BI	Analiză și înțelegere a datelor de afaceri.
Platforme de management al proiectelor	Trello, Asana, Jira, GitHub, GitLab	Gestionarea proiectelor și colaborarea echipelor.
Platforme de cloud computing	Amazon Web Services (AWS), Microsoft Azure	Stocarea datelor și dezvoltarea de aplicații.
Platforme de învățare online	Coursera, Udemy, edX	Livrarea de cursuri și formare la distanță.
Platforme de procesare a plăților	PayPal, Stripe, Square	Procesarea plăților online și gestionarea financiară.
Platforme de dezvoltare de software	GitHub, GitLab, Bitbucket	Dezvoltarea colaborativă a software-ului.
Platforme de marketing digital	Google Ads, Facebook Business Manager, HubSpot	Gestionarea campaniilor de marketing online.
Platforme de analiză financiară	QuickBooks, Xero, Zoho Books	Gestionarea financiară a afacerilor, inclusiv contabilitatea și raportarea financiară.

Sursă: Elaborat de autor

Diversitatea platformelor digitale disponibile oferă afacerilor soluții versatile pentru o gamă largă de operațiuni, de la gestionarea proiectelor la analiza datelor și procesarea plăților. Alegerea platformelor potrivite poate contribui la eficiența și succesul afacerilor în mediul digital modern, oferind instrumentele necesare pentru a rămâne competitive și inovatoare.

Importanța crucială a platformelor pentru economie a determinat realizarea de multiple studii focusate pe analiza impactului platformelor asupra economiei. Studiile realizate în domeniu, abodează trei aspecte principale ale impactului platformelor: infrastructurile de date, dinamica pieței și mecanismele de guvernanță.

- *Infrastructuri de date:* Autori precum Kitchin (2014) și Mayer-Schönberger&Cukier (2013) abordează procesul de "dataficare", unde platforme precum Apple și Google

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

transformă activitățile în date, schimbând practicile culturale și sectoare economice. Nieborg&Helmond (2019) accentuează importanța colectării datelor comportamentale prin intermediul infrastructurilor platformelor [4] [5] [6].

- *Dinamica piețelor:* Autori precum Rochet&Tirole (2003) și Argentesi&Filistrucchi (2007) explorează ideea piețelor multi-fațete create de platforme, analizându-le în contrast cu piețele tradiționale. Se discută modul în care platformele restructurează relațiile economice, subliniind efectele de rețea și distribuția puterii economice [7] [8].
- *Guvernanța:* Gillespie (2018) și Gorwa (2019) se concentrează pe guvernanța platformelor, evidențiind modul în care acestea structurează interacțiunile utilizatorilor prin interfețe, algoritmi și politici. Langlois&Elmer (2013) analizează tensiunile între guvernanța platformelor și normele locale/regulatorii [9] [10] [11].

Analizând literatura de specialitate, se observă că impactul platformelor asupra proceselor economice este profund și multidimensional. Platformele digitale, prin procesul de dataficare, nu doar că transformă interacțiuni obișnuite în date valoroase, dar și reconfigurează fundamental sectorul economic, influențând modul în care se colectează, se analizează și se utilizează informațiile. Acest aspect are implicații semnificative asupra practicilor culturale și comportamentului consumatorilor.

În contextul piețelor, platformele digitale creează ecosisteme multi-fațetate care modifică structura tradițională a pieței. Ele facilitează relații complexe între diferiți stakeholderi, cum ar fi utilizatorii, dezvoltatorii și advertiserii, amplificând efectele de rețea și redefinind distribuția puterii și a bogăției în economie. Acest fenomen conduce la noi modele de afaceri și strategii de piață, obligând companiile să se adapteze rapid pentru a rămâne competitive.

Pe planul guvernanței, platformele impun noi reguli și standarde, exercitând un control semnificativ asupra modului în care sunt gestionate interacțiunile și conținutul. Aceasta implică o reevaluare a cadrului regulatoriu și o conștientizare a impactului algoritmilor și politicilor platformelor asupra libertăților individuale și a concurenței de piață.

ROLUL PLATFORMELOR ÎN ADOPTAREA MUNCII REMOTE DE CĂTRE COMPANII

Munca remote, cunoscută și ca telemuncă sau muncă la distanță, reprezintă modul de lucru în care angajații își desfășoară activitățile profesionale din afara unui mediu de birou tradițional. Definițiile oferite muncii remote în literatura de specialitate scot în evidență caracterul flexibil de angajare, importanța tehnologiei și impactul benefici asupra anagajilor. Astfel, Ferrara (2022) definește munca la distanță ca un model în care angajații își îndeplinesc sarcinile în afara organizației folosind tehnologia, menționând flexibilitatea și autonomia acordată angajaților în acest model, afectând percepțiile lor despre muncă și bunăstarea personală [12].

Contextul apariției și dezvoltării muncii remote este strâns legat de progresul tehnologic. Astfel, pot fi distinse câteva etape în evoluția muncii remote, care presupun, de fapt, sincronizarea practicilor de utilizare a muncii remote cu evoluția tehnologiilor de comunicare:

- *Pre-Internet (înainte de anii 1990*): Munca la distanță era limitată și adesea se referea la lucrul de acasă pentru scriitori, artiști sau în telemarketing. Comunicarea se făcea prin telefon sau corespondență.

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

- *Începutul erei Internet (anii 1990 - începutul anilor 2000):* Internetul a început să faciliteze munca la distanță. Emailul și primele forme de comunicare online au apărut, dar munca remote era încă neobișnuită.
- *Dezvoltarea tehnologiei și software (începutul anilor 2000 - 2010):* Apariția Internetului de mare viteză, îmbunătățirea tehnologiilor de comunicație și colaborare (cum ar fi Skype) au făcut munca remote mai accesibilă și eficientă.
- *Adoptarea pe scară largă (2010 - 2020):* Instrumente ca Slack, Zoom, și Google Workspace au devenit populare. Multe companii au început să adopte politici flexibile de muncă, iar munca remote a devenit mai acceptată.
- *Boom-ul cauzat de pandemie (2020 - prezent):* Pandemia COVID-19 a accelerat tranziția către munca remote. Multe companii au fost forțate să adopte munca la distanță, iar unele au decis să continue acest mod de lucru chiar și după pandemie.

Perioada pandemiei COVID-19 a reprezentat un punct de cotitură atât pentru acceptarea muncii remote de către companii, cât și pentru investițiile în tehnologii dedicate organizării acestei forme de muncă. Platformele online au devenit o resursă cheie a multor companii, ele facilitând organizarea muncii la distanță, dar și permițând creșterea eficienței muncii și diminuarea chletuielilor legate de organizarea muncii. Vezi în babelul 3 tipurile de platforme dedicate facilitării muncii remote.

Tabelul 3. Platforme online implicate în organizarea muncii remote

Tip de platformă	Exemple	Modul de implicare în organizarea muncii remote
Platforme de comunicare	Zoom, Microsoft Teams, Slack	Facilitează comunicarea în timp real prin mesagerie, apeluri video și audio, esențiale pentru întâlniri și discuții de echipă.
Platforme de management al proiectelor	Asana, Trello, Jira	Ajută la organizarea sarcinilor, urmărirea progresului și gestionarea termenelor limită, vitale pentru menținerea organizării.
Platforme de partajare a fișierelor	Google Drive, Dropbox, OneDrive	Permit stocarea, partajarea și editarea colaborativă a documentelor, fundamentale pentru accesul ușor și securizat la documente.
Platforme pentru managementul HR	BambooHR, Gusto	Oferă soluții pentru gestionarea aspectelor HR, cum ar fi recrutarea și onboarding-ul, esențiale pentru gestionarea resurselor umane.
Platforme de monitorizare a timpului	Time Doctor, Toggl	Urmăresc timpul petrecut pe sarcini, oferind date despre productivitate, utile pentru managementul timpului și evaluarea eficienței.
Platforme de securitate și VPN	NordVPN, ExpressVPN	Asigură conexiuni securizate și protejează datele, cruciale pentru menținerea securității informațiilor într-un mediu de lucru distribuit.
Platforme de dezvoltare software	GitHub, GitLab	Facilitează colaborarea în dezvoltarea software și gestionează versiunile codului sursă, fundamentale pentru echipele de dezvoltare.

Sursă: Elaborat de autor

Platformele online sunt esențiale în facilitarea și optimizarea muncii remote, oferind un cadru integrat pentru diverse aspecte ale activității profesionale la distanță. Ele permit o comunicare eficientă, organizarea riguroasă a proiectelor, accesul facil la resurse și

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

documente, gestionarea eficientă a resurselor umane, monitorizarea productivității și asigurarea securității datelor. Prin aceste funcționalități, platformele online nu doar simplifică tranziția către un mediu de lucru distribuit, dar și sporesc eficiența, colaborarea și adaptabilitatea organizațiilor în fața provocărilor și dinamicii pieței muncii contemporane.

Importanța platformelor digitale în soluționarea diverselor probleme remote poate fi demonstrată prin numărul mare de utilizatori a acestor platforme (vezi tabelul 4).

Tabelul 4. Popularitatea platformelor utilizate în organizarea muncii remote

Platforma	Anul lansari i	Solutia specifica oferita	Numar de utilizatori
Asana	2008	Planificare și organizare proiecte	Peste 75.000 de echipe
Trello	2011	Tablouri Kanban pentru task management	Peste 50 de milioane de utilizatori
Slack	2013	Comunicare și colaborare în timp real	Peste 10 milioane de utilizatori zilnic
Zoom	2013	Videoconferințe, întâlniri virtuale, webinare	Peste 300 de milioane de utilizatori zilnic
Notion	2018	Organizare proiecte, gestiunea sarcinilor și documentelor	Peste 4 milioane de utilizatori
Hubstaff	2012	Monitorizarea timpului, managementul proiectelor și facturarea clienților	Peste 10.000 de companii
Todolist	2007	Organizare task-uri și managementul timpului	Peste 25 milioane de utilizatori

Sursă: Elaborat de autor

Popularitatea platformelor utilizate în organizarea muncii remote a crescut semnificativ, în special în contextul pandemiei COVID-19, care a accelerat tranziția către modalități de lucru flexibile și distribuite. Aceste platforme oferă numeroase avantaje, contribuind la eficientizarea muncii, economia de resurse și îmbunătățirea colaborării în cadrul echipelor.

Facilitarea organizării muncii la distanță prin intermediul platformelor digitale a condus la producerea unei schimbări radicale în potențialul de recrutare și angajare a specialiștilor. Companiile nu mai sunt limitate la angajarea de specialiști din zona geografică în care se află birourile lor fizice, platformele digitale deschizând calea către o forță de muncă mai diversă și mai calificată.

EXODUL VIRTUAL DE CREIERE

Revoluția produsă în economie ca rezultat a platformizării a generat multiple transformări esențiale în viața socio-economică, cît și apariția de noi fenomene. Unul dintre fenomenele generate de platformizare este cel al „exodului virtual de creiere”.

Exodul virtual de creiere este un termen care descrie fenomenul în care profesioniștii talentați și bine pregătiți părăsesc sau lucrează din afară țării lor de origine pentru a desfășura activități în cadrul economiei digitale și a platformelor online. Esența acestui fenomen rezidă în migrația "virtuală" a capitalului intelectual, cunoștințelor și competențelor, în detrimentul locațiilor geografice tradiționale.

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

Diferența cheie între exodul virtual de creiere și cel tradițional constă în modul în care se desfășoară și în domeniile de activitate pe care le afectează (vezi figura 1).

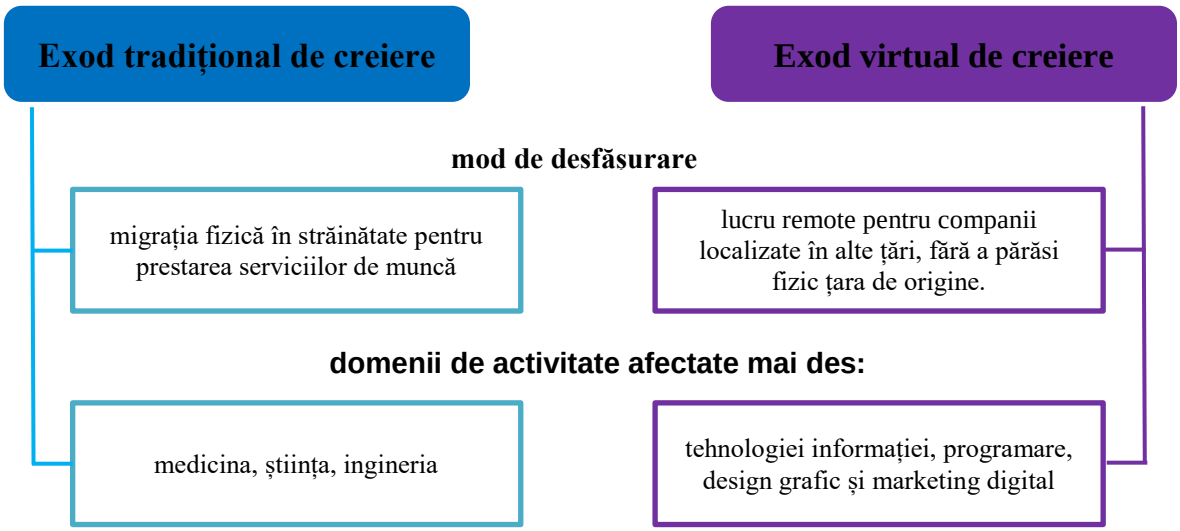


Figura 1. Exod virtual de creiere versus exod tradițional
Sursă: Elaborat de autor

Exodul virtual de creiere este în mare măsură rezultatul revoluției digitale și al platformizării economiei, permițând profesioniștilor să-și valorifice abilitățile într-un mod mai flexibil și global, fără a părăsi fizic țara lor.

Amploarea fenomenului de exod virtual al creierelor este studiat în timp real de Organizația Internațională a muncii, în cadrul proiectului iLabour project (vezi figura 2).

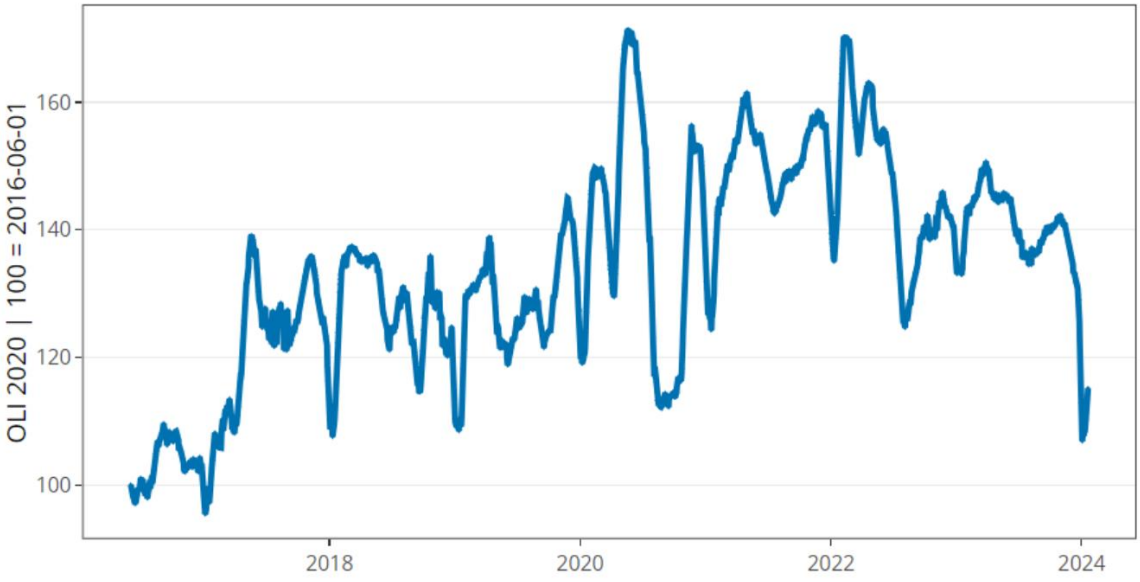


Figura 2. Evoluția cererii pentru munca online la nivel global, 01.06.2016=100%
Sursă: http://onlinelabourobservatory.org/oli-demand/

In cadrul observatorului muncii online sunt monitorizate atât cererea companiilor pentru munca online, cât și oferta. Datele oferite indica că în topul țărilor beneficiare a exodului virtual de creiere sunt Statele Unite ale Americii și Marea Britanie, iar domeniile

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

cu cea mai înaltă cerere pentru talentele angajate virtual sunt dezvoltarea de soft, împreună cu domeniul creativ și multimedia (vezi figura 3).

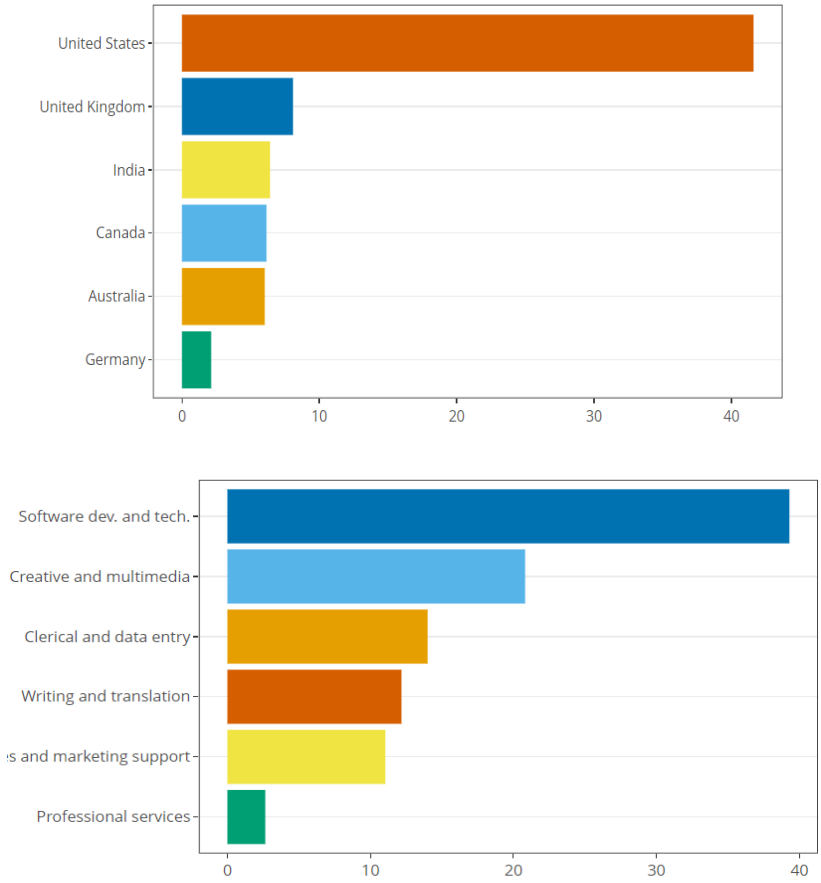
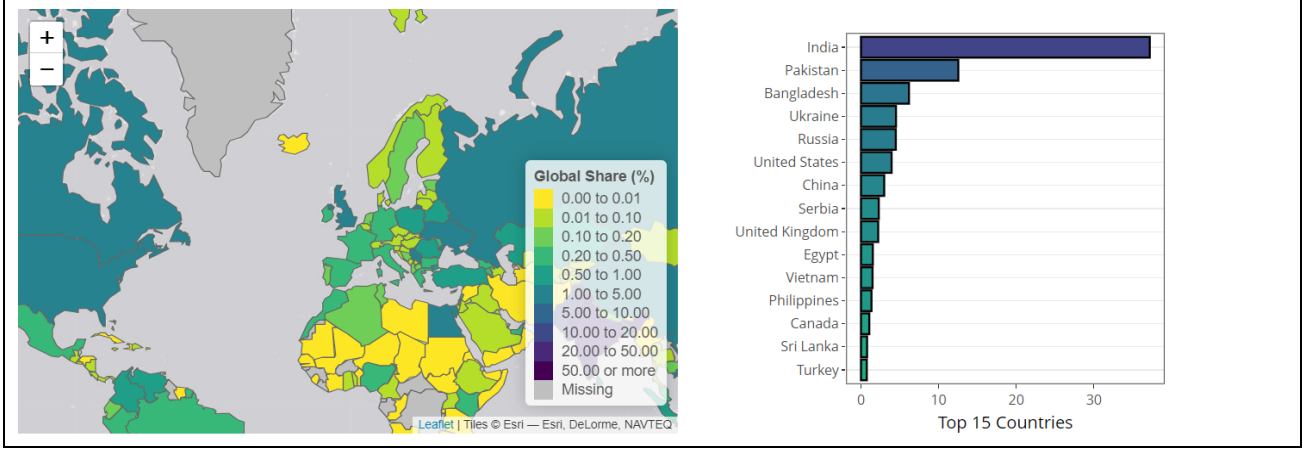


Figura 3. Top țări și domenii în cererea pentru munca online
Sursă: http://onlinelabourobservatory.org/oli-demand/

Similar exodului tradițional de creiere, și în cazul exodului virtual în calitate de țări de destinație a exodului sunt țările mai dezvoltate cu activitate înalta a businessului și salarii competitive, tări de origine fiind țările cu economii mai slab dezvoltate, respectiv, cu un nivel mai redus al salariilor (vezi figura 4)



DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

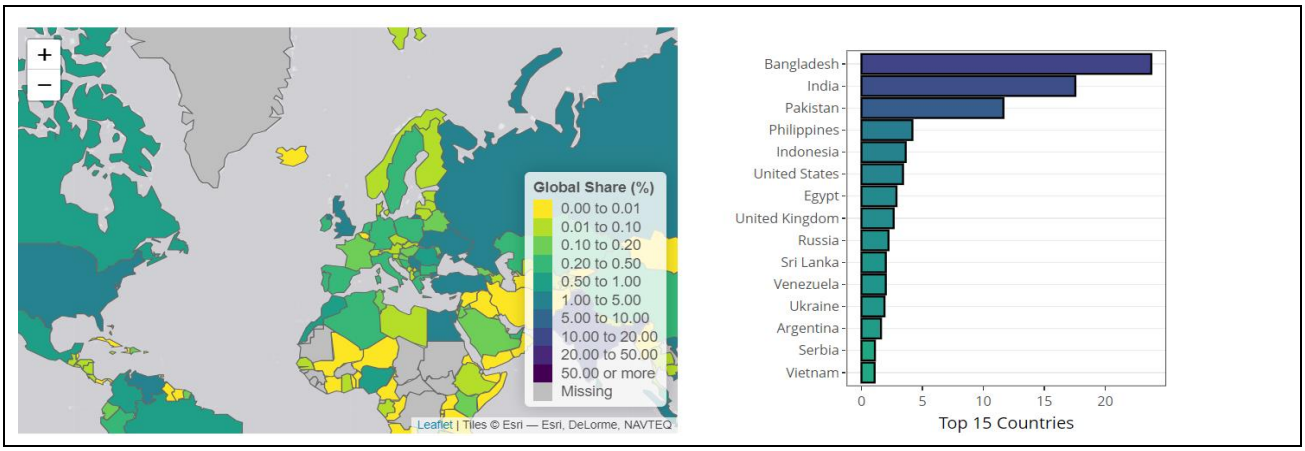


Figura 4. Top 15 țări în oferta de muncă online (1) în domeniul dezvoltare de soft, (2) în domeniu creativ și multimedia

Sursa: http://onlinelabourobservatory.org/oli-supply/

Un studiu realizat în anul 2021 de către Boston Consulting Group, pe un eșantion de 209,000 respondenți din 190 țări arată că indiferent de forma de migragie în scopuri de muncă, tradițională sau virtuală, țările de destinație aflate în topul preferințelor, sunt aceleași (vezi figura 5).

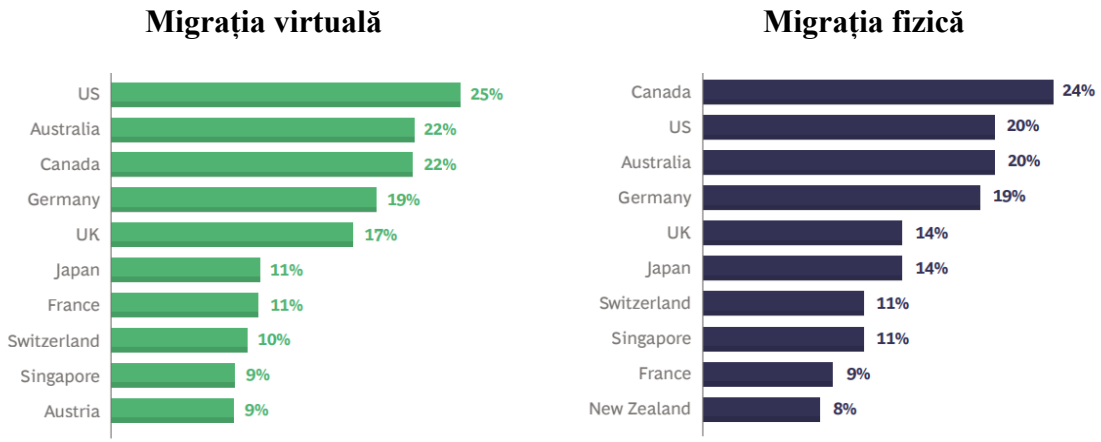


Figura 5. Tările de destinație în migrația pentru muncă (unde ar dori să migreze respondenții)

Sursă: preluat din sursa 14, p.11.

Răspândirea fenomenului "exod virtual de creiere" a adus modificări semnificative pe piața muncii, reflectând schimbările în modul în care talentul este atras, reținut și gestionat într-un mediu de lucru globalizat și digitalizat. Pe de o parte, grație platformelor digitale ce permit munca remote, companiile au acces la un pool global de talente, permițându-le să angajeze cei mai buni profesioniști din întreaga lume, indiferent de localizarea lor geografică. Pe de altă parte, crește semnificativ concurența pentru talentele de top, companiile fiind nevoiete să adopte strategii de recrutare mai inovatoare și să utilizeze tehnologii digitale pentru a atrage și a evalua candidații de la distanță.

În același timp, utilizarea de către companii a echipelor de specialiști localizați în diferite țări aduce provocări specifice pentru managementul resurselor umane, precum:

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

- *Diferențe culturale și de comunicare:* Managementul unei forțe de muncă diverse cultural necesită o înțelegere profundă a diferențelor culturale și a modurilor de comunicare. Aceste diferențe pot influența stilurile de lucru, așteptările și interpretarea feedback-ului.
- *Conformitatea cu legislația locală:* Fiecare țară are propriile sale legi și reglementări privind munca, inclusiv contracte de muncă, beneficii, ore de lucru, concedii și impozitare. Navigarea și respectarea acestor legi poate fi complexă și consumatoare de timp.
- *Diferențe în fusurile orare:* Coordonarea și planificarea întâlnirilor sau termenelor limită poate fi dificilă datorită diferențelor de fus orar. Acest lucru poate duce la întârzieri în comunicare și poate afecta productivitatea.
- *Managementul performanței la distanță*: Evaluarea și monitorizarea performanței angajaților care lucrează remote și în diferite locații geografice pot fi provocatoare. Există riscul lipsei de vizibilitate și a dificultăților în menținerea angajamentului și motivației.
- *Probleme de securitate și confidențialitate:* Asigurarea securității datelor și a confidențialității într-un mediu de lucru distribuit este o provocare majoră, mai ales când angajații accesează sistemele companiei de la distanță.
- *Construirea și menținerea culturii organizaționale:* Crearea unei culturi organizaționale coezive și a unui sentiment de apartenență în rândul angajaților care nu se întâlnesc fizic poate fi dificilă. Acest lucru necesită eforturi conștiente pentru a promova valorile și obiectivele companiei.
- *Comunicarea și colaborarea efectivă:* Asigurarea unei comunicări eficiente și a colaborării între membrii echipei care nu se întâlnesc față în față necesită utilizarea eficientă a tehnologiilor digitale și a unor strategii de comunicare adaptate.

În contextul angajărilor remote și al formării echipelor de specialiști localizați în diferite țări, companiile adoptă abordări inovatoare pentru a gestiona aceste provocări. Acestea includ investiții în tehnologii avansate de colaborare și comunicare, dezvoltarea unei culturi organizaționale care promovează diversitatea și incluziunea, și implementarea unor strategii de recrutare și onboarding adaptate la mediul virtual. De asemenea, companiile pun accent pe flexibilitate, adaptându-se la diferite fusuri orare și stiluri de lucru, și se concentrează pe managementul performanței și feedbackul continuu pentru a menține angajamentul angajaților. Programele de dezvoltare profesională accesibile remote, politicile HR care respectă legislația locală și internațională, promovarea echilibrului muncă-viață și construirea de echipe virtuale eficiente sunt, de asemenea, esențiale. În plus, securitatea datelor și confidențialitatea sunt prioritizate pentru a proteja informațiile sensibile într-un mediu de lucru distribuit.

CONCLUZII

1. Ascensiunea economiei bazate pe platforme, parte a revoluției Industriei 4.0, transformă fundamental sistemele economice și de afaceri, modificând paradigma tradițională prin digitalizare, conectivitate extinsă, personalizare masivă și colaborarea om-mașină.
2. Platformele digitale au un impact profund și multidimensional asupra economiei, influențând modul în care se colectează, se analizează și se utilizează informațiile, reconfigurând sectorul economic, practicile culturale și comportamentul consumatorilor.

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

3. Munca remote, facilitată de progresul tehnologic, a evoluat de la o practică limitată pre-internet la o adopție pe scară largă în era digitală, cu un boom semnificativ cauzat de pandemia COVID-19.
4. Platformele online au devenit resurse cheie pentru organizarea muncii la distanță, oferind un cadru integrat pentru comunicare, gestionarea proiectelor, securitatea datelor și alte aspecte ale activității profesionale.
5. Fenomenul de exod virtual de creiere, unde profesioniștii talentați lucrează la distanță pentru companii internaționale fără a părăsi țara de origine, este o consecință a revoluției digitale și platformizării economiei.
6. Exodul virtual de creiere diferă de cel tradițional prin natura sa virtuală, concentrându-se pe domenii precum tehnologia informației, programarea, designul grafic și marketingul digital.
7. Companiile care adoptă munca remote se confruntă cu provocări specifice, cum ar fi diferențele culturale, conformitatea cu legislația locală, diferențele în fusurile orare, managementul performanței la distanță și securitatea datelor.
8. Pentru a gestiona provocările muncii remote, companiile investesc în tehnologii de colaborare, dezvoltă culturi organizaționale care promovează diversitatea și adoptă strategii de recrutare adaptate la mediul virtual.
9. Fenomenul "exod virtual de creiere" a adus modificări semnificative pe piața muncii, reflectând schimbările în modul în care talentul este atras, reținut și gestionat într-un mediu de lucru globalizat și digitalizat.

BIBLIOGRAFIA

1. KENNEY, Martin; ZYSMAN, John. The rise of the platform economy. *Issues in science and technology*, 2016, 32.3: 61.pp. 61-69. ISSN: 0748-5492.
2. CHOUDARY, Sangeet Paul. Platform scale: How an emerging business model helps startups build large empires with minimum investment. *(No Title)*, 2015. ISBN 10: 9810967586
3. DELOITE. *The rise of the platform economy*. [online]. 2019. [accesat 05.12.2023]. Disponibil: <https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/humancapital/deloitte-nl-hc-the-rise-of-the-platform-economy-report.pdf>
4. KITCHIN, Rob. The data revolution: Big data, open data, data infrastructures and their consequences. *The Data Revolution*, 2014, 1-240. ISSN 2116-5289.
5. MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. *Big Data: die Revolution, die unser Leben verändern wird*. Redline Wirtschaft, 2013. ISBN: 9783868815061.
6. NIEBORG, David B.; HELMOND, Anne. The political economy of Facebook's platformization in the mobile ecosystem: Facebook Messenger as a platform instance. *Media, Culture & Society*, 2019, 41.2: 196-218. ISSN: 1460-3675.
7. ROCHET, Jean-Charles; TIROLE, Jean. Platform competition in two-sided markets. *Journal of the european economic association*, 2003, 1.4: 990-1029. ISSN: 152-4774.
8. ARGENTESI, Elena; FILISTRUCCHI, Lapo. Estimating market power in a two-sided market: The case of newspapers. *Journal of Applied Econometrics*, 2007, 22.7: 1247-1266. ISSN:1099-1255.

DOI: https://doi.org/10.53486/escst2023.01
International Conference, December 07-08, 2023, Chișinău, Moldova

9. GILLESPIE, Tarleton. *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press, 2018. ISBN-13978-0300173130.
10. GORWA, Robert. What is platform governance? *Information, communication & society*, 2019, 22.6: 854-871.
11. LANGLOIS, Ganaele; ELMER, Greg. The research politics of social media platforms. *Culture machine*, 2013, 14.
12. FERRARA, Bruna, et al. Investigating the role of remote working on employees' performance and well-being: an evidence-based systematic review. *International Journal of Environmental Research and Public Health*, 2022, 19.19: 12373. ISSN: 1660-4601
13. KOVÁCS-ONDREJKOVIC, Orsolya, et al. Decoding global talent, onsite and virtual. *Boston Consulting Group*, 2021.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

TRANSFORMĂRI STRUCTURALE ALE PIEȚEI MUNCII ÎN ERA INTELIGENȚEI ARTIFICIALE

STRUCTURAL TRANSFORMATIONS OF THE LABOR MARKET IN THE AGE OF ARTIFICIAL INTELLIGENCE

Oxana BARBĂNEAGRĂ

PhD, Associate professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0009-0008-2567-0170
E-mail: oxana.barbaneagra@ase.md

Abstract: *The extent of artificial intelligence can be realized by contributing to the scientific, technological, economic and social development and progress of humanity. While AI is driving growth in many industries and bringing economic benefits, it is causing deep disruption and structural transformations in the labor market, in both positive and negative ways. We are witnessing the replacement of job roles by AI-driven automation and a growing demand for professionals with AI expertise, new professions emerging that did not exist before. On the other hand, the introduction of technologies leads to the reduction of middle-skilled workers, increases the gap between low-wage and high-wage workers. Under these conditions, employees and employers must adapt to these challenges in the labor market that produce changes in the occupational structure by acquiring new skills.*

Keywords: *labor market, artificial intelligence, soft skills, hard skills, professional competences, occupational structure.*

UDC: *331.52:004.8*

JEL Classification: *J21, J23, J24.*

INTRODUCERE

Relevanța subiectului se datorează influenței utilizării sistemelor de inteligență artificială asupra pieței muncii, producând schimbări semnificative în cererea de personal dar și a cerințelor față de angajați. Inteligența artificială (IA) are un impact transformator asupra pieței muncii prin automatizarea proceselor, îmbunătățirea procesului decizional și deschiderea de noi oportunități într-o varietate de industrii.

Odată cu avansarea rapidă a tehnologiilor digitale, IA influențează semnificativ modul de desfășurare al activității profesionale a indivizilor. Adoptarea la scară largă a tehnologiilor și sistemelor de IA ridică preocupări pe piața muncii, care sunt legate de micșorarea cererii pentru unele profesii, apariția de noi profesii, schimbarea structurii ocupaționale, modificarea profilurilor de competențe la unele categorii de personal, creșterea cerințelor de adaptibilitate a personalului, cerințe sporite pentru „soft skills", cerere mare pentru specialiști cu dexteritate digitală.

Avansarea accelerată la nivel global al sistemelor de IA resetează piața muncii prin crearea de noi locuri de muncă pentru tineri și persoane de înaltă calificare, întrucât dezvoltarea și menținerea sistemelor de IA necesită o forță de muncă specializată și înalt calificată. Această stare de fapt, denotă o creștere pentru profesioniști cu expertiză în IA și domenii conexe, precum știința datelor și învățarea automată. În același timp, adoptarea pe scară largă a tehnologiilor IA ridică preocupări privind înlocuirea locurilor de muncă (unele locuri de muncă dispar și apar altele noi). În aceste condiții, se identifică problema adaptării

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

la schimbările de pe piața muncii prin dobândirea de noi abilități, acceptarea învățării pe tot parcursul vieții, perfecționarea și dezvoltarea continuă a competențelor profesionale.

INTELIGENȚA ARTIFICIALĂ

Inteligența artificială înseamnă capacitatea sistemelor inteligente de a executa funcții creative, care tradițional sunt efectuate de către om. Inteligenta artificiala se prezintă drept o noțiune interdisciplinară, având mai multe sensuri. În Dicționarul explicativ al limbii române, IA este un domeniu al informaticii care dezvoltă sisteme tehnice capabile să rezolve probleme dificile de inteligența umană [5]. Autorul P.H. Winston definește inteligența artificială "ca fiind studiul proceselor computaționale care permit percepție, gândire și acțiune" [19]. Într-o altă definție „Inteligența artificială este acea activitate dedicată fabricării mașinilor inteligente, iar inteligența este acea calitate care permite unei entități să funcționeze în mod adecvat și cu previziune în mediul său" [12]. Printre primii care a încercat să definească IA a fost Alan Turing, care în anii 1950 pentru a răspunde la întrebarea ce este un sistem „inteligent" creat de om, a prezentat o soluție: „Dacă un ascultător nu poate spune dacă aude o conversație umană sau una cu o mașină, atunci putem spune că avem un sistem inteligent, sau inteligență artificială" [8].

Termenul inteligență artificială este folosit pentru a descrie mașinile care imită funcțiile „cognitive", pe care oamenii le asociază cu mintea umană, cum ar fi „învățarea" și „rezolvarea problemelor". Capacitățile mașinilor moderne clasificate în general ca IA includ înțelegerea cu succes a vorbirii umane, concurența în sistemele de joc strategice, mașini care operează în mod autonom, rutare inteligentă în rețelele de livrare a conținutului și simulări militare [6, p. 47].

IA este de două tipuri: software și încorporată. IA software include asistenți virtuali, motoare de căutare, sisteme de recunoaștere facială și vocală, programe informatice care analizează imagini. IA încorporată include roboții, dronele, mașini automate și internetul obiectelor. În funcție de performanță sau de capacitatea de a realiza diverse sarcini IA poate fi:

IA tradițională poate efectua sarcini specifice pe seama unor algoritmi stabiliți, reprezintă sisteme care nu pot învăța din date, adică nu pot fi îmbunătățite în timp.

Învățarea automată (machine learning), reprezintă un proces în care un program de calculator se poate adapta independent și învăța din noile date.

IA conversațională permite mașinilor să înțeleagă și să răspundă limbajului uman într-un mod asemănător omului, se utilizează pentru a crea sisteme interactive angajate în dialog asemănător omului.

IGA (Inteligența general artificială) se referă la sisteme extrem de autonome, în present ipotetice, care pot depăși munca umană în cel mai valoros mod economic. Dacă s-ar realiza, AGI ar fi capabil să înțeleagă, să învețe, să se adapteze și să implementeze cunoștințele într-o gamă largă de sarcini.

IAG (Inteligența artificială generativă) – poate învăța din date și poate genera date, utilizează tehnici de învățare automată, generează text asemănător omului și diferite tipuri de date. Este utilă în proiectarea asistenților virtuali, care generează răspunsuri asemănătoare oamenilor, în dezvoltarea jocurilor video, poate genera chiar date sintetice pentru antrenarea altor modele di IA. Are un impact puternic asupra aplicațiilor de afaceri. Poate stimula inovația, poate automatiza sarcinile creative și poate oferi experiențe personalizate clienților. Multe companii văd în IA generativă un instrument nou puternic

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

pentru crearea de conținut, rezolvarea problemelor complexe și transformarea modului în care clienții și lucrătorii interacționează cu tehnologia.

Sondajul global anual efectuat de McKincey privind starea actuală a inteligenței artificiale denotă o creștere a instrumentelor de IA generative.

Automatizarea și robotizarea în sfera activității economice, prin sporirea multiplă a productivității factorilor de producție și a produsului finit contribuie și accelerează creșterea economică, creează noi posibilități pentru dezoltarea umană, influențând, totodată, piața muncii prin deplasarea și substituirea forței de muncă.

În condițiile unor proiecții globale se estimează că până în 2030 cca. 70% din companii vor utiliza cel puțin o tehnologie IA (viziune computerizata, prelucrarea limbajului natural, asistenți virtuali, automatizare/robotizare, machine learning), iar tehnologia va genera rezultate economice adiționale de cca. 1.2% creștere anuală a PIB global [3].

Apărută de la începuturi drept o ramură a informaticii, astăzi IA reprezintă un domeniu multidisciplinar cu implicații a economiei, psihologiei, ingineriei calculatoarelor, lingvisticii, matematicii etc. cu influențe reciproce, determinând și provoacând schimbări în unele domenii de științe cu care se intersectează.

Avansarea fără precedent a tehnologiilor de vârf în toate domeniile vieții (transport, logistică, medicină, comunicații, sector militar, producție) nu a substituit forța de muncă ca factor de producție, ci a redefinit-o, creând noi oportunități de aplicații intensive a computerelor și tehnologiilor de vârf [9].

IA este utilizată pe larg pe piața muncii, contribuind la transformări în majoritatea industriilor. În domeniul sănătății, prin IA cercetătorii analizează volume uriașe de date medicale pentru inovarea și perfecționarea diagnosticării, spre exemplu un program de IA poate să recunoască un atac de cord în timpul apelului de urgență. În domeniul transportului aerian se utilizează un sistem inteligent de organizare a navigării, de planificare a rutelor și de asigurare a funcționmării eficiente a navei aeriene. Fabricile inteligente utilizează roboți în procesul de producție și optimizarea vânzărilor, în utilizarea eficientă a resurselor umane și creșterea satisfacției profesionale. Sisteme de inteligență artificială sunt utilizate în bănci pentru înlesnirea tranzacțiilor financiare și înlăturarea tranzacțiilor ilicite. Utilizarea IA în agricultură permite utilizarea la o scară mai redusă a îngrășămintelor chimice, monitorizarea calității solului, stabilirea cantității necesare de hrană pentru animale, modificarea genetică a semințelor ca să reziste în condiții de mediu neprielnice. IA în educație face ca învățarea elevilor să fie mai ușoară, să găsească mai rapid informația necesară la câteva click-uri distanță, aici adăugându-se table inteligente, software-uri de comunicare între părinți și pedagogi. IA este folosită cu success în domeniul resurselor umane, se automatizează sarcinile repetitive, procesul de recrutare, evaluarea performanței, comunicarea internă și traininguri.

Aplicabilitatea IA în viața de zi cu zi se evidențiază prin cumpărăturile și publicitatea online, căutări pe internet, asistenți personali digitali, traduceri automate, case inteligente, securitatea cibernetică, reducerea dezinformării (extragerea de falsuri de pe rețelele sociale prin aplicații de inteligență artificială), detectarea și înlăturarea conturilor teroriste de pe platformele sociale etc.

IA accelerează schimbul de profesii, creând noi locuri de muncă, în acest sens vom preciza două aspecte importante: înlocuirea forței de muncă (eliminarea sau reducerea locurilor de muncă) și modificarea ponderii forței de muncă în valoarea adăugată a economiei [2].

IA este un domeniu dinamic și în evoluție rapidă, care cuprinde dezvoltarea de sisteme software inteligente capabile să îndeplinească sarcini, care necesită în mod

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

tradițional inteligență umană. Sistemele IA manipulează și analizează cantități mari de date, extragând informații valoroase, care sporesc eficiența și inovația afacerii. IA are potențialul de a ne revoluționa viața și munca, de la automatizarea sarcinilor banale până la crearea de noi produse și servicii. Aplicațiile IA sunt vaste și variate, de la mașini cu conducere autonomă și asistenți virtuali până la diagnosticare medicală și analiză financiară.

Inteligența artificială vine să reseteze piața muncii prin utilizarea tot mai largă a inteligenței artificiale generative, în rezultatul aplicării căreia se automatizează sarcinile repetitive, are loc îmbunătățirea procesului decizional uman și crearea de noi oportunități de angajare. După cum am menționat anterior, impactul asupra creșterii economice, productivității și competitivității este simțitor, însă aceste beneficii comportă provocări structurale pe piața muncii.

În studiul McKencey (2023) se menționează că IA generativă și alte tehnologii simulative comportă un potențial de a automatiza circa 70% din activitățile angajaților, care se datorează în principal posibilității IA generative de a înțelege limbajul natural. În rezultat, impactul inteligenței artificiale generative se resimte semnificativ în domeniile ocupate în prezent de angajați cu un nivel educațional peste medie. Potrivit analiștilor McKinsey, aproximativ jumătate dintre activitățile de lucru de astăzi ar putea fi automatizate între anii 2030 și 2060 [10].

Totuși, avantajul IA generative de a influența creșterea productivității muncii de la 0,1 la 0,6% către anul 2040 (în funcție rata tehnologiilor adoptate) vine la pachet cu necesitatea de a sprijini angajații în tranziția spre noi locuri de muncă, schimbarea domeniilor de activitate, dezvoltarea de noi competențe [10].

În condițiile create, se observă, că transformările generate de IA la scară globală exercită o presiune tot mai mare asupra forței de muncă, mai ales, cu referire la lucrătorii bine plătiți, ale căror activități erau considerate relative imune la automatizare.

Era inteligenței artificiale generative abia începe, iar primele studii de caz sunt încurajatoare. Cu toate acestea, este necesar timp pentru a realiza o analiză comprehensivă a beneficiilor aduse de această tehnologie, iar autoritățile publice și liderii de afaceri vor trebui să facă față unor provocări diverse, cum ar fi gestionarea impactului asupra forței de muncă sau reorganizarea proceselor de afaceri.

În opinia noastră, polarizarea demonstrează cel mai evident schimbările în structura pieței muncii influențată puternic de avansările IA. Aceasta se explică prin creșterea semnificativă a numărului de lucrători cu înaltă calificare și slabă calificare pe piața muncii, și în același timp, printr-o scădere semnificativă a numărului de locuri de muncă care necesită un nivel mediu de calificare. Aceasta înseamnă că potențialul pieței muncii nu permite realizarea deplină a capitalului uman al unui număr de profesioniști angajați în muncă, care necesită calificări de nivel mediu. Ca urmare, situația ce se conturează conduce la o lipsă de ofertă pe piața muncii și la deprecierea investițiilor într-o serie de profesii, care implică muncă manuală și semi-automatizată, dar necesită un nivel suficient de calificare și implicare, ceea ce duce la o scădere a veniturilor clasei de mijloc și o reducere a bunăstării lor.

Amenințarea polarizării pieței muncii din Republica Moldova, este asociată în primul rând cu stabilitatea în sfera reînnoirii capitalului uman la nivel național. Importanța tot mai mare a învățământului superior și a competențelor specializate pe piața muncii au condus la o piață a muncii polarizată, locurile de muncă cu calificare înaltă devin tot mai solicitate, iar locurile de muncă cu salarii medii în scădere. Considerăm că dezvoltarea învățământului secundar profesional și actualizarea programelor din punctul de vedere al tendințelor

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

tehnologice moderne pot sprijini transformarea tehnologică a profesiilor aflate în pericol. Prin urmare, o modalitate de a aborda polarizarea pieței muncii este de a investi în programe de educație și formare care îi ajută pe lucrătorii să dobândească abilitățile de care au nevoie pentru a reuși în profesiile care sunt relevante pentru nivelurile date de tehnologie.

Recrutarea resurselor umane s-a transferat de ceva timp în zona online. Companiile specializate în recrutare oferă soft-uri tip roboți pentru analiza datele candidaților, precum și a comportamentului acestora în timpul intervieverii (RPA-Robotic Process Automation). Implicarea inteligenței artificiale în recrutare oferă posibilitate companiilor să analizeze fluxuri de date în selecția celui mai optim candidat. Rețelele și platformele sociale, precum LinkedIn, Blog, Instagram, Facebook, Google+ au început să fie utilizare pe larg de către companii în procesul de recrutare digital a resurselor umane.

Una dintre schimbările majore dintre care au intervenit pe piața muncii în ultimul deceniu, ține de dezvoltarea masivă și avansareaa așa-numitei „Economie Gig" (Gig economy), care se referă la angajarea resursei umane pe termen scurt, în realizarea unor sarcini și proiecte concrete. Economia Gig readuce persoanele inactive, oferindu-le locuri de muncă, cu referire și la persoanele, care au pierdut locuri de muncă ca urmare al impactului IA asupra pieței muncii, oferindu-le oportunități de flexibilitate, diversificare și avantaje financiare.

Prin urmare Economia Gig are un impact pozitiv asupra nivelului de activitate al populației apte muncă, idee susținută și de cercetătoarea D. Mulcahy, care menționează că "prin intermediul economiei gig oamenii au acces la o varietate de oportunități de muncă, care nu au fost disponibile în trecut, în același timp, economia gig deschide ușile către piață persoanelor care nu au acces la piața tradițională a muncii" [11].

Mai multe companii internaționale specializate în recrutarea personalului analizează impactul IA asupra pieței muncii, în acest sens Linkedin a evidențiat cinci tendințe de dezvoltare a pieței muncii sub impactul aplicării pe larg a IA, după cum urmează [18]:

1. *Automatizare și înlocuirea locurilor de muncă.*

Automatizarea proceselor de muncă prezintă motive de îngrijorare privind impactul pe care îl are asupra pieții muncii. Pe de o parte, crește productivitatea și eficiența, care se soldează cu profituri mai mari pentru afaceri cu costuri mai mici; Automatizarea creează, noi oportunități de muncă, cum ar fi rezolvarea de probleme, gândirea critică și comunicarea. Pe de altă parte, se înregistrează pierderi semnificative de locuri de muncă și scăderi ale salariilor. Pentru a atenua aceste efecte, lucrătorii trebuie să-și dezvolte noi abilități și să se adapteze la cele mai noi tehnologii pentru a rămâne competitivi pe piața muncii.

Automatizarea locurilor de muncă slab calificate a devenit o problemă critică în era inteligenței artificiale. Pentru a reduce impactul automatizării asupra acestor categorii de lucrători, este imperativ să se asigure accesul la formare și educație, să se investească în programe de recalificare, care să echipeze lucrătorii cu abilitățile de care au nevoie pentru a reuși într-o economie în evoluție.

2. *Creșterea tehnologiilor bazate pe IA și impactul lor asupra creării de locuri de muncă*

Se așteaptă ca inteligența artificială să revoluționeze piața muncii prin încurajarea inovației și a creșterii în diverse industrii, cum ar fi sănătatea, finanțele și educația. Tehnologiile bazate pe inteligență artificială, cum ar fi procesarea limbajului natural și viziunea computerizată, deschid calea pentru colaborarea om-mașină, ceea ce duce la noi oportunități de angajare. Sistemele de asistență medicală bazate pe inteligență artificială

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

pot ajuta medicii să diagnosticheze și să trateze pacienții mai precis și mai eficient, în timp ce sistemele financiare bazate pe inteligență artificială pot ajuta băncile și instituțiile financiare să ia decizii de investiții mai bune. În plus, tehnologiile bazate pe inteligența artificială pot contribui la reducerea decalajului de competențe, oferind oportunități de formare și perfecționare pentru lucrători.

Totodată, tehnologiile bazate pe inteligența artificială crează pe piața muncii o varietate de noi profesii (noi roluri de muncă), cum ar fi analisti de date, ingineri de învățare automată și eticieni în inteligență artificială. Pentru a se distinge în aceste noi profesii, indivizii trebuie să posede un amestec interdisciplinar de abilități tehnice și soft, cum ar fi comunicarea și creativitatea. Companiile trebuie să se adapteze și să îmbrățișeze aceste noi tehnologii pentru a rămâne competitive într-un peisaj în continuă schimbare. În plus, crearea de noi roluri de muncă prezintă oportunități interesante pentru persoanele, care doresc să intre în industria tehnologiei sau să-și extindă setul de abilități.

Se resimte mai puternic impactul IA asupra locurilor de muncă de înaltă calificare prin faptul că sarcinile banale se automatizează, iar locurile de muncă cu înaltă calificare se îmbunătățesc. Este esențial să recunoaștem potențialul IA de a transforma piața muncii, deoarece unele locuri de muncă pot deveni învechite, altele vor fi redefinite și vor apărea noi oportunități. Pentru a crea o forță de muncă mai eficientă și mai productivă, este esențial să îmbrățișăm IA și potențialul acesteia de a spori capacitățile umane. Acest lucru va îmbunătăți calitatea muncii. Procedând astfel, putem crea o forță de muncă mai eficientă și mai productivă, care valorifică punctele forte ale oamenilor și ale mașinilor.

3. *Perfecţionarea şi recalificarea pentru piaţa muncii bazată pe inteligenţă artificială*

În timp ce piața muncii evoluează continuu și este bazată pe IA, tot mai important este ca lucrătorii să accepte perfecționarea și recalificarea, ca să rămână competitivi și relevanți în economia bazată pe IA. Îmbunătățirea competențelor implică îmbunătățirea abilităților și cunoștințelor existente, în timp ce recalificarea implică învățarea abilităților actualizate. Abilitățile soft, cum ar fi comunicarea și rezolvarea problemelor, sunt, de asemenea, esențiale pentru succesul într-o economie bazată pe inteligență artificială, or angajatorii caută din ce în ce mai mult să angajeze lucrători cu abilități tehnice și soft (hard skill și soft skill).

În aceste condiții intervine necesitatea programelor de instruire pentru piața muncii bazată pe inteligența artificială, dat fiind faptul că nevoia de competențe legate de IA este în creștere. Universitățile și școlile tehnice au dezvoltat programe de studii specializate axate pe IA și domenii conexe, iar organizațiile oferă programe de formare și certificări în domenii precum analiza datelor, învățarea automată și programare.

4. *Tendințe emergente în viitorul muncii*

Inteligența artificială și alte tehnologii de ultimă oră modelează viitorul muncii. Este posibil ca automatizarea să înlocuiască locurile de muncă tradiționale, în timp ce Economia Gig câștigă avânt datorită flexibilității și autonomiei mai mari. De asemenea, înaintează și accelerează munca la distanță, datorită progreselor tehnologice, facilitând colaborarea și comunicarea lucrătorilor de oriunde în lume.

Inteligența artificială va deveni un factor cheie în viitorul muncii, deoarece va permite companiilor să automatizeze sarcinile banale și să ofere informații bazate pe date. Chatbot-urile bazate pe inteligență artificială pot gestiona intrebarile și reclamațiile clienților, eliberând resursele umane pentru a se concentra pe sarcini mai complexe. De asemenea, inteligența artificială va îmbunătăți performanța angajaților prin analiza datelor

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

și furnizarea de programe de formare personalizate, îmbunătățind productivitatea, satisfacția în muncă și ratele de reținere.

5. *Provocări și oportunități pentru viitorul lucrului cu AI*

IA la locul de muncă are potențialul de a revoluționa munca, dar nu este lipsită de provocări. Deplasarea locurilor de muncă poate fi una dintre cele mai importante provocări. Cu toate acestea, poate conduce și la crearea de noi locuri de muncă în domenii precum analiza datelor, învățarea automată și dezvoltarea AI. Pentru a se adapta la aceste schimbări, atât angajatorii, cât și angajații trebuie să fie pregătiți să accepte schimbarea. Angajatorii trebuie să investească în formarea și îmbunătățirea forței de muncă pentru a se asigura că sunt echipați de a ține piept schimbărilor și a face față cerințelor la locul de muncă bazate pe inteligență artificială, în timp ce angajații trebuie să achiziționeze noi abilități actualizate și să-și asume roluri provocatoare pentru a rămâne relevanți pe piața muncii.

Astfel, tendințele care se proiectează pe piața muncii bazată pe IA evidențiază importanța soft skill-urilor și ale hard skill-urilor în procesul de acomodare ale lucrătorilor și angajatorilor la noile condiții proiectate pe piața muncii de către sistemele de IA.

Soft skill-urile sunt abilități interpersonale, care ajută la adaptarea și interacționarea cu alte persoane. Printre cele mai importante se conturează comunicarea, empatia și creativitatea.

Comunicarea eficientă reprezintă un soft skill esențial, deoarece lucrătorii trebuie să poată să comunice eficient atât cu colegii, cât și cu clienții. Empatia, se prezintă la fel de necesară, deoarece lucrătorii care pot înțelege și pot relaționa cu clienții au șanse mai mari să reușească. Capacitatea de a gândi creativ și de a găsi soluții inovatoare în rezolvarea problemelor reprezintă un alt soft skill din ce în ce mai căutat pe piața muncii bazată pe inteligență artificială. Soft skill-urile sunt considerate trăsături de caracter sau abilități interpersonale, care ajută resursele umane să se adapteze, să interacționeze și să poată lucre în echipă.

Nu vom trece cu vederea și un alt soft skiil ce ține de managementul timpului, estimat de angajatori, care apreciază abilitatea angajaților de a gestional cât mai eficient timpul. Angajații trebuie să reușească să termine sarcinile în timpul programului de lucru.

Etica la locul de muncă - un soft skill care presupune integritate și profesionalism, responsabilitate în relațiile cu colegii și cu clienții, respectarea culturii organizaționale a companiei. Și atenția la detalii, constituie un soft skill de top, mult apreciat de angajatori, care poate ajuta la înlăturarea unor erori sau greșeli.

Spre deosebire de soft skill-uri, hard skill-urile sunt abilități tehnice măsurabile, vizibile, care se învață, cu alte cuvinte reprezintă competențe de care personalul are nevoie ca să-și desfășoare activitatea, aceste abilități țin de calificarea profesională și se cultivă prin practică.

Aceste două tipuri de aptitudini personale analizate, hard și soft, formează împreună competențele profesionale. Aptitudinile hard ajută la obținerea unui loc de muncă, iar cele soft – la menținea și păstrarea acestuia. Atunci când persoana intră pe piața muncii, de cele mai multe ori, își prezintă hard skill-urile, de aceea educația și formarea profesională se concentrează mai mult pe formarea acestor abilități. În acest sens, subliniem că în procesul de pregătire al specialiștilor se ignoră abilitățile soft, accentul fiind pus mai mult pe pregătirea specialității. În aceste condiții, persoanele prezintă hard skill-uri performante la angajare, dar faptul că nu tot timpul posedă un set necesar de abilități soft, chiar dacă sunt experți în profesia pe care o exercită, nu prea au șanse de a avansa în carieră, deoarece nu posedă competențe de relaționare.

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

În această ordine de idei, menționăm importanța ambelor tipuri de skill-uri, care reprezintă avantaje puternice pe piața muncii dominate de IA. În baza studiilor bazate pe sinteza materialelor publicate pe platforme online care intermediază angajare și recrutare în câmpul muncii, evidențiem cele mai semnificative avantaje ale skill-urilor pe piața muncii dominate de IA.

Avantajele posedării hard skill-urilor:

1) Competențe specializate: cunoașterea aptitudinilor hard permite obținerea de competențe specializate într-un domeniu specific, cum ar fi programarea, ingineria, contabilitatea.
2) Demnitate profesională: abilități tehnice și încredere în abordarea sarcinilor complexe.
3) Cerință pe piața muncii: candidații cu aptitudini hard sunt mai solicitați pe piața muncii, beneficiază de oportunități mai mari la angajare și avansare în carieră.
4) Precizie și eficiență: abilitățile hard asigură precizie și eficiență în realizarea sarcinilor, contribuind la rezolvarea problemelor, într-un mod concret și practic.

Avantajele cunoașterii soft skill-urilor:

1) Flexibilitate și adaptabilitate în fața schimbărilor și a cerințelor variate ale mediului de lucru;
2) Comunicarea eficientă facilitează relațiile interpersonale sănătoase și constructive;
3) Managementul conflictelor, aptitudinile soft dezvoltă abilități de gestionare a conflictelor, soluționare a problemelor, contribuind la un mediu de lucru armonios.

Potrivit sursei Global Manager.ro, cele mai căutate hard skill-uri pe piața muncii bazată pe inteligența artificială din România sunt: Computer skills (Outlook, Microsoft Word, Microsoft Excel, PowerPoint) - 88%; Limbaje de programare (Java, C++, Smalltalk, PHP, .NET) -41%; Cunoștințele de limbi străine – 41%, Project Management (Waterfall, Agile, SCRUM Methodology, Business analysis knowledge, certificari PMP, PRINCE etc.) – 29% [7].

Aceiași sursă citată relatează despre cele mai căutate competențe soft pe piața forței de muncă din România, după cum urmează: Capacitatea de adaptare la diferite sarcini şi de a găsi soluţii inovatoare – 59%; Abilitatea de a lucra în medii culturale diverse – 59%; Întelegerea sarcinilor și orientarea către rezultate – 41%; Agilitatea în învățare – 41%; Flexibilitatea cognitivă – abilitatea unei persoane de a se gândi la mai multe concepte simultan – 29%; Abilitatea de a acționa într-un mediu de business cu un nivel de previzibilitate mai scăzut – 29 % [7].

Potrivit unui studiu al ANOFM [1] angajatorii din Republica Moldova se confruntă cu lipsa competențelor necesare în rândul angajaţilor, factor ce influențează negativ activitatea agenților economici. Se reclamă lipsa următoarelor competențe profesionale:

a. Cunoştinţe şi competenţe profesionale specifice locului de muncă (hard skill);
b. Competenţe de a învăţa să înveţi (dorinţa de învăţa lucruri noi) (soft skill);
c. Competenţe lingvistice în limba maternă (abilitatea de a citi şi înţelege, precum şi de a scrie la un nivel relevant pentru locul de muncă) (soft skill);
d. Competențe digitale de operare a calculatorului pentru slujbaşi (hard skill);
e. Competenţe sociale şi civice (de comunicare şi lucru în echipă) pentru muncitori (soft skill).

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

Rezultatele studiului sugerează idea ca politicile educaționale și de formare din țara noastră ar trebui să se axeze și pe dezvoltarea competențelor, având în vedere cererea de competențe de pe piața muncii autohtone [1].

Deși utilizate pe larg în diferite sectoare ale economiei, sistemele de IA nu sunt reglementate adecvat, cu toate că la nivel global și regional se depun eforturi în acest sens. În condițiile evoluției accelerate a utilizării IA în economie la scară globală apare necesitatea adoptării unor măsuri și politici strategice privind evidențierea și valorificarea potențialului inovativ al IA, precum și gestionarea riscurilor pe care le comportă evoluția IA, fie sub formă de mecanisme juridice, standarde de bune practici, tratate obligatorii.

La nivelul statelor UE deja s-au întreprins și continua să se întreprindă măsuri de reglamentare a IA. Astfel, politicile și documentele strategice europene privind IA pe linia consolidării capacității tehnologice și industriale a UE, pregătirea pentru schimbările generate de IA, asigurarea unui cadru etic și juridic adecvat și urmărirea unei abordări unitare la nivelul UE se regăsesc în următoarele documente reglamentare la nivelul UE:

- Strategia europeană privind IA din aprilie 2018 (COM(2018)237)
- Inteligență artificială pentru Europa (SWD(2018)137)
- Cartea albă privind Inteligența Artificială (2020)
- Comunicarea CE privind datele, 2020 (COM (2020) 66)
- Planul coordonat privind inteligența artificială - AI Act din aprilie 2021
- Planul de acțiune pentru educația digitală 2021-2027 ((COM(2020) 0624)

În aceste documente, inteligența artificială este prezentată drept o dimensiune cheie care aduce beneficii în multe sectoare de activitate pe piața comunitară. În același timp, se subliniază că UE dorește să aibă pe piață sisteme de IA sigure și conforme cu legislația aplicabilă privind drepturile fundamentale și valorile UE.

În documentele la care ne-am referit mai sus, distingem îmbunătățirea și obținerea de noi competențe, care includ oportunități de formare, identificarea locurilor de muncă, elaborarea strategiilor naționale în materie de competențe, adaptarea cerințele și exigențelor viitoare în procesul de formare profesională („meserii ale viitorului”), cooperare între instituțiile de învățământ superior și cercetare-dezvoltare etc. Totodată, sunt concretizate sectoarele prioritare pentru adoptarea IA în statele UE: transporturile, asistența medicală și industria prelucrătoare. O importanță în creștere este acordată finanțării investițiilor în IA, începând cu introducerea domeniului în cadrul Programelor Orizont 2020 și Europa Digitală.

În aprilie 2021, Comisia Europeană a publicat propunerea de cadru juridic privind inteligența artificială, denumit la această etapă „Legea privind inteligența artificială”, aceasta stabilește aspectele inteligenței artificiale care trebuie să fie reglementate, categorisind practicile de inteligență artificială interzise, cum ar fi sistemele care manipulează persoanele prin tehnici subtile și influențează oamenii la nivelul subconștientului sau cele care utilizează tehnici de punctare a comportamentului social [4].

În Republica Moldova, IA este menționată doar în Strategia națională de dezvoltare „Moldova 2030”, aprobată de guvern în anul 2018, care prevede ca acțiune prioritară „elaborarea și adoptarea activă a tehnologiilor avansate (blockchain, inteligență artificială și algoritmi de învățare asistată de calculator) pentru a spori transparența, integritatea și trasabilitatea activității autorităților publice și managementului public, cu un accent special pe sistemul finanțelor publice, administrarea proprietății publice și achizițiile publice” [15]. Cu toate acestea, în țara noastră deja există un mediu favorabil pentru dezvoltarea și implementarea ecosistemelor inteligenței artificiale, chiar dacă nu este încă elaborată o

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

strategie națională în domeniul IA. Faptul că Moldova este pregătită pentru aplicarea IA se confirmă de către indexul produs de Oxford Insights [13], care clasează Moldova undeva la mijloc (locul 80 din 171 de ţări). Indexul se bazează pe trei piloni: (1) guvernul; (2) datele și infrastructura și (3) sectorul tehnologiei. În cadrul fiecărui pilon, indexul evaluează existența condiţiilor favorabile pentru inteligența artificială, cum ar fi disponibilitatea datelor, a infrastructurii pentru capabilităţi digitale sau a capitalului uman [13].

CONCLUZII

Impactul IA asupra pieții muncii este incontestabil, pe de o parte produce provocări și presiuni pe piața muncii, iar pe de altă parte, prezintă oportunități pentru persoanele aflate în căutarea unui loc de muncă și angajatorii dispuși să se adapteze. Reușita de a rezita la schimbările ce intervi rezultă din flexibilitatea angajților și angajatorilor de a fi capabili să-și actualizeze continuu abilitățile și să îmbrățișeze cele mai noi tehnologii. Totodată, angajatorii trebuie să investească în formarea angajaților, pentru a se asigura că au abilitățile necesare pentru a prospera la locul de muncă bazat pe inteligență artificială.

IA are un impact transformator asupra pieții muncii prin automatizarea proceselor, îmbunătățirea procesului decizional și deschiderea de noi oportunități într-o varietate de industrii. Automatizarea contribuie la creșterea productivității, dar comportă dezavantaje, inclusiv pierderea locurilor de muncă de către indivizii, care nu sunt dispuși sau nu pot să se adapteze. Îmbunătățirea competențelor și îmbrățișarea noilor responsabilități pe care IA le oferă este o cerință înaintată lucrătorilor care doresc să se adapteze.

Întrucât, IA promovează inovația, persoanele au nevoie de abilități tehnice (hard skill) și abilități soft (soft skill) pentru a reuși în profesie, deoarece, succesul într-o economie bazată pe inteligență artificială necesită atât perfecționare, cât și recalificare. Pentru a reuși pe o piață a forței de muncă în schimbare, programele de formare și dezvoltarea competențelor soft sunt esențiale.

Vom puncta efectele utilizării pe larg a sistemelor de inteligență artificială în toate ramurile asupra pieții muncii:

1. IA influențează semnificativ modul în care angajații desfășoară activitatea profesională. Mașinile și software-urile alimentate de IA înlocuiesc munca manuală în diverse industrii, determinând scăderea anumitor oportunități de muncă. Are loc schimbarea de sarcini. Această tendință se menține pe măsură ce IA devine mai sofisticată și capabilă.
2. Se formează o cerere crescută pentru profesioniști cu expertiză în IA și domenii conexe (învățarea automata, știința datelor).
3. IA îmbunătățește capacitatea de muncă umană și productivitatea, datorită faptului că poate oferi informații valoroase și asista procesele decizionale.
4. Are loc înlocuirea locurilor de muncă, eliminarea celor vechi și apariția altor noi. Pentru a suporta această presiune este necesar ca indivizii să se adapteze la schimbările de pe piața muncii prin dobândirea de noi abilități și să accepte învățarea continuă pe tot parcursul vieții. Guvernele și organizațiile ar trebui, de asemenea, să investească în programe de reantrenare și să creeze un mediu care susține tranziția către o economie condusă de IA.
5. Apar unele comprimări ale pieţei muncii și a gradului de ocupare, deoarece sunt necesare alte abilităţi şi performanţe profesionale ale lucrătorilor şi o flexibilitate mult mai mare a managementului organizațiilor.

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chișinău, Moldova

6. IA redefinește spațiile sau mediile de lucru, care necesită un grad înalt de alfabetizare digitală a populației.
7. S-a observat că există o legătură între procesul de utilizare largă a IA şi gradul de ocupare. Pe de o parte, inovarea de proces poate conduce la reducerea locurilor de muncă pe seama creşterii productivităţii, iar pe de altă parte, inovarea de produs conduce la un efect invers – nevoia de noi locuri de muncă, această situație se explică prin faptul că noile produse implică o diversificare și o creștere a producției, respectiv și a cererii. Astfel, putem considera că șomajul cunoaşte fluctuaţii mai mari sau mai mici, în dependență de inovațiile tehnologice utilizate, deoarece lansarea de noi produse determină creșterea numărului de consumatori, și respectiv a numărului locurilor de muncă din ce în ce mai calificate.

Suntem încă la o fază incipientă pentru a înțelege potențialul și impactul IA asupra economiei în întregime, precum și asupra pieții muncii. Considerăm oportun promovarea unui dialog social între toate părțile implicate – cercetători, factori de decizie, reprezentanți ai mediului de afaceri, reprezentanți ai sindicatelor, politicieni privind beneficiile, oportunitățile, dar și amenințările IA.

Cel puțin, societatea nu trebuie să aibă o atitudine pasivă față de IA, pentru că viteza cu care avansează tehnologia provoacă perturbări semnificative pe piața muncii, dar și la nivel de societate în întregime.

BIBLIOGRAFIE

1. ANOFM. *Prognoza pieței muncii pentru anul 2022 din perspectiva angajatorilor* [online]. [citat: 12 noiembrie 2023] Disponibil: <https://anofm.md/view_document?nid=19888>
2. AUTOR, David & SALOMONS, Anna. *Is Automation Labor-Displacing? Productivity Growth, Employment, and the Labor Share* [online]. In: BPEA Conference Drafts. 2018, No. 6. [citat: 18 noiembrie 2023]. Disponibil: <https://www.brookings.edu/wp-content/uploads/2018/03/1_autorsalomons.pdf>
3. Cadrul strategic național în domeniul inteligenței artificiale din România 2023-2027 [online]. [citat: 12 noiembrie 2023]. Disponibil: <https://www.mcid.gov.ro/wp-content/uploads/2023/10/Propunere-Cadru-Strategic-National-IA-.pdf>
4. COMISIA EUROPEANĂ, Propunere de Regulament al Parlamentului European și al Consiliului de stabilire a unor norme armonizate privind inteligența artificială (Legea privind inteligența artificială) și de modificare a anumitor acte legislative ale uniunii (2021) [online]. [citat: 10 noiembrie 2023]. Disponibil: < https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A52021PC0206>
5. Dicționarul explicativ al limbii române [online]. [citat: 10 noiembrie 2023]. Disponibil: <https://dexonline.ro/>
6. GASNAȘ, A., GLOBA, A. *Rolul inteligenței artificiale în educație* [online]. În: Acta et Commentationes. Sciences of Education. 2023, Nr. 2(32), pp. 46-57
7. GlobalManger.ro. [online]. [citat: 12 noiembrie 2023]. Disponibil: <https://www.globalmanager.ro/>
8. GOMEDE, E. et al. *Application of computational intelligence to improve education in smart cities* [online]. In: Sensors (Switzerland), 2018. no. 18(1), pp. 1–26. [citat: 14 noiembrie 2023]. Disponibil: <https://doi.org/10.3390/s18010267>

DOI: https://doi.org/10.53486/escst2023.02
International Conference, December 07-08, 2023, Chişinău, Moldova

9. JONES, Charles & Romer, Paul. *The New Kaldor Facts: Ideas, Institutions, population, and Human Capital*. In: American Economic Journal: Macroeconomics. 2010, No. 2.
10. McKINSEY. *Cum ne raportăm la piața muncii în epoca inteligenței artificiale : studiu* [online]. [citat: 19 noiembrie 2023]. Disponibil: <https://portalhr.ro/studiu-mckinsey-cum-ne-raportam-la-piata-muncii-in-epoca-inteligentei-artificiale/>
11. MULCAHY, Diane. *The Gig Economy*. AMACOM, 2016. 240 p. ISBN 9780814437339.
12. NILSSON N. J. *The Quest for Artificial Intelligence: A History of Ideas and Achievements*. Cambridge: Cambridge University Press, 2010.
13. OXFORD INSIGHTS. *Government AI Readiness Index 2020* [online]. [citat: 18 noiembrie 2023]. Disponibil: < https://www.oxfordinsights.com/government-ai-readiness-index-2020>
14. PETROPOULOS, G. *The impact of artificial intelligence on employment* [online]. [citat: 15 noiembrie 2023]. Disponibil: <https://www.bruegel.org/sites/default/files/wp-content/uploads/2018/07/Impact-of-AI-Petroupoulos.pdf>
15. Strategia naţională de dezvoltare „Moldova 2030" [online]. [citat: 10 noiembrie 2023] Disponibil: <https://gov.md/ro/moldova2030>
16. Strategia de transformare digitală a Republicii Moldova pentru anii 2023–2030 (STDM 2030) [online]. [citat: 10 noiembrie 2023]. Disponibil: <https://cancelaria.gov.md/sites/default/files/document/attachments/nu-300-mded-2023.pdf>
17. *The ECONOMIC potential generative AI: The next productivite frontier* [online]. [citat: 17 noiembrie 2023]. Disponibil: <https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier#introduction>
18. *The Impact of Artificial Intelligence on the Job Market: 5 Key Trends* [online]. [citat: 14 noiembrie 2023] Disponibil: <https://www.linkedin.com/pulse/impact-artificial-intelligence-job-market-5-key-trends>
19. WINSTON, Patrick Henry. *Artificial Intelligence*. 3rd ed. Addison-Wesley, 1992. ISBN 9780201533774.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.03
International Conference, December 07-08, 2023, Chișinău, Moldova

IMPACTUL SCHIMBĂRILOR DEMOGRAFICE ASUPRA SECURITĂȚII ECONOMICE A REPUBLICII MOLDOVA

THE IMPACT OF DEMOGRAPHIC CHANGES ON THE ECONOMIC SECURITY OF THE REPUBLIC OF MOLDOVA

Marina COBAN

PhD, Associate professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0009-0005-1984-9682
E-mail:mcoban.mcoban@gmail.com

Abstract: *This article presents changes in the demographic sphere of the Republic of Moldova, their impact on the economic security of the country as a whole. The most serious threat to the country's economic security is that as the population structure changes as the workforce shrinks (a shrinking and aging population) and welfare costs increase for needy citizens, the economy may slow. The Republic of Moldova at this stage is experiencing problems in the demographic sphere, which reduces the level of economic security. The article presented the main trends in the demographic sphere and their impact on the economic security of the country. Statistical indicators of demographic processes in the Republic of Moldova were analyzed, and conclusions were drawn that in the Republic of Moldova there is a trend towards a decrease in the birth rate, population size, an increase in mortality, and an increase in emigration , which reduces the level of economic development. In this regard, it is necessary to take effective measures to improve the level and quality of life of the population of the Republic of Moldova.*

Keywords: *demographic situation, demographic trends, demographic indicators, fertility, mortality, depopulation.*

UDC: *314.18:338.24(478)*

JEL Classification: *J11.*

INTRODUCERE

Situația demografică este un factor important în dezvoltarea oricărei țări, deoarece problemele din acest domeniu pot afecta semnificativ economia în ansamblu, piața muncii, sistemul de pensii și sfera socială din orice țară. Fertilitatea, mortalitatea, schimbările demografice, compoziția societății, îmbătrânirea și migrația sunt importante pentru înțelegerea modului în care un guvern ar trebui să utilizeze resursele limitate cel mai eficient din perspectivă economică.

În ultimii ani, procesele demografice au trezit un interes sporit în rândul oamenilor de știință, deoarece, pe de o parte, natalitatea țării este sub nivelul de înlocuire, pe de altă parte, speranța de viață a crescut și continuă să crească - un fenomen numit „societate de îmbătrânire”. Toate acestea afectează reducerea resurselor de muncă din țară, ceea ce reprezintă o amenințare la adresa securității economice. Prin urmare, rezolvarea problemelor demografice este de importanță majoră.

Scopul cercetării a fost de a analiza principalele tendințe din sfera demografică Republicii Moldova. Pentru a atinge acest obiectiv, au fost analizați indicatorii demografici ai Republicii Moldova în ultimii ani, au fost identificate problemele și formulate concluzii cu privire la rezolvarea acestor probleme.

Pentru a analiza sfera demografică a Republicii Moldova, am selectat următorii indicatori: dinamica populației, dinamica fertilității și mortalității, creșterea naturală a populației și declinul, dinamica migrației internaționale, dinamica structurii populației,

DOI: https://doi.org/10.53486/escst2023.03
International Conference, December 07-08, 2023, Chișinău, Moldova

dinamica căsătoriilor și divorțurilor, speranța de viață la naștere în Republica Moldova, și în unele țări dezvoltate.

ANALIZA ȘI INTERPRETAREA REZULTATELOR

Factorul demografic este unul dintre factorii cheie în asigurarea securității economice a țării. Populația nu este niciodată statică; ea crește sau se contractă ca urmare a interacțiunii dintre fertilitate, mortalitate și migrație. Înțelegerea cauzelor și consecințelor dinamicii demografice a populației și prognoza acesteia ne permit să fie luate deciziile corecte în dezvoltarea socio-economică a țării.

Procesele demografice sunt influențate de șocuri economice, evenimente politice, crizelor de guvernare, schimbări în viziunea asupra lumii (de exemplu, unul dintre motivele scăderii natalității este că cetățenii abandonează copiii pentru că preferă cariera), creștere și bunăstare materială.

Țările pot avea diverse aspecte ale securității demografice. Principalele amenințări demografice pot fi sistematizate astfel: dimensiunea populației, distribuția populației, structura populației, mișcarea naturală a populației, mișcarea migrațională a populației, reproducerea populației.

Dimensiunea populației include astfel de indicatori ca:
- depopularea;
- creșterea excesivă a numărului de locuitori;
- densitate mică sau mare a populației etc.

Distribuția populației se caracterizează prin:
- disproporționalitatea distribuției teritoriale a rezidenților;
- discrepanța între distribuția efectivă a populației și obiectivele strategice ale dezvoltării socio-economice a statului;
- atenuarea și micșorarea populației rurale etc.

Structura populației se referă la:
- îmbătrânirea populației;
- disproporționalitatea componenței pe sexe a populației;
- modificări negative în componența familiilor;
- schimbarea proporţiilor etnice (rasiale, naţionale, religioase şi lingvistice) ale populaţiei etc.

Mișcarea naturală a populației se poate caracteriza prin:
- natalitatea scăzută sau excesiv de mare a populației;
- rata mare de mortalitate;
- creşterea (scăderea) naturală negativă a populaţiei;
- creşterea ratei divorţurilor a populaţiei etc.

Mișcarea migrațională a populației include astfel de indicatori ca:
- ieșirea rezidenților în alte regiuni sau în afara țării;
- afluxul excesiv de migranți;
- migrația ilegală;
- creșterea (scăderea) migrației populației;
- fluxurile de migraţie internă nu corespund obiectivelor strategice ale dezvoltării socio-economice a statului etc.

Reproducerea populației se poate caracteriza prin:
- speranța de viață scăzută a populației;
- pierderi mari în reproducerea populaţiei din cauza mortalităţii etc.

DOI: https://doi.org/10.53486/escst2023.03
International Conference, December 07-08, 2023, Chișinău, Moldova

Securitatea demografică a oricărei țări din lume este determinată nu numai de procesele demografice care au loc în aceasta, ci și de procesele demografice care au loc în afara granițelor acesteia (în statele, regiunile învecinate etc.).

Influența demografiei asupra securității economice a unei țări se exprimă în următoarele trei aspecte principale:

În primul rând, situația demografică afectează semnificativ oferta de muncă.

În al doilea rând, demografia influențează consumul de bunuri și servicii de către populație, datorită influenței sale asupra formării cererii în sectoarele de alimente interne și de import.

În al treilea rând, o scădere a populației în vârstă de muncă duce la cote mai mari atât ale impozitelor, cât și ale contribuțiilor de asigurări sociale (pentru a oferi beneficii sociale și plăți de pensii). Ca urmare, pe măsură ce ratele cresc, costul bunurilor și serviciilor crește, competitivitatea produselor interne scade, iar cotele de impozitare ridicate reduc stimulentele de a munci și, în consecință, încetinesc creșterea economică.

Se remarcă impactul problemelor din sfera demografică asupra structurii societății: cu o penurie de muncitori, țările trebuie să crească migrația, migranți din alte țări, care înlocuiește populația indigenă și care poate provoca probleme interculturale, interetnice.

De aceea trebuie rezolvate problemele demografice. Politica demografică are ca scop reglarea și stimularea creșterii naturale și a migrației și a speranței de viață a populației, ținând cont de necesitatea îmbunătățirii calității vieții.

În unele cercetări se remarcă scăderea populației în majoritatea țărilor din Europa Centrală și de Est, atât din cauza scăderii fertilității, cât și în urma migrației (Fihel, Okólski, 2019). Republica Moldova este una din cele mai afectate țări din regiune, populația căreia, către anul 2050, poate să se micșoreze cu 44,2%, cauza principală fiind migrația în masă. Conform prognozelor demografice elaborate de Centrul de Cercetări Demografice pentru anii 2019-2040 în baza datelor cu privire la populația cu reședința obișnuită a Republicii Moldova în deceniile viitoare declinul demografic va continua cu ritmuri rapide, scăderea anuală, conform scenariului scăzut, se va majora de la 1,6% până la 2,3%, numărul populației micșorându-se până la 1754,6 mii (cu 34,5%) către anul 2040 [1].

Vom analiza unii indicatori a schimbărilor demografice în Republica Moldova.

Numărul preliminar al populaţiei cu reşedinţa obişnuită

Numărul preliminar al populaţiei cu reşedinţa obişnuită în Republica Moldova, la 1 ianuarie 2023, a constituit 2,5 milioane persoane, în scădere cu 52,3 mii persoane (sau cu 2,0% faţă de începutul anului precedent), ceea ce confirmă o tendinţă clară de micşorare a efectivului populaţiei [4].

Tabelul 1. Populaţia cu reşedinţa obişnuită în Republica Moldova, la 1 ianuarie

	2020	2021	2022	2023
Total populaţie, persoane, mii inclusiv pe grupe de vârstă, în %:	2643,7	2626,6	2565,0	2512,8
0-14	18,5	18,4	18,3	18,1
15-59	59,8	59,3	58,7	58,1
60-79	19,3	20,0	20,6	21,4
80+	2,4	2,3	2,4	2,4

Sursă: Biroul Național de statistică https://statistica.gov.md/

DOI: https://doi.org/10.53486/escst2023.03
International Conference, December 07-08, 2023, Chişinău, Moldova

Până în 2018, scăderea naturală a populaţiei a fost nesemnificativă. Începând cu 2018, numărul deceselor a depăşit numărul născuţilor-vii, diferenţa majorându-se până în 2021, ajungând la 16,1 mii persoane, iar în 2022, aceasta s-a redus la 9,2 mii de persoane [4].

Migraţia netă (diferenţa dintre imigranţi şi emigranţi) rămâne negativă. În anul 2022, au ieşit din ţara cu 43 mii de persoane mai mult, decât au venit, faţă de 45 mii în anul 2021 [4].

Tendinţa de reducere a populaţiei ţării s-a păstrat şi în anul 2022. Factorii care au influenţat declinul populaţiei au fost atât migraţia internaţională, cât şi sporul natural negativ al populaţiei .

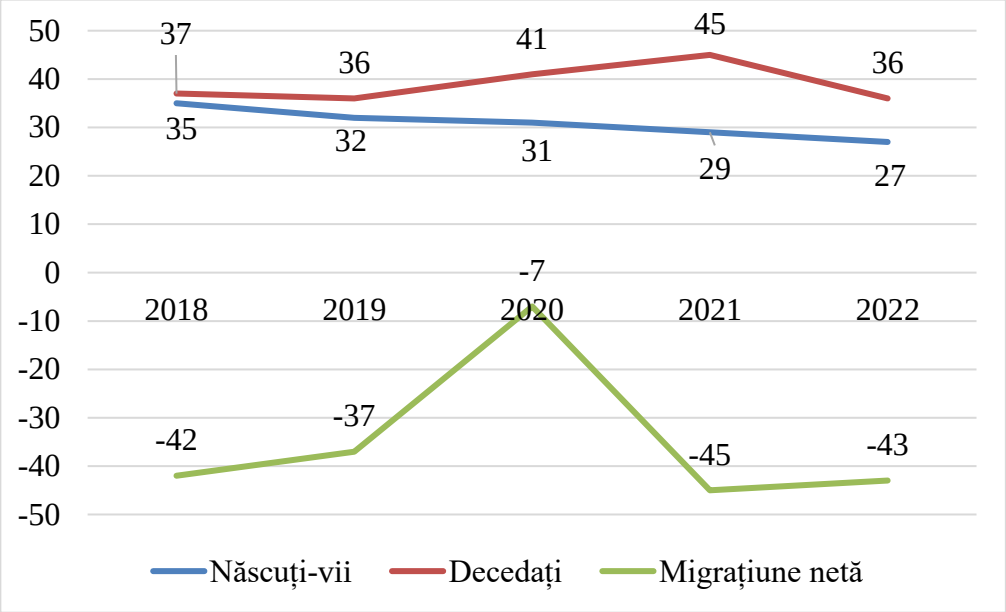


Figura 1. Tendințe demografice, mii persoane
Sursă: Moldova în cifre https://statistica.gov.md

Mişcarea naturală

În 2022, în Republica Moldova s-au născut 27,0 mii copii, fiind în descreştere cu 2,4 mii copii (sau cu 8,1%) faţă de anul 2021. Numărul mediu de copii per femeie de vârstă fertilă, în 2022 a constituit 1,69, fiind în scădere faţă de anul 2018, unde valoarea a fost de 1,78 copii per femeie[4].

Numărul femeilor de vârstă fertilă (15-49 de ani) a fost în continuă scădere, cu 142 mii în ultimii 9 ani.

În anul 2022 s-a înregistrat cel mai mic număr de decese comparativ cu ultimii ani, fiind în descreştere cu 9305 persoane (20,5%) faţă de anul precedent.

In anul 2022 s-au înregistrat 18157 căsătorii şi 9565 divorţuri, din total cupluri căsătorite, 52,6% divorţează [4].

DOI: https://doi.org/10.53486/escst2023.03
International Conference, December 07-08, 2023, Chișinău, Moldova

Tabelul 2. Indicatori demografici

	2019	2020	2021	2022
Speranța de viață la naștere, ani				
bărbați	66,8	66,0	65,2	67,2
femei	75,2	73,9	73,0	75,7
Rata totală de fertilitate, per femeie	1,78	1,76	1,75	1,69
Vârsta medie la prima căsătorie, ani				
bărbați	28,9	27,8	29,4	29,4
femei	26,0	25,4	25,5	26,4
Căsătorii, la 1000 locuitori	7,6	5,9	7,8	7,2
Divorțuri, la 1000 locuitori	4,0	3,3	3,8	3,8
Născuți-vii, la 1000 locuitori	12,2	11,7	11,3	10,6
Decedați, la 1000 locuitori	13,7	15,4	17,5	14,2
Mortalitatea infantile, la 1000 născuți-vii	8,4	8,7	8,5	9,0
Mortalitatea copiilor sub 5 ani, la 1000 născuți-vii	9,9	10,4	9,8	10,3

Source: Moldova în cifre https://statistica.gov.md

Populația vârstnică

Numărul persoanelor vârstnice (60 ani şi peste) la 100 locuitori din Moldova înregistrează o tendinţă de creştere continuă de la an la an. Populația vârstnică crește atât în termeni absoluți, cât și relativi.

În Republica Moldova, la începutul anului 2023 locuiau 598,3 mii de persoane în vârstă de 60 ani şi peste, ceea ce constituie 23,8% din totalul populației cu reședință obișnuită. Din numărul total al vârstnicilor, 359,7 mii de persoane erau femei (sau 60,1%), fiecare a treia persoană avea vârsta cuprinsă între 60-64 ani (32,6%) (figura 3). Ponderea persoanelor în vârstă de peste 60 ani este în creştere continuă. În ultimii cinci ani a crescut cel mai mult ponderea vârstnicilor din grupul de vârstă de 70-74 de ani – cu 8,5 puncte procentuale (de la 13,6%, la începutul anului 2019 până la 22,1% la începutul anului 2023) [7].

DOI: https://doi.org/10.53486/escst2023.03
International Conference, December 07-08, 2023, Chişinău, Moldova

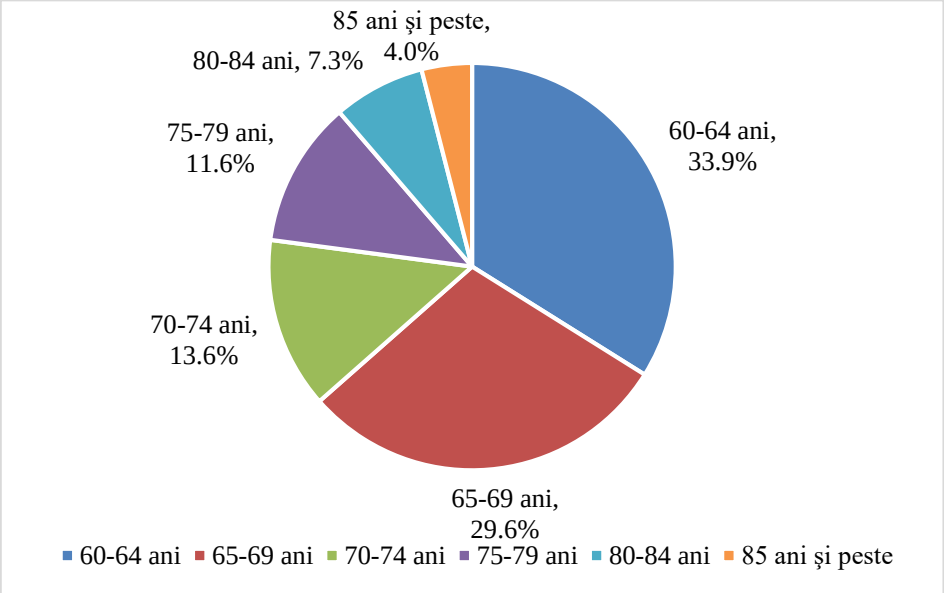


Figura 2. Populația vârstnică pe grupe de vârstă, la 1 ianuarie 2019

Source: Biroul Național de statistică https://statistica.gov.md/

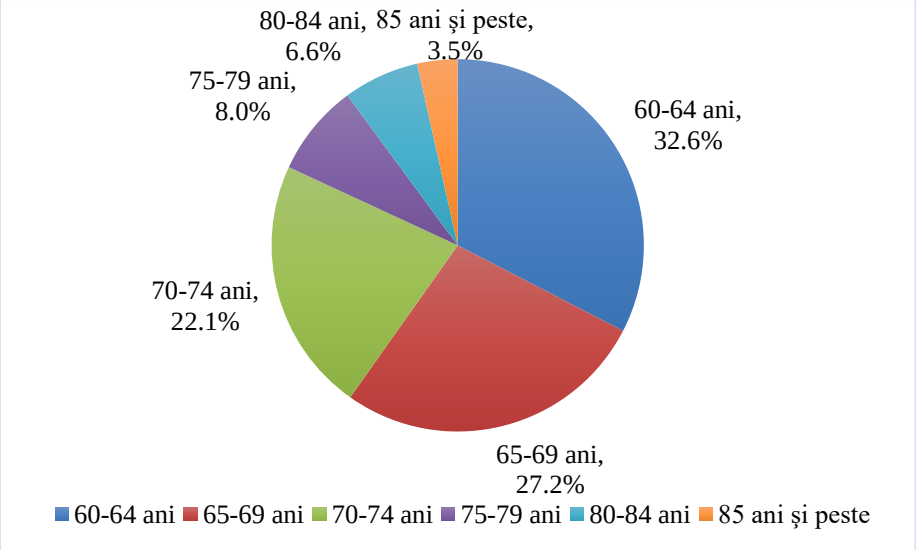


Figura 3. Populația vârstnică pe grupe de vârstă, la 1 ianuarie 2023

Source: Biroul Național de statistică https://statistica.gov.md/

Coeficientul de îmbătrânire al populaţiei

La începutul anului 2023, coeficientul de îmbătrânire a populaţiei (numărul persoanelor în vârstă de 60 ani și peste la 100 locuitori) a constituit 23,8%, ceea ce corespunde unui nivel înalt de îmbătrânire demografică. Comparativ cu începutul anului 2019 acesta a înregistrat o majorare cu 3,0 puncte procentuale.

Diferenţe se constată şi în repartizarea pe sexe, coeficientul îmbătrânirii populației feminine la începutul anului 2023 fiind cu 7,0 puncte procentuale mai înalt față de cel al bărbaților și a constituit 27,1% comparativ cu 20,1% în cazul bărbaților [7].

.

DOI: https://doi.org/10.53486/escst2023.03
International Conference, December 07-08, 2023, Chișinău, Moldova

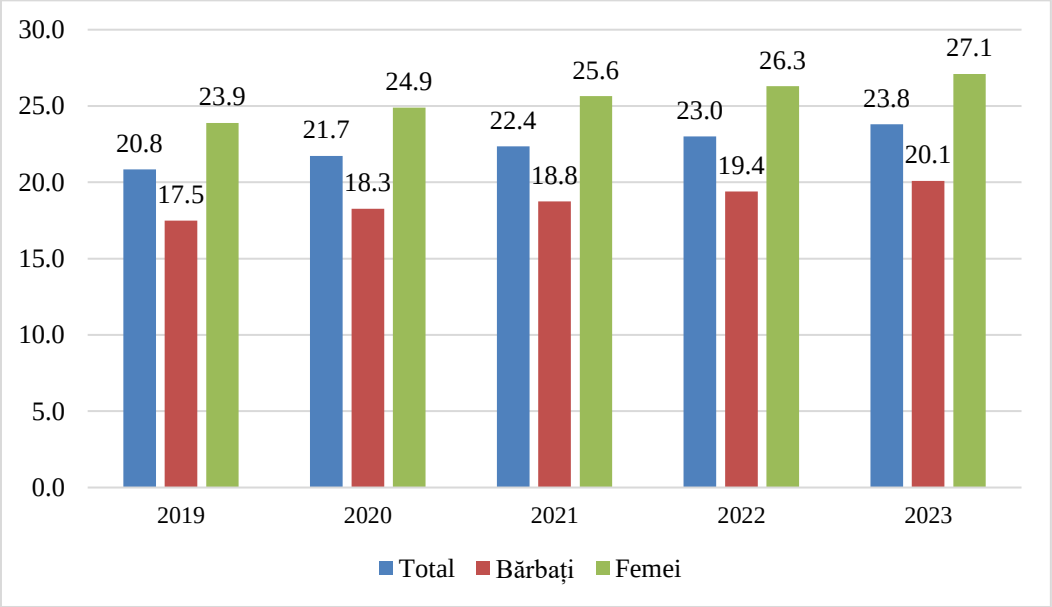


Figura 4.Coeficientul de îmbătrânire al populaţiei pe sexe, la 1 ianuarie 2023
Source: Biroul Național de statistică https://statistica.gov.md/

Migrația internațională

Migrația netă a populației (diferența dintre numărul de imigranți și cel al emigranților) cu reședința obișnuită, în anul 2021, a urmat tendința descrescătoare din ultimii ani, înregistrând o valoare negativă, de (-45,4) mii persoane. Din totalul emigranților, ponderea cea mai mare, de circa 44%, o dețin persoanele tinere din grupele de vârstă 20-29 de ani și 30-39 de ani, cu 23% și, respectiv, 21%. În cazul imigranților, cea mai mare pondere, de circa 40% din total, o dețin grupele de vârstă 30-39 ani cu 22% și, respectiv, 40-49 de ani cu 18%. (Figura 5) [6].

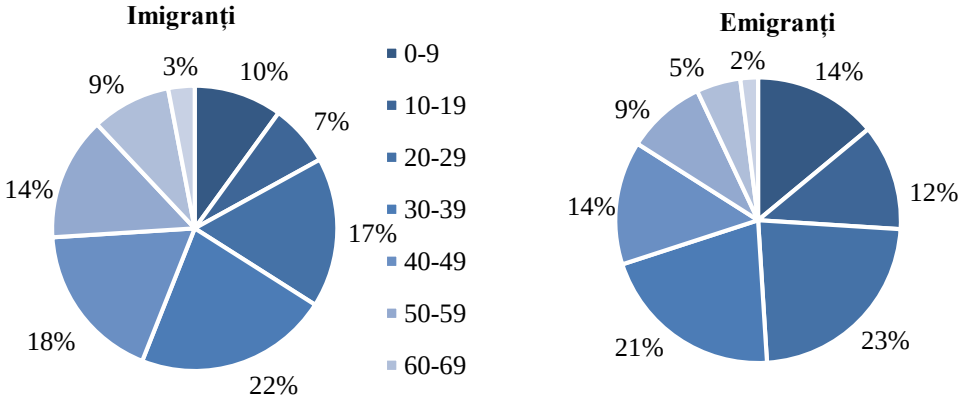


Figura 5. Disribuția imigranților și emigranților pe grupe de vârstă în anul 2021
Source: Biroul Național de statistică https://statistica.gov.md/

DOI: https://doi.org/10.53486/escst2023.03
International Conference, December 07-08, 2023, Chișinău, Moldova

Moldova în prezent se confruntă cu al treilea val de migrație: migrația tinerilor. Primul val a fost în anii 2000-2005, când cetățenii Republicii Moldova plecau peste hotare să-și rezolve problema de supraviețuire [4]. Al doilea val a fost în perioada 2015-2018, valul pentru o viața mai bună. Acești oameni nu mai erau într-o sărăcie extremă, aveau venituri satisfăcătoare, majoritatea de vârsta 30-45 ani, oameni formați, cu familii, dar au plecat pentru o viață mai bună, calitativă. Acolo unde pe lângă salarii bune mai ai și drumuri, școli, spitale, infrastructură. Într-un cuvânt bunăstare oferită de autorități [4]. După 2018 a început al treilea val de migrație a tinerilor care pleacă la studii.

CONCLUZII

În general, pentru îmbunătățirea indicatorilor demografici, este importantă creșterea ponderii celor mai productive grupe de vârstă și reducerea ponderii populației incapabile de muncă. Pentru a atenua consecințele îmbătrânirii populației și a prelungi anii sănătoși ai vieții oamenilor, este necesar să se dezvolte sistemul de sănătate publică, să se producă noi medicamente care încetinesc procesul de îmbătrânire și să prelungească anii sănătoși ai vieții oamenilor.

Pentru o creștere naturală a populației, este importantă îmbunătățirea calității vieții populației.Pentru a îmbunătăți procesele de migrație, este necesar să se creeze condiții pentru o viață modernă și confortabilă și să se reducă tensiunea socială.

Deci sunt necesare măsuri în domeniul politicilor demografice și de migrație. Este necesară îmbunătățirea cadrului legislativ legat de demografie, îmbunătățirea sistemului de sănătate, stimularea creșterii natalității și a populației, îmbunătățirea condițiilor de viață pentru familiile tinere, i.e. îmbunătățește în general calitatea vieții populației.

BIBLIOGRAFIE

1. FIHEL, A., OKÓLSKI, M. Population decline in the post-communist countries of the European Union. *Le bulletin Population & Societies*. 2019, nr. 567, 1-4.
2. GAGAUZ, O. Depopularea Republicii Moldova în contextul declinului populației din Europa Centrală și de Est. In: *Creşterea economică în condiţiile globalizării.* Ed. 15, 15-16 octombrie 2021. Chișinău: Foxtrot SRL, 2021, pp. 6-11.
3. IONIȚĂ, V. *Analize, Comentarii, Opinii. Migrația. Al III-lea val: Migrația Tinerilor* [online]. Chișinău, 2023 [accesat 18 decembrie 2023]. Disponibil: <https://ionita.md/2023/07/21/migratia-al-iii-lea-val-migratia-tinerilor/>.
4. *Moldova în cifre: Breviar statistic* [online]. Chișinău, 2023 [accesat 19 decembrie 2023]. Disponibil: <https://statistica.gov.md>.
5. Numărul populației cu reședință obișnuită, pe sexe și grupe de vârstă, în profil teritorial la 1 ianuarie 2023. In: *Biroul Național de Statistică al Republicii Moldova* [online]. Chișinău, 2023 [accesat 19 decembrie 2023]. Disponibil: <https://statistica.gov.md/ro/>.
6. Situația demografică în anul 2022. In: *Biroul Național de Statistică al Republicii Moldova* [online]. Chișinău, 2023 [accesat 19 decembrie 2023]. Disponibil: <https://statistica.gov.md/ro/>.
7. Vârstnicii în Republica Moldova în anul 2022. In: *Biroul Național de Statistică al Republicii Moldova* [online]. Chișinău, 2023 [accesat 19 decembrie 2023]. Disponibil: <https://statistica.gov.md/ro/varstnicii-in-republica-moldova-in-anul-2022-9578_60729.html>.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.04
International Conference, December 07-08, 2023, Chișinău, Moldova

SECURITATEA ECONOMICĂ DURABILĂ PRIN INOVAȚII: UN MODEL INTEGRAT PENTRU REPUBLICA MOLDOVA

THE SUSTAINABLE ECONOMIC SECURITY THROUGH INNOVATIONS: AN INTEGRATED MODEL FOR THE REPUBLIC OF MOLDOVA

Boris COREȚCHI

PhD, Associate professor,
Moldova State University, Moldova,
ORCID 0000-0001-8841-4838
E-mail: boris.coretchi@usm.md

Abstract: *This paper holds paramount importance as it presents a pioneering approach to economic development and state security through an economic-mathematical model. Focused on the Republic of Moldova, the author delves into the intricate interplay between innovation, economic progress, and economic security. The paper aims to establish a comprehensive model that integrates these elements, offering a holistic vision for efficient management and the enhancement of economic competitiveness. The originality of this work lies in its thorough analysis of the connections between innovation, economic progress, and economic security specific to the Republic of Moldova. The author introduces an economic-mathematical model, emphasizing the significance of information technologies and scientific leadership in fortifying economic security. Notably, the paper utilizes a fuzzy model based on real data, providing personalized strategies for sustainable economic growth and long-term security.In summary, the integrated model underscores the critical role of adopting and implementing information technologies, equipping institutions with advanced technology, leveraging scientific achievements, and implementing effective personnel policies. These elements are identified as crucial for consolidating the economic security of the Republic of Moldova. The promotion of these key factors is highlighted as a substantial contribution to bolstering institutional effectiveness in the face of economic and security challenges, ultimately supporting sustainable economic growth and ensuring the long-term security of the country.*

Keywords**:** *economic development, economic security, economic-mathematical model, innovation, impact factors, economic security management, information technologies.*

UDC: *[338.1:001.895]:330.4(478)*

JEL Classification: *O11, O21, O32, C02, Q01.*

INTRODUCERE

În lumina schimbărilor rapide la nivel global, acest articol propune un model economico-matematic inovator pentru analiza interdependențelor dintre inovație, progres economic și securitatea economică în Republica Moldova. Prin referiri la literatura de specialitate și sintetizarea cunoștințelor actuale despre subiect, se conturează contextul pentru investigarea acestor aspecte cheie.

Scopul lucrării constă în formularea unui cadru conceptual și practic pentru elaborarea de strategii personalizate și durabile menite să consolideze securitatea economică a Republicii Moldova într-un mediu global dinamic și competitiv. Acest obiectiv este exprimat prin intermediul ipotezelor și întrebărilor referitoare la interacțiunile complexe dintre inovație și securitatea economică.

DOI: https://doi.org/10.53486/escst2023.04
International Conference, December 07-08, 2023, Chișinău, Moldova

Pentru atingerea acestui scop, lucrarea adoptă o abordare metodologică ce include utilizarea unui model de concluzii fuzzy și a programării matematice. Analiza detaliată pune în evidență importanța unor factori cheie precum securitatea financiară, fiscală, socială și tehnologiile informaționale în consolidarea securității economice a Republicii Moldova.

Rezultatele relevate de studiu, susținute de metode economice și matematice, demonstrează că adoptarea tehnologiilor informaționale, echiparea instituțiilor, realizările științifice și o politică de personal eficientă sunt esențiale pentru întărirea securității economice. Implementarea strategiilor personalizate și durabile, conform modelului propus, poate contribui semnificativ la promovarea unei creșteri economice durabile și asigurarea securității pe termen lung a Republicii Moldova.

CONSOLIDAREA SECURITĂȚII ECONOMICE DURABILE PRIN INOVAȚII

Procesul de dezvoltare economică și inovație este intrinsec complex și influențat de o varietate de factori interdependenți. În cadrul acestui context, securitatea economică devine o preocupare majoră, iar abordarea gestionării acesteia necesită o analiză detaliată a interacțiunilor dintre diverși parametri. Pentru o gestiune eficientă a impactului factorilor asupra dezvoltării economice și a securității statului, se propune aplicarea unui model economico-matematic, cât și la alte informații relevante.

Abordarea comprehensivă și orientată către dezvoltare din această perspectivă presupune adoptarea unei viziuni holistice asupra interdependențelor dintre inovație, progres economic și securitate economică [1]. Este important să identificăm și să evaluăm cu atenție factorii care pot influența asupra acestor domenii, astfel încât să putem elabora strategii eficiente pentru promovarea competitivității economiei naționale.

Modelarea repercusiunilor factorilor devine astfel un instrument fundamental în înțelegerea dinamicii acestor interdependențe. Prin utilizarea schemei-bloc analitice și a indicatorilor corespunzători, statul poate evalua pericolele și oportunitățile asociate cu diverse aspecte ale progresului economic, inclusiv impactul inovațiilor [2]. Această abordare integratoare facilitează elaborarea unor strategii personalizate și durabile care să întărească securitatea economică a Republicii Moldova [3].

În continuare vom nota convențional toate mărimile fundamentale și a constantelor. În vederea modelării, vom desemna în mod obișnuit factorii de impact F_1, F_2, F_3, F_4. Deoarece în realitate, securitatea economică a unei țări este afectată de o multitudine de factori, îi vom reprezenta convențional ca F_n. Inovațiile reprezintă în sine unul dintre acești factori care influențează performanța securității economice. Așa cum am menționat anterior, inovațiile depind și de alți factori, astfel încât îi vom nota ca pe niște elemente esențiale. Pentru a ilustra această interconectare, este necesar să prezentăm un model economico-matematic al impactului complexului de factori asupra creșterii eficienței gestiunii și dezvoltării securității economice a statului $(F_{m1}, F_{m2}, F_{m3}, F_{m4})$, care va fi reprezentat prin relația funcțională prin forma dată: $F = F_{m1}, F_{m2}, F_{m3}, F_{m4} \rightarrow I$, unde: F_m este vectorul de factori de influență; $F_{m1}, F_{m2}, F_{m3}, F_{m4}$ sunt factorii de influență; iar I este criteriul eficienței funcționării inovațiilor.

În vederea construirii ulterioare a relației dintre securitatea economică a statului și inovații, este obligatoriu să se contureze sub forma unui model economico-matematic. Modelul economico-matematic al impactului criteriului eficienței funcționării inovațiilor *(I)* asupra criteriului eficienței funcționării securității economice a statului va fi reprezentat printr-o relație funcțională de forma: $F = F_m, F_2, F_3, F_4 \ldots F_n \rightarrow C$, unde: F este vectorul de

DOI: https://doi.org/10.53486/escst2023.04
International Conference, December 07-08, 2023, Chișinău, Moldova

factori de influență; $F_m, F_2, F_3, F_4 \dots F_n$ reprezintă factorii de influență; C este criteriul eficienței funcționării securității economice a statului.

Într-o formulare mai abstractă, complexitatea impactului generat de un număr extins de factori asupra eficienței gestionării și dezvoltării securității economice a statului este reprezentată în figura 1.

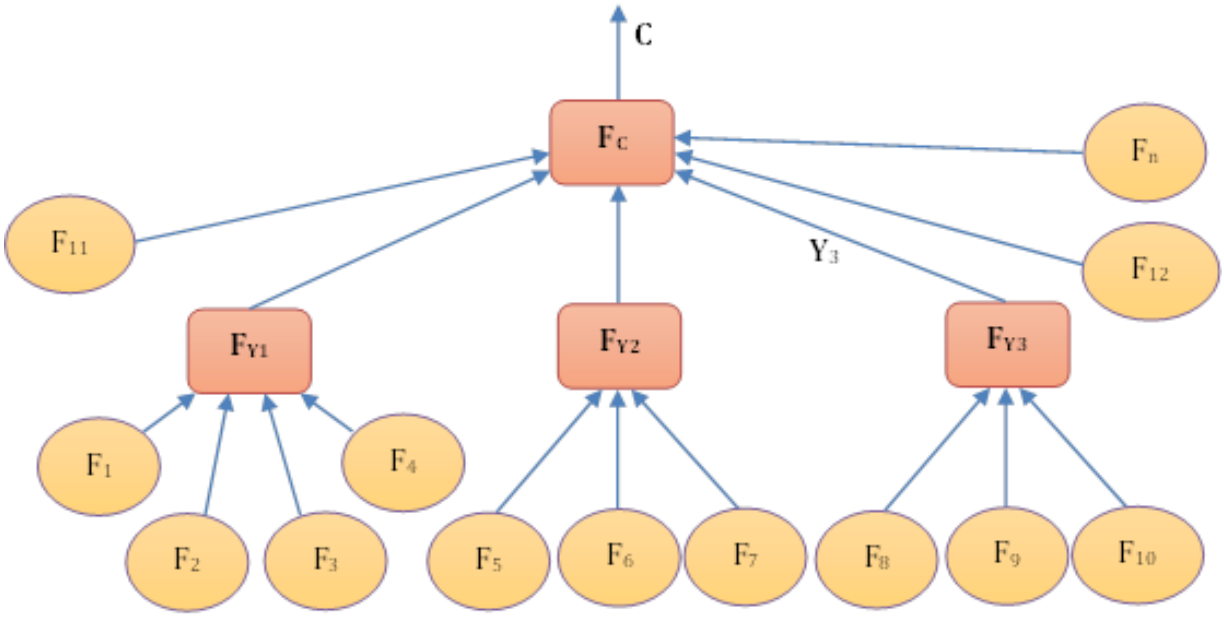


Figura 1. Impactul factorilor asupra eficienței gestionării și dezvoltării securității economice a statului
Sursa: elaborat de autor

Valorile $F_c, F_{y1,} \dots, F_n$ sunt obținute prin intermediul unei concluzii logice bazate pe modelul de concluzii *fuzzy*. Aceste valori ale factorilor vor reflecta abaterea (exprimată în procente) față de medii în ceea ce privește securitatea economică a statului, într-un interval de timp predefinit.

Pentru a modela impactul complex al factorilor, este necesar să: *(1) utilizeze un model de concluzii fuzzy:* pentru a atribui valori și a evalua impactul fiecărui factor asupra securității economice a statului; *(2) stabilească devierile față de medii:* valorile factorilor trebuie să reflecte abaterile procentuale față de mediile considerate ca reprezentând starea normală sau de referință.

În procesul de modelare, este important să avem în vedere că rezultatele concluziilor *fuzzy* pot să nu coincidă întotdeauna cu concluziile *experimentale* sau *de facto*. Aceasta poate să fie explicată prin faptul că modelul de evaluare a impactului inovațiilor asupra securității economice a statului este construit pe baza datelor statistice *(care nu totdeauna reprezintă adevărul)*. Astfel, discrepanțele între concluziile *fuzzy* și datele *reale* pot să apară din cauza complexității și a dinamicii reale a factorilor implicați (tabelul 1).

Pentru o analiză mai detaliată, este necesar să identificăm și să descriem factorii de influență (1-4) care afectează direct securitatea economică a Republicii Moldova. Acești factori sunt interconectați și au o relație proporțională între ei, având un impact direct asupra stării economice generale. Deoarece aceștia sunt strâns legați de aspectele financiare ale statului, exercită o influență directă asupra structurii administrative.

Impactul factorilor (5-7) asupra securității economice a statului se realizează prin intermediul organelor fiscale și de reglementare guvernamentale. Aceste entități joacă un

DOI: https://doi.org/10.53486/escst2023.04
International Conference, December 07-08, 2023, Chișinău, Moldova

rol important în gestionarea și menținerea stabilității economice prin implementarea politicilor fiscale și a reglementărilor corespunzătoare.

Factorii 8, 9 și 10 afectează securitatea economică în mod indirect, dar importanța lor crește în mod semnificativ în contextul proceselor globale de creștere din ultimii ani [4].

Impactul factorilor (11, 12) au un impact semnificativ în evoluția securității economice a Republicii Moldova. De menționat, că este decisiv să se înțeleagă și să se gestioneze acești factori în procesul de dezvoltare economică pentru a asigura o securitate economică sustenabilă.

Tabelul 1. Analiza factorilor de influență în dezvoltarea competitivității economice și securității statului

Factori de influență	Denumirea factorilor	Modelul eficacității și dezvoltării managementului competitivității economice a securității statului
Factor 1 Factor 2 Factor 3 Factor 4	Securitatea financiară a statului (f_1); Securitatea bugetară a statului (f_2); Securitatea internațională a statului (f_3); Securitatea bugetară a statului (f_4);	$K = f(f_1, f_2, f_3, f_4)$
Factor 5 Factor 6 Factor 7	Securitatea fiscală a statului (f_5); Securitatea a statului(f_6); Securitatea juridică a statului (f_7);	$K = f(f_5, f_6, f_7)$
Factor 8 Factor 9 Factor 10	Securitatea socială a statului (f_8); Securitatea științifică a statului (f_9); Securitatea politică a statului (f_{10});	$K = f(f_8, f_9, f_{10}$
Factor 11	Securitatea energetică a statului (f_{11});	$K = f(f_{11})$
Factor 12	Securitatea ecologică a statului (f_{12});	$K = f(f_{12})$

Sursa: elaborat de autor

Pentru o credibilitate mai bună a rezultatelor obținute, este obligatoriu să se efectueze o efectuare practică a modelului *fuzzy*, având la bază date statistice reale. Aceasta implică rezolvarea unei probleme de optimizare non-liniară, prin intermediul metodelor de programare matematică.

Într-un context mai amplu, sistemul poate fi perceput ca o reprezentare a unui model care reflectă factorii ce influențează eficacitatea managementului în dezvoltarea competitivității și securității economice a statului, precum și eficacitatea proceselor inovaționale în cadrul sistemului de securitate economică.

Sistemul în ansamblu are o dublă semnificație. Pe de o parte, poate fi utilizat pentru elaborarea unui set de măsuri menite să sporească eficacitatea gestionării dezvoltării competitivității și securității economice a statului. Acesta permite evaluarea impactului eficacității inovațiilor asupra sistemului și oferă mijloacele necesare pentru evaluarea prognozelor privind nivelul de eficacitate al acestora.

Pentru a asigura credibilitatea rezultatelor, este necesar să se efectueze o identificare practică a modelului *fuzzy* pe baza datelor experimentale reale. Aceasta este o problemă de optimizare non-liniară, rezolvată prin metode de programare matematică (tabelul 2).

Într-un sens mai larg, sistemul poate fi văzut ca o reprezentare a sistemului de modele care reflectă sistemul de factori care afectează eficacitatea managementului

DOI: https://doi.org/10.53486/escst2023.04
International Conference, December 07-08, 2023, Chișinău, Moldova

dezvoltării competitivității securității economice a statului și a eficacității proceselor inovaționale în sistemul securității economice a statului [5].

Sistemul general are o dublă semnificație. Pe de o parte, poate fi utilizat pentru dezvoltarea unui set de măsuri privind dezvoltarea eficacității gestionării dezvoltării competitivității securității economice a statului, evaluarea eficacității impactului inovațiilor asupra acesteia, evaluarea prognozelor nivelului de eficacitate.

Implementarea în practică a modelului *fuzzy* bazat pe date statistice reale și rezolvarea problemelor de optimizare non-liniară prin metode de programare matematică sunt esențiale pentru asigurarea credibilității rezultatelor. Sistemul propus nu doar reflectă factorii cheie ce influențează eficacitatea managementului în dezvoltarea competitivității și securității economice, ci oferă și instrumente necesare pentru evaluarea impactului inovațiilor și anticiparea nivelului de eficacitate.

Tabelul 2. Modelul integrat al inovațiilor asupra eficacității și dezvoltării securității economice a statului

Factori de influență	Denumirea factorilor	Modelul studiului eficacității influenței a inovațiilor pentru securitatea economică a statului
Factor 1	Inovații de informații (f_m 1)	$K = f(f_m 1)$
Factor 2	Inovații tehnologice (f_m 2)	$K = f(f_m 2)$
Factor 3	Inovații științifice (f_m 3)	$K = f(f_m 3)$
Factor 4	Inovații organizaționale (f_m 4)	$K = f(f_m 4)$

Sursa: elaborat de autor

Analizând modelul integrat al inovațiilor asupra eficacității și dezvoltării securității economice a statului, menționăm că este necesar să elucidăm factorii de influență care au un impact direct asupra securității economice a statului.

Factorul 1. Tehnologiile informaționale, influențate de globalizare, au devenit omniprezente în instituțiile statului, având un impact semnificativ asupra securității economice.

Factorul 2. Echiparea tehnică a instituțiilor contribuie la eficiența acestora în gestionarea resurselor, având un impact pozitiv asupra securității economice.

Factorul 3. Realizările liderilor de știință în domeniul politicii aduc contribuții semnificative la dezvoltarea soluțiilor avansate, influențând securitatea economică.

Factorul 4. Politica eficientă de personal contribuie la un mediu propice pentru inovații, influențând reziliența instituțiilor și capacitatea de a gestiona provocările economice.

Sistemul generează o multitudine de derivate independente în relația cercetată, având ca scop evaluarea eficacității gestionării dezvoltării competitivității și a proceselor inovaționale în sistemul securității economice a statului. Analiza factorială este esențială în acest context multifactorial pentru a reprezenta conexiunile complexe dintre securitatea economică și inovații.

Prin prisma impactului inovațiilor asupra instituțiilor, cheia pentru securitatea statului, acestea contribuie la eficiența operațională, capacitatea de adaptare rapidă la schimbări, gestionarea eficientă a riscurilor, consolidarea competitivității și promovarea cercetării și dezvoltării. Înțelegerea și gestionarea acestor inovații devin esențiale pentru asigurarea securității economice a Republici Moldova.

DOI: https://doi.org/10.53486/escst2023.04
International Conference, December 07-08, 2023, Chișinău, Moldova

CONCLUZII

Modelul integrat al inovațiilor și securității economice evidențiază interconexiunea strânsă dintre tehnologii, leadership științific, echipamentul instituțional și politica de personal. Acești factori, când sunt gestionați eficient, pot contribui semnificativ la consolidarea securității economice a Republicii Moldova.

Analiza factorială relevă că adoptarea și implementarea tehnologiilor informaționale, dotarea tehnică a instituțiilor, realizările științifice și o politică de personal eficientă sunt elemente cheie pentru eficacitatea și reziliența instituțiilor în fața provocărilor economice și de securitate. Aceste aspecte influențează în mod direct capacitatea instituțiilor de a opera eficient, de a se adapta rapid la schimbări și de a gestiona riscurile.

Prin promovarea inovațiilor în diferite domenii și crearea unui mediu propice pentru dezvoltarea acestora, Republica Moldova poate experimenta îmbunătățiri semnificative în eficiența operațională, capacitatea de adaptare, gestionarea riscurilor și consolidarea competitivității sale economice la nivel global. Este esențial ca guvernul și instituțiile relevante să înțeleagă și să gestioneze acești factori în mod integrat, adoptând strategii personalizate și durabile care să consolideze securitatea economică a țării. Implementarea acestor măsuri ar putea aduce beneficii semnificative în promovarea unei creșteri economice durabile și în asigurarea securității pe o perioadă mai extinsă în Republica Moldova.

BIBLIOGRAFIE

1. DANILIUC A. *Securitatea economică a Republicii Moldova: Amenințări și perspective*. În Revista: Vector European, 2018, p.67-70.
2. NICOLAE M. *Managementul inovatiei organizationale.* București: Tritonic, 2013, 236p.
3. Hotărârea Parlamentului nr. 153 din 15.07.2011, pentru aprobarea Strategiei securității naționale a Republicii Moldova. În Monitorul Oficial nr. 170-175, art. 499. Chișinău: Editura Monitorul Oficial, 2011. Colecție, număr de colecție: Monitorul Oficial, nr. 170-175.
4. MUNTEANU C. *Economic security threats and their amplification in the globalization process*. În: Metode matematice și tehnologii informaționale în economie, Universitatea Națională „Iurii Fedkovici", Cernăuți, Ukraina , 2015, p. 3-4.
5. ȘOIMU O., TROFIMOV V. *Securitatea economică a Republicii Moldova: unele probleme și căi de soluționare*. În: Revista Științifică a Universității de Stat din Moldova, nr.8. Seria Științe exacte și economice, 2007, p.126-128.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.05
International Conference, December 07-08, 2023, Chișinău, Moldova

PROVOCĂRI PENTRU SISTEMUL COMERCIAL INTERNAȚIONAL ÎN CONTEXTUL INSECURITĂȚII GLOBALE

CHALLENGES FOR THE INTERNATIONAL TRADING SYSTEM IN THE CONTEXT OF GLOBAL SECURITY

Natalia LOBANOV

PhD habilitat, Professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0003-3800-9038
E-mail:lobanov.natalia@ase.md

Abstract: *The article analyzes the challenges to the security and functionality of the international trade system, consisting of the trade flows between the states of the world, as well as a series of international regulatory institutions.Among the main challenges we mention military and trade conflicts, divergent growth trends in different regions, volatility of raw material prices, economic instability, governance issues within the World Trade Organization, the increase in the number and importance of regional trade agreements that gradually shift the focus of to the multilateral trade system to regional rules, the friendshoring trend. These factors increase the fragmentation of the single trade space, by eroding the basic principles of the international trade system, such as non-discrimination (the most favored nation clause, equal treatment for domestic and foreign products), progressive trade liberalization, predictability through consolidation and transparency, promoting fair competition, encouraging economic development and reforms. The outlook for the international trading system remains uncertain. At the same time, even if in the current conditions the countries aim, as a priority, to protect their national interests, we mention that from a strategic point of view, all WTO members will benefit from the development of multilateral cooperation. Thus, it is extremely important that the efforts of the world community support the multilateral systemic development of trade relations.*

When conducting the study, methods such as the systemic approach, analysis and synthesis, generalization, comparative analysis were used. International statistical data, WTO, UNCTAD publications, official documents of the European Union, international publications were used as informational support.

Keywords: *global economy, international trade system, instability, fragmentation, WTO.*

UDC: *339.52:339.9*

JEL Classification: *F13, F53.*

ÎNTRODUCERE

În momentul de față economia mondială se află în punctul de schimbare a tendințelor pe termen lung care s-au dezvoltat în ultimul sfert de secol. Condițiile convenționale care au susținut globalizarea în ultimele decenii, și anume banii ieftini, energie în cantitate suficientă, forță de muncă ieftină, logistică globală relativ ieftină – nu mai funcționează.

Agravarea contradicțiilor politice și economice dintre state, poate fi considerată drept principala provocare pentru sistemul comercial internațional, dar și sursă a instabilității economiei globale. Războiul Federației Ruse împotriva Ucrainei a devenit un declanșator pentru multe probleme în economia globală. Organizația pentru Cooperare și Dezvoltare Economică estimează că în 2023, războiul din Ucraina ar putea costa PIB-ul global 2,8 trilioane de dolari producție pierdută [1]. Are loc o redistribuire vădită a resurselor în favoarea sectoarelor economiei care lucrează pentru război. Cheltuielile pentru demografie, dezvoltare durabilă, mediu, educație și sănătate sunt în scădere relativă.

DOI: https://doi.org/10.53486/escst2023.05
International Conference, December 07-08, 2023, Chișinău, Moldova

Instabilitatea este o caracteristică a economiei globale, iar incertitudinea și riscurile negative în ce privește perspectivele economice persistă.

REZULTATE ȘI DISCUȚII

Deși se evidențiază o redresare a economiei globale în urma pandemiei și a crizei energetice din 2022, tendințele de creștere sunt din ce în ce mai divergente pe plan global, iar perspectivele pe termen mediu sunt considerate „mediocre".

Se conturează îngrijorări legate de reintensificarea inflației, în deosebi în țările în dezvoltare, de criza pieței imobiliare din China, volatilitatea prețurilor la materii prime, fragmentarea geopolitică. De asemenea, riscuri noi au apărut în urma conflictului dintre Israel și Palestina.

Conform datelor Fondului Monetar Internațional (FMI), în 2022 PIB-ul mondial a înregistrat o creștere de 3,5%. În raportul „World Economic Outlook" publicat în luna octombrie 2023, FMI a menținut estimarea creșterii economice globale la 3% pentru anul 2023, însă a redus prognoza pentru anul 2024 de la 2,9% la 2,8%. Se așteaptă că economiile avansate vor încetini de la 2,6% în 2022 la 1,5% în 2023 și 1,4% în 2024. În SUA, se prognozează o încetinire a creșterii de la 1,1% în 2023, la 0,8% în 2024, în mare parte datorită impactului continuu al majorării puternice a ratelor dobânzilor din ultimul an și jumătate [2].

În ce privește economia europeană, aceasta și-a pierdut avântul în 2023 pe fondul unui cost ridicat al vieții, al cererii externe slabe și al înăspririi monetare. Prognoza de toamnă a Comisiei Europene revizuiește creșterea PIB-ului UE în scădere în comparație cu proiecțiile sale de vară. În ansamblu, prognoza de toamnă prevede o creștere a PIB-ului în 2023 cu 0,6% atât în UE, cât și în zona euro, cu 0,2 puncte procentuale sub prognoza de vară a Comisiei. Se estimează, că în 2024 creșterea PIB-ului UE va fi de 1,3%. Aceasta este încă o revizuire descendentă în raport cu prognoza din vară. În zona euro, creșterea PIB-ului este proiectată să fie ușor mai scăzută, la un nivel de 1,2%. În 2025, odată cu diminuarea inflației, se așteaptă ca creșterea să ajungă la 1,7% pentru UE și 1,6% pentru zona euro [3].

În cele 27 de țări din Uniunea Europeană, creșterea prețurilor în termeni anuali în septembrie 2023 a fost de 4,9%. Față de luna precedentă, prețurile în UE au crescut cu 0,3%. Cea mai scăzută inflație anuală din septembrie a fost observată în Danemarca (0,6%) și Belgia (0,7%). Mai mult, în Olanda, deflația anuală a fost înregistrată la un nivel de 0,3%. Cea mai mare creștere a prețurilor de consum a fost înregistrată în Ungaria (12,2%), România (9,2%) și Slovacia (9,0%). În Germania, inflația anuală a scăzut la 4,3% de la 6,4% în august. În Franța, prețurile au crescut cu 5,7% în septembrie, la fel ca în august. În Italia, inflația a crescut la 5,6% de la 5,5% cu o lună mai devreme. Se estimează, că inflația a scăzut la un minim din ultimii doi ani în zona euro în octombrie și va continua să scadă. Se așteaptă, că inflația în zona euro va fi de 5,6% în 2023 și de 2,9% în 2024 - încă departe de obiectivul de 2% anual, pe care Banca Centrală Europeană încearcă să-l atingă prin creșterea ratelor dobânzilor [4].

În ce privește inflația globală, conform previziunilor FMI, aceasta va scădea de la 8,7% în 2022 la 6,8% în 2023 și 5,2% în 2024. Se estimează, că inflația de bază va scădea mai treptat, iar previziunile privind inflația pentru 2024 au fost revizuite în sus. Rezolvarea recentă a controversei privind plafonul datoriei din SUA și acțiunile guvernamentale decisive de la începutul anului 2023 pentru a limita tensiunile din sectoarele bancare în SUA și Elveția au redus riscurile imediate ale turbulențelor din sectorul financiar. Măsurile adoptate au atenuat riscurile negative asupra perspectivelor de dezvoltare. Cu toate acestea, riscurile referitoare la creșterea economică globală persistă și este posibilă înrăutățirea situației.

DOI: https://doi.org/10.53486/escst2023.05
International Conference, December 07-08, 2023, Chișinău, Moldova

Inflația ar putea rămâne ridicată și chiar să crească dacă vor avea loc șocuri, inclusiv cele asociate cu situația în Ucraina și evenimente meteorologice extreme, care să conducă la o politică monetară mai restrictivă. Turbulențele din sectorul financiar ar putea reveni pe măsură ce piețele se adaptează la înăsprirea în continuare a politicilor băncilor centrale [5].

„Economia globală se află într-o situație precară", spune Indermeet Gill, economist șef și vicepreședinte senior pentru economia dezvoltării la Grupul Băncii Mondiale. „Toate regiunile, cu excepția Asiei de Est și de Sud, sunt departe de dinamismul de dezvoltare necesar pentru eradicarea sărăciei, combaterea schimbărilor climatice și refacerea capitalului uman" [6].

Banca Mondială a apreciat, în octombrie 2023, că răspândirea efectelor negative este în curs de desfășurare și a estimat, că Asia va avea o creștere de 4,5% în 2024, în timp ce înainte de vară, instituția miza pe o creștere de 4,8% a PIB-ului în această regiune. O posibilă sursă a instabilității economice provine din China, a cărei redresare economică ar putea încetini, parțial ca urmare a problemelor nerezolvate din sectorul imobiliar, ceea ce va avea efecte negative transfrontaliere. Căderea companiei Evergrande, al doilea cel mai mare dezvoltator imobiliar din China, „dezvăluie explozia unei bule imobiliare care a fost în pregătire de zeci de ani, ducând la o scădere severă a cererii interne și a investițiilor, împovărând economia în general", consideră Xin Sun, specialist în economia chineză [7].

După cum arată prognozele recente ale Băncii Mondiale, șocurile suprapuse ale pandemiei, războiul din Ucraina și o recesiune economică bruscă pe fondul înăspririi condițiilor globale de creditare au împiedicat evoluția economică în țările emergente și în dezvoltare pentru o lungă perioadă de timp, iar situația nu se va schimba în viitorul apropiat. Activitatea economică așteptată în aceste țări până la sfârșitul anului 2024 va fi cu aproximativ 5% sub nivelul prognozat înainte de pandemie. Țările cu venituri mici au suferit pagube enorme, în special cele mai sărace. În mai mult de o treime din aceste țări, veniturile pe cap de locuitor în 2024 vor rămâne sub nivelurile din 2019. Ca urmare a acestei creșteri lente a veniturilor, sărăcia extremă se va accentua în multe țări cu venituri mici.

„Multe economii emergente se luptă să abordeze o creștere economică slabă, o inflație constantă ridicată și un nivel ridicat al datoriei. Dar noi pericole, cum ar fi posibilitatea unei răspândiri mai largi a efectelor reapariției tensiunilor financiare în economiile avansate, ar putea înrăutăți situația acestora", a declarat Ayhan Kose, economist șef adjunct la Grupul Băncii Mondiale. „Politicienii din aceste țări trebuie să acționeze rapid pentru a preveni contagiunea financiară și pentru a atenua vulnerabilitățile interne pe termen scurt" [8].

Astfel, constatăm, că redresarea economică globală rămâne lentă, cu divergențe tot mai mari între regiuni, cu accentuarea fragmentării spațiului global, ceea ce contravine principilor de bază a sistemului comercial internațional.

În anul 2022 comerțul global a atins un record de 32 de trilioane de dolari, dar tendința a devenit negativă în a doua jumătate a anului, pe fondul înrăutățirii condițiilor economice și al incertitudinii în creștere [9].

Conform prognozelor Organizației Mondiale a Comerțului (OMC) publicate în octombrie 2023, volumul comerțului global de mărfuri este de așteptat să crească cu 0,8% în acest an, mai puțin de jumătate din creșterea de 1,7% prognozată în aprilie. Creșterea de 3,3% proiectată pentru 2024 rămâne practic neschimbată față de estimarea anterioară. Încetinirea comerțului pare să aibă o bază largă, acoperind un număr mare de țări și o gamă largă de produse, în special anumite categorii industriale, cum ar fi metalele, echipamentele de birou și de telecomunicații, textilele și îmbrăcăminte [10].

DOI: https://doi.org/10.53486/escst2023.05
International Conference, December 07-08, 2023, Chișinău, Moldova

Raportul privind dezvoltarea lanțurilor valorice globale (LVG) elaborat de OMC și publicat în anul 2023, subliniază riscurile tot mai mari ale dependenței de câteva economii pentru anumite produse și evidențiază vulnerabilitatea LVG în fața tensiunilor comerciale în creștere și a crizelor globale [11].

În ultimii ani, lanțurile valorice globale au fost perturbate de o serie de factori: amenințările cibernetice, războiul comercial dintre SUA și China, pandemia, șocuri climatice, conflictul militar din Ucraina. Cooperarea politică internațională a slăbit și ea în perioada dată. Combinația acestor tendințe a condus la o regândire a lanțurilor globale de aprovizionare și a adus sustenabilitatea în prim-plan, în special ce ține de produse strategice. Astfel, odată cu creșterea cererii de semiconductori, jucători mondiali precum SUA, China și UE își subvenționează puternic capacitatea de producție internă într-un efort de a reduce dependența de lanțurile de aprovizionare. În acest context, guvernul francez a semnat un acord cu STMicroelectronics și GlobalFoundries pentru a construi o uzină de semiconductori, care prevede subvenții guvernamentale. Costul total al proiectului este de 7,5 miliarde de euro, investiția guvernului francez în uzină este de 2,9 miliarde de euro. Dimensiunea investiției guvernamentale în uzină a stârnit dezbateri în Franța, după retrogradarea ratingului de credit al țării la AA din cauza datoriei excesive a guvernului (111,6% din PIB). Criticii proiectului atrag atenția către așa-numita „cursă a subvențiilor", în care producătorii de cipuri solicită investiții suplimentare în timpul fazei de construcție a uzinelor, profitând de dorința guvernelor de a asigura independența față de livrările importate [12].

Un alt exemplu. Guvernul german va subvenționa planurile companiei americane Intel de a produce cipuri și instalații de semiconductori în Magdeburg. Securitatea lanțului de aprovizionare european a intrat în centrul atenției, parțial ca urmare a COVID-19. Intel preconizează că construcția va costa în jur de 30 de miliarde de euro și va crea aproximativ 3000 de locuri de muncă. În februarie 2022, Intel a cerut guvernului german să mărească asistența guvernamentală deja convenită pentru construirea a două uzine de cipuri în Magdeburg. Solicitarea a fost justificată de creșterea costurilor la energie și materii prime. În 2022, Germania a oferit aproximativ 6,6 miliarde de euro subvenții pentru a sprijini proiectul [13].

În contextul asigurării securității economice naționale, conceptul de friendshoring capătă aplicație practică. Acesta se bazează pe- construirea lanțurilor de producție și comerț în cadrul unor blocuri de țări care cooperează în alte domenii (organizații de integrare, militare) și cu care riscul de conflicte este minim. Se întâmplă atunci când un guvern impune întreprinderile să restructureze lanțurile de aprovizionare, deplasând producția de la rivalii geopolitici către puterile prietene. Interzicerea sau limitarea investițiilor companiilor americane în sectorul tehnologic al Chinei în august 2023 este un exemplu. Restricțiile vizează capitalul privat, capitalul de risc, întreprinderile mixte și investițiile în proiecte noi [14]. Friendshoring-ul este similar cu nearshoring-ul, care mută producția mai aproape de casă. Ambele politici vizează consolidarea securității comerciale. Ele au un cost, deoarece atunci când politica, mai degrabă decât profitul, determină locul în care sunt fabricate bunurile, este probabil că producția va fi mai puțin eficientă [15]. Mai mult, acest fapt este probabil să crească decalajul tehnologic și dezechilibrele de dezvoltare în economia globală și ar putea duce la o polarizare mai mare între țările dezvoltate și cele în curs de dezvoltare, tendință care a devenit deja destul de evidentă în ultimii ani. Eșecul Rundei Doha este o mărturie în acest sens.

Această Rundă lansată în 2001, și planificată inițial să dureze trei ani, nu a putut fi încheiată din cauza diferențelor de opinie profunde dintre statele membre ale OMC.

DOI: https://doi.org/10.53486/escst2023.05
International Conference, December 07-08, 2023, Chișinău, Moldova

Obiectivul principal al Rundei este liberalizarea economiei globale prezentată ca un program de dezvoltare care să permită țărilor cel mai puțin dezvoltate să acceseze piețele țărilor bogate [16]. Dintre blocajele deosebit de importante, care împiedică realizarea obiectivelor Rundei, putem numi pe de o parte, ratele de deschidere ale țărilor în curs de dezvoltare în ceea ce privește taxele vamale, iar pe de altă parte, subvenții din partea țărilor dezvoltate, în special pentru produsele agricole, acuzate că denaturează concurența și împiedică accesul pe piață pentrul țările în curs de dezvoltare.

Deși statele membre încearcă în mod regulat să relanseze Runda Doha, totuși, deteriorarea relațiilor interstatale și revenirea protecționismului sumbinează sistemul comercial internațional. Din cauza imposibilității depășirii intereselor uneori contradictorii ale membrilor săi, se constată în ultimii ani o revenire la acorduri regionale sau bilaterale, care nu sunt în deplin acord cu dinamica multilaterală.

Conform datelor Organizației Mondiale a Comerțului, numărul total de acorduri comerciale regionale în vigoare a crescut de la 98 în anul 2000 la 360 în 2023 [17]. Marea majoritate a acordurilor regionale sunt încheiate sub formă de acorduri de liber schimb (ALS). Conform regulilor OMC, ALS și uniunile vamale sunt excepții de la regula generală a OMC, deoarece oferă anumite beneficii și preferințe pentru un număr limitat de participanți, ceea ce nu corespunde principiului de bază al națiunii celei mai favorizate. Dar normele OMC nu împiedică încheierea de acorduri privind zonele de liber schimb și uniuni vamale, cu condiția ca astfel de acorduri să contribuie la dezvoltarea comerțului liber și să nu conducă la crearea de obstacole în calea comerțului între participanții săi și țările terțe.

Totodată, conținutul acordurilor comerciale regionale s-a schimbat semnificativ. Pe lângă reducerea tarifelor și eliminarea barierelor netarifare între teritoriile vamale unite într-o zonă de liber schimb, acordurile reglementează aspectele legate de proprietatea intelectuală, dezvoltarea durabilă, investițiile, drepturile consumatorilor și standardele de mediu.

O altă provocare pentru sistemul comercial internațional este criza organului de apel al OMC declanșată la sfârșitul anului 2019, din cauza refuzului Statelor Unite să aprobe numirea de noi judecători în Organul de soluționare a litigiilor (OSL) odată cu plecările planificate. Fără un număr suficient de judecători, OSL nu mai poate funcționa, ceea ce înseamnă în mod concret că conflictele comerciale, legate de exemplu de subvenții sau bariere comerciale nejustificate, nu vor mai putea găsi soluții dezvoltate într-un cadru multilateral. Această situație deschide ușa multiplelor acorduri locale, bilaterale [18].

În absența instrumentului eficient pentru a regla diferendele comerciale între statele, funcționarea sistemului comercial internațional riscă să fie perturbată. Membrii OMC întâmpină dificultăți în stabilirea, negocierea și încheierea acordurilor comerciale, atât pentru problemele restante, cât și pentru problemele noi. Prin urmare, în condiții de instabilitate globală sunt necesare măsuri proactive pentru a proteja rolul vital al OMC în dezvoltarea sistemului comercial multilateral.

CONCLUZII

Instabilitatea economică este o caracteristică a dezvoltării economiei globale, exprimată prin modificări semnificative cauzate de întreruperea conexiunilor existente în relațiile economice internaționale, pierderea dinamismului sistemului economic, incapacitatea de a se adapta rapid la schimbările parvenite.

Perspectivele sistemului comercial internațional rămân incerte pe fondul tensiunilor geopolitice în curs, precum și al preocupărilor legate de inflație și prețuri ridicate ale materiilor prime. Una din consecințele răspândirii friendshoring-ului ar putea fi

DOI: https://doi.org/10.53486/escst2023.05
International Conference, December 07-08, 2023, Chișinău, Moldova

fragmentarea spațiului comercial unic, excluderea țărilor sărace care au cel mai mult nevoie de comerțul global pentru a deveni mai bogate și mai democratice. Fapt va crește riscul ca acestea să devină state eșuate, teren fertil pentru creșterea migrației ilegale și a rețelelor criminale internaționale.

Este necesară căutarea unor noi abordări în dezvoltarea modelului de reglementare multilaterală în cadrul sistemului comercial internațional. Trebuie luate măsuri proactive pentru a proteja rolul vital al OMC în dezvoltarea sistemului comercial multilateral, deoarece dinamica pozitivă a economiei globale este parțial rezultatul a două dintre cele mai fundamentale principii ale sistemului comercial: fluxul fără restricții al comerțului internațional și furnizarea unei platforme constructive și echitabile pentru țări de a soluționa diferendele comerciale. Pacea, de asemenea, este rezultatul încrederii și cooperării internaționale generate și consolidate de sistem.

BIBLIOGRAFIE

1. DNIPROPETROVSK INVESTMENT AGENSY. Какой будет динамика мировой экономики в 2023 году. Опубликовано - 18.01.2023. [viewed 10 December2023]. Available from: < https://dia.dp.gov.ua/ru/kakoj-budet-dinamika-mirovoj-ekonomiki-v-2023-godu/ >.
2. INTERNATIONAL MONETARY FUND. WORLD ECONOMIC OUTLOOK. Navigating Global Divergences .Oct.2023 [viewed 10 December 2023]. Available from: <https://www.imf.org/en/Publications/WEO/Issues/2023/10/10/world-economic-outlook-october-2023) >.
3. EUROPEAN COMMISSION. PRESS RELEASE. 15 november 2023. Autumn 2023 Economic Forecast: A modest recovery ahead after a challenging year. [viewed 13 December 2023]. Available from: <https://ec.europa.eu/commission/presscorner/detail/en/ip_23_5743>.
4. JORGE LIBOREIRO. L'économie de l'UE perd de son dynamisme en raison de la guerre en Ukraine, de l'inflation, des catastrophes naturelles et de la hausse des taux d'intérêt. EURONEWS. Publié le 11/09/2023. [viewed 13 December 2023]. Available from: <https://fr.euronews.com/business/2023/09/11/leconomie-de-lue-perd-de-son-dynamisme-en-raison-de-la-guerre-en-ukraine-de-linflation-des >.
5. FONDS MONETAIRE INTERNATIONAL. PERSPECTIVES DE L 'ECONOMIE MONDIALE. RÉSILIENCE À COURT TERME, DIFFICULTÉS PERSISTANTES. JUILLET 2023. [viewed 10 December 2023]. Available from: <https://www.imf.org/fr/Publications/WEO/Issues/2023/07/10/world-economic-outlook-update-july-2023 >.
6. LA BANQUE MONDIALE. COMMUNIQUÉS DE PRESSE. 06 JUIN 2023.Une économie mondiale fragilisée dans un contexte de taux d'intérêt élevés. [viewed 10 December 2023]. Available from: < https://www.banquemondiale.org/fr/news/press-release/2023/06/06/global-economy-on-precarious-footing-amid-high-interest-rates >.
7. SÉBASTIAN SEIBT. Comment la Chine risque d'exporter ses déboires économiques. [viewed 10 December 2023]. Available from: <https://www.france24.com/fr/%C3%A9co-tech/20231003-comment-la-chine-risque-d-exporter-ses-d%C3%A9boires-%C3%A9conomiques >.
8. ВСЕМИРНЫЙ БАНК. Пресс релиз. 6.06. 2023. Неустойчивость мировой экономики на фоне высоких процентных ставок. [viewed 4 December 2023].

DOI: https://doi.org/10.53486/escst2023.05
International Conference, December 07-08, 2023, Chişinău, Moldova

Available from: < https://www.vsemirnyjbank.org/ru/news/press-release/2023/06/06/global-economy-on-precarious-footing-amid-high-interest-rates >.

9. ОРГАНИЗАЦИЯ ОБЪЕДИНЕННЫХ НАЦИЙ. Доклад ЮНКТАД: мировая торговля замедляется, но перспективы позитивные. 23 марта 2023. [viewed 4 December2023]. Available from: < https://news.un.org/ru/story/2023/03/1439067 >.
10. RALPH OSSA. Quelles sont les perspectives de croissance du commerce mondial en 2023 et 2024? [viewed 10 December 2023]. Available from: <https://www.wto.org/french/news_f/archive_f/tfore_arc_f.htm >.
11. ORGANISATION MONDIALE DU COMMERCE. Rapport 2023 sur le développement des CVM: des CVM durables et résilientes en des temps agités. [viewed 4 December 2023]. Available from: <https://www.wto.org/french/news_f/news23_f/publ_16nov23_f.htm>.
12. THÉOPHANE HARTMANN. France signs off €7.5bn chip factory. 6.06.2023. [viewed 10 December 2023]. Available from: < https://www.euractiv.com/section/industrial-strategy/news/france-signs-off-e7-5bn-chip-factory/ >.
13. SEMI-CONDUCTEURS: L'ALLEMAGNE CASSE SA TIRELIRE POUR OBTENIR LA FUTURE USINE D'INTEL. Par Euronews avec AFP. Publié le 20/06/2023. [viewed 4 December 2023]. Available from: < https://fr.euronews.com/2023/06/20/semi-conducteurs-lallemagne-casse-sa-tirelire-pour-obtenir-la-future-usine-dintel >.
14. U.S. DEPARTMENT OF THE TREASURY. PRESS RELEASES, August 9, 2023. Treasury Seeks Public Comment on Implementation of Executive Order Addressing U.S. Investments in Certain National Security Technologies and Products in Countries of Concern. [viewed 10 December 2023]. Available from: <https://home.treasury.gov/news/press-releases/jy1686>.
15. THE ECONOMIST EXPLAINS. What is "friendshoring"? The Economist. Aug 30th 2023 [viewed 10 December 2023]. Available from: < https://www.economist.com/the-economist-explains/2023/08/30/what-is-friendshoring>.
16. ORGANISATION MONDIALE DU COMMERCE. La Déclaration de Doha expliquée. [viewed 4 December 2023]. Available from: <https://www.wto.org/french/tratop_f/dda_f/dohaexplained_f.htm >.
17. ORGANISATION MONDIALE DU COMMERCE. Accords commerciaux régionaux. [viewed 14 December 2023]. Available from: <https://www.wto.org/french/tratop_f/region_f/region_f.htm >.
18. PARLEMENT EUROPEEN. La crise de l'Organe d'appel de l'OMC (débat) Mardi 26 novembre 2019 – Strasbourg. [viewed 14 December 2023]. Available from: <https://www.europarl.europa.eu/doceo/document/CRE-9-2019-11-26-ITM-017_FR.html>.

Economic Security in the Context of Systemic Transformations
DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

CONVERGENCE OF BANKING CYBERSECURITY STRATEGIES TO THE NEW RULES ON DIGITAL OPERATIONAL RESILIENCE

CONVERGENȚA STRATEGIILOR DE SECURITATE CIBERNETICĂ BANCARĂ LA NOILE NORME PRIVIND REZILIENȚA OPERAȚIONALĂ DIGITALĂ

Ilinca GOROBEȚ

PhD, Associate Professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0002-8429-9585
Email: gorobet.ilinca@ase.md

Abstract: *Banks in the EU must ensure enhanced cyber security by the end of 2024 to comply with the Digital Operational Resilience Requirements (DORA), which was adopted by the European Council in November 2022. Every bank in the EU will have to be sure that its suppliers and their security controls comply with resilience standards. This is necessary to align banks' efforts with potential risks. The DORA sets uniform requirements for the security of banks' networks and IT systems, as well as third parties providing ICT services to them: cloud platforms or data analytics services. ICT service providers from outside the EU will have to set up subsidiaries in the EU so that supervision can be implemented uniformly. Research methods will be description, comparison, synthesis. As a result, we will elucidate the degree of convergence of cybersecurity requirements in banks in the domestic market and in European practice.*

Keywords: *digital economy, banking, convergence, information technology, globalization, regulation*.

UDC: *004.056:336.71*

JEL Classification: *F65, F69, G21, G28, O31*.

INTRODUCERE

Pandemia COVID-19 a fost o punte spre accelerarea introducerii digitalizării, iar digitalizarea necesită soluții tehnologice avansate atât pentru persoanele fizice, cât și pentru persoanele juridice.

În contextul actual, post-pandemic, se utilizează pe larg munca la distanță sau o varianta mixtă a acesteea, iar realizarea ei, o precondiție rămână a fi accelerarea digitalizării și automatizarea mai multor procese, inclusiv și a muncii. Însă, nu toate muncile pot fi efectuate la distanță, acestea pot fi atribuite mai mult muncii care se realizează la birou. Toate acestea presupun o reorientare profesională a posturilor de muncă și creșterea numărului de secialiști IT.

Un alt aspect important în ultima perioada o constituie creșterea comerțului electronic, care necesită instantaneitate, siguranță și securitate a plăților, precum și spațiu de stocare a informației sub formă de cloud, iar persoanele juridice, chiar și întreprinderile mici au nevoie de sistematizarea și prelucrarea datelor și apelează tot mai frecvent la servicii de tip Big Data.

În UE, tot mai mult se descută de finanțe digitale, astfel, „în 2020, în luna septembrie, s-a aprobat, la nivel de Comisie Europeană, un **pachet compus din strategii (prima ține de finanțele digitale și alta privește plățile retail) și propuneri legislative (vizează** criptoactivele și reziliența digitală).

DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

Cele menționate abordează sectorul financiar european în contextul concurenței și inovațiilor, cu posibilitatea de creștere a calității serviciilor financiare și de plată, totodată oferind **protecție consumatorilor** și **stabilitatea financiară"** [4]**.**

„Actul privind reziliența operațională digitală (DORA) își propune de a analiza și a gestiona riscurile ce apar în sistemele TIC. Acest risc devine tot mai pregnant, deoarece sectorul financiar care este tot mai digitalizat și dependent de tehnologii".

„Cerințele stabilite de DORA sunt **uniforme. Ele analizează securitatea rețelelor și a sistemelor informatice** ale entităților care își desfășoară activitatea în sectorul financiar. La fel, se vor uniformiza cerințele și față de terții care le vor furniza serviciile legate de TIC", adică cei ce livrează cloud sau Big Data. „Aceste cerințe trebuie respectate pentru ca sectorul financiar al spațiului european să poată gestiona riscurilor operaționale **și să aibă suficiente resurse pentru a le contracara**. Acest Act a fost aprobat în noiembrie 2022, iar entitățile asupra cărora cad incidențele acestui act (in speță, băncile) le pot implementa până în anul 2025" [4].

REZULTATE ȘI DISCUȚII

Uniunea Europeană „a adoptat politica „Deceniul Digital" – 2021-2030. Obiectivele deceniului digital sunt măsurabile pentru domeniile: *conectivitate, competențe digitale, întreprinderi digitale și servicii publice digitale*.

„Raportul cu indicele DESI reflectă gradul de digitalizare la nivelul UE. Indicele economiei și societății digitale *(Digital Economy and Society Index – DESI)* reflectă progresul înregistrat de statele membre ale Uniunii Europene în domeniul digitalizării și este publicat anual de Comisia Europeană, începând cu anul 2014. Pandemia COVID-19 a sporit eforturile de digitalizare a statelor membre ale UE, dar încă se luptă să reducă decalajele în ceea ce privește competențele digitale, transformarea digitală a IMM-urilor și lansarea rețelelor 5G avansate" [3].

„UE a pus la dispoziție 127 de miliarde EUR pentru a sprijini transformarea digitală în statele membre prin planuri naționale de redresare și reziliență și presupun facilități de redresare și reziliență (FRR). Consolidarea securității cibernetice se realizează în context geopolitic și se efectuează ținând cont de dezinformarea online. Autoritățile naționale, sub egida instituțiilor UE au accelerat cooperarea în domeniul securității cibernetice. Planurile naționale de redresare și reziliență urmăresc următoarele ținte europene": [5]

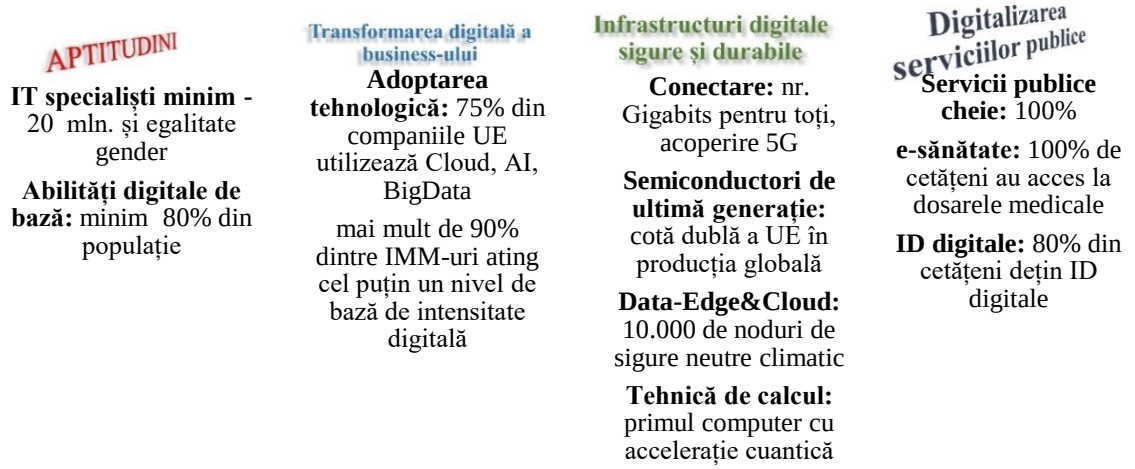


Figura 1. Țintele propuse de „Deceniul Digital"

Sursa: Digital Economy and Society Index (DESI) 2022. Thematic chapters

DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

Raporturile anuale DESI includ profiluri de țară sintetizate, grupate pe anumiți indicatori ce sunt vizați de politica UE în domeniul digitalizării.

„De la an la an, indicatorii DESI se actualizează astfel, în 2021, indicele s-a aliniat la țintele corespunzătoare din „Deceniul Digital" și acest lucru s-a reflectat în structura următorilor indicatori:

- *capitalul uman* – indicatorilor abilități de utilizator de internet și abilități digitale avansate;
- *conexiune* – utilizare în bandă largă fixă, acoperire în bandă largă fixă, acoperire mobilă și prețurile de acoperire în bandă largă;
- *integrarea tehnologiei digitale* – digitalizarea afacerilor și comerțul electronic;
- *servicii publice digitale* – e-guvernare" [5].

Indicele DESI 2022, include deja unsprezece indicatori, pentru a evalua progresul către obiectivele „Deceniului digital" a nivelului statelor membre europene. „Acest indice suportă ajustări și cele patru elemente (capitalul uman, conexiune, integrarea tehnologiei digitale, servicii digitale), în anul 2022, vor fi caracterizate

- *capitalul uman* – cel puțin abilități digitale de bază, specialişti IT, femei specialiste IT;
- *conexiune* – Gigabit pentru toată lumea (acoperire fixă a rețelei de foarte mare capacitate), acoperire 5G;
- *integrarea tehnologiei digitale* – IMM-urile ating cel puțin un nivel de bază de intensitate digitală, AI (inteligență artificială), Cloud, Big Data;
- *servicii publice digitale* – servicii publice digitale pentru cetățeni și servicii publice digitale pentru business" [5].

Indicele DESI va fi și în continuare aliniat planului „Deceniul Digital" pentru a se asigura că toate obiectivele vor fi cuantificate și analizate în rapoartele viitoare.

În continuare, ținând cont de datele prezentate în indicele DESI pentru anul 2022, vom încerca să prezentăm și să analizăm situația privind realizarea obiectivelor „Deceniului digital".

Pentru analiză, autorul, a ținut să prezinte următorii indicatori:

- *utilizatori internet*, grupați gender (femei/bărbați), precum și poziția (rating-ul) în grupul statelor membre UE;
- gradul de utilizare a *online banking-ul* conform repartiției gender (femei/bărbați), precum și poziția (rating-ul) în grupul statelor membre ale Uniunii Europene (UE);
- gradul de utilizare a *serviciilor publice electronice* (e-government) conform repartiției gender (femei/bărbați), precum și poziția (rating-ul) în grupul statelor membre UE, și;
- la final, analizăm care e poziția fiecărui stat în cadrul UE conform gradului de utilizare a internetului.

Acești indicatori au fost selectați pentru a reprezenta o privire de ansamblu a implementării internetului în necesitățile cotidiene a oricărui individ. Întâi, analizăm numărul de utilizatori, după anumite criterii, apoi vedem câți din acești utilizatori, utilizează internetul pentru a li se facilita activitatea și a li se economisi timpul petrecut la ghisee, adică, plățile retail, analizând online banking-ul și relațiile cu instituțiile statului, analizând gradul de implementare și utilizare a serviciilor publice digitale. Această analiză o efectuăm pentru cele 27 de state membre ale Uniunii Europene și pentru cele două state candidate la aderare

DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

la UE: Republica Moldova și Ucraina (țări candidate la UE fiind Albania, Bosnia și Herțegovina, Muntenegru, Macedonia de Nord, Serbia, Georgia și Turcia).

Tabelul 1. Principalii indicatori ai economiei digitale în statele membre ale Uniunii Europene și în statele candidate UE - Republica Moldova și Ucraina, în anul 2022

Țara	Utilizatori internet, persoane fizice			Online banking			Utilizatori e-government			Utilizarea internetului
	Femei, %	Bărbați, %	Poziția	Femei, %	Bărbați, %	Poziția	Femei, %	Bărbați, %	Poziția	Poziția
Belgia	92	91	8	82	80	9	73	76	15	12
Bulgaria	73	75	27	20	19	26	36	32	26	26
Cehia	87	88	18	83	81	8	79	72	10	16
Danemarca	98	97	2	96	95	2	94	92	1	5
Germania	88	90	13	53	57	23	53	56	23	23
Estonia	90	89	10	90	89	4	90	89	5	4
Grecia	77	77	25	51	57	24	69	70	18	21
Spania	92	92	7	67	72	17	71	75	17	11
Franța	90	89	12	79	78	11	88	86	7	14
Croația	76	85	26	67	69	16	51	59	24	25
Irlanda	98	97	1	81	75	10	91	93	4	3
Italia	79	82	24	51	60	25	39	41	25	22
Cipru	90	91	9	70	73	15	64	62	19	18
Letonia	90	89	11	89	87	5	85	83	8	9
Lituania	86	85	20	83	83	7	72	68	16	15
Luxemburg	96	98	3	72	73	13	77	81	12	8
Ungaria	87	87	15	62	64	20	82	81	9	17
Malta	87	86	17	71	72	14	73	71	14	10
Țările de Jos	94	94	6	96	96	3	89	94	6	2
Austria	87	91	16	75	79	12	77	80	13	13
Polonia	83	84	21	62	60	21	56	53	22	24
Portugalia	79	81	23	63	66	19	58	59	21	19

DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

România	81	82	22	18	19	27	15	18	27	27
Slovenia	88	88	14	61	67	22	78	75	11	7
Slovacia	87	88	19	64	66	18	62	62	20	20
Finlanda	95	95	5	97	96	1	94	91	3	1
Suedia	96	94	4	87	86	6	94	93	2	6
Media UE	**87**	**88**	-	**64**	**66**	-	**65**	**65**	-	-
Republica Moldova [9]	**87,9**	**89,7**	-	**46,3**		-	**47,6**		-	-
Ucraina	**77,8 [7]**		-	**67 [6]**		-	**63 [2]**		-	-

Sursa: Women in Digital Scoreboard 2022. Country profiles.

Statele membre UE cu cele mai înalte rezultate au fost evidențiate cu verde, iar cele care se clasează spre finalul clasamentului au fost evidențiate cu roșu.

Analizând indicatorul numărul de utilizatori internet persoane fizice, conform datelor pentru anul 2022, observăm că cei mai mulți utilizatori sunt în Irlanda, Danemarca și Luxembrug. Amintim că acest indicator trebuie să depășească 80% din populație. Sub 80% avem Portugalia – femei, Grecia, Croația și Bulgaria, atât bărbați cât și femei.

Conform indicatorului utilizării online-banking-ului pe prima poziție în 2022 a fost Finlanda, pe a doua poziție Danemarca și pe poziția a treia – Țările de Jos, varind de la 95% până la 96% pentru bărbați și de 96% - 97% pentru femei. Amintim că valoarea medie europeană a acestui indicator este 64% pentru femei și 66% pentru bărbați. La polul opus cu rezultate modeste sunt Italia, Bulgaria și România pe poziția 27 cu 18% femei și 19% bărbați. Țările, care în 2022, înregistrează rezultate sub valoarea medie sunt Grecia, Germania, Polonia, Ungaria, Slovenia și Portugalia – doar femei.

Dacă e să analizăm indicatorul utilizării e-government, rezultatele nu se deosebesc mult de rezultatele înregistrate la indicatorul utilizării online banking-ului. Primele 3 clasate cu 94% femei sunt Danemarca, Suedia, Finlanda, diferența este înregistrată doar pentru bărbați și oscilează de la 91% la 93%. Rezultate modeste înregistrează Italia, Bulgaria și România, de la valoarea cea mai mică pentru femei înregistrată în Romania cu 15% pentru femei și 18% bărbați. Deși Bulgaria și Italia înregistrează valori modeste, dar cifrele sunt duble față de România. Media în UE a acestui indicator este 65%, iar Europa tinde spre minim 80%. Țările care nu ating valoarea medie sunt – Croația, Germania, Polonia, Portugalia, Slovacia, Cipru – atât pentru femei cât și pentru bărbați.

Dacă e să facem o privire de ansamblu, Finlanda, Danemarca, Țările de Jos și Suedia continuă să fie liderii UE, însă provocările digitale rămân a fi actuale pentru toți.

Celelalte state membre, în ultimul timp, înregistrează tendința accentuată de creștere și de convergență în UE. Multe state membre care au rămas în urma liderilor, Italia, Polonia și Grecia și-au îmbunătățit indicele DESI în ultima perioadă, datorită investițiilor europene cu accent pe digitalizare. Necesită eforturi considerabile pentru a spori digitalizare în Bulgaria și România.

Un alt aspect care îl putem evidenția constă în faptul că în multe state utilizatorii nu pot fi transformați și adaptați la servicii publice și la plăți. Din această categorie este: Germania, Croația, Ungaria, Polonia, Slovacia și Bulgaria. România și cel mai

DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

reprezentativ exemplu, unde numărul utilizatorilor internet depășește 80%, iar utilizarea online-banking-ul și utilizarea e-government este sub 20%.

Dacă e să analizăm statele candidate la membre UE – Ucraina și Republica Moldova, rezultatele sunt următoarele: Republica Moldova, înregistrează rezultate pozitive din punct de vedere al numărului de utilizatori internet, dar are deficiențe (ca și România) la transformarea acestora în utilizatori online banking și utilizatori e-government. Valorile ultimilor doi indicatori sunt mult sub media europeană, dar depășesc valorile înregistrate de Bulgaria și România, iar la indicatorul utilizării e-government depășesc și valorile înregistrate de Italia.

Cât privește Ucraina, după numărul de utilizatori internet este sub obiectivul european de 80%, dar este peste rezultatele înregistrate de Croația și Bulgaria. Dacă este să analizăm online banking-ul, Ucraina este peste media europeană, iar la utilizarea e-government, Ucraina aproape atinge media europeană.

Cele menționate au fost realizate ținând cont cât de digitalizată este economia fiecărei țări. Cu cât economia este mai digitalizată cu atât poate fi mai vulnerabilă și prezenta o țintă pentru hackeri.

Lacunele de securitate a datelor reprezintă o problemă frecventă în digitalizare. Din analiza anterioară, am analizat indicatorul utilizării online banking-ul și am observat că numărul utilizatorilor crește progresiv. Băncile și alte entități financiare trebuie să-și întărească mai mult securitatea cibernetică, pentru a corespunde prevederilor „Actului legislativ privind reziliența operațională digitală (DORA), adoptat de Consiliul European în noiembrie 2022, fiind cea mai importantă inițiativă de reglementare a UE privind reziliența operațională și securitatea cibernetică în sectorul serviciilor financiare”.

Furnizorii băncilor și altor instituții financiare din UE vor trebui să-și asigure standardele de reziliență, pentru ca eforturile să fie proporționale cu riscurile existente.

„DORA stabilește cerințe comune și standard pentru securitatea rețelelor și a sistemelor informatice ale entităților din sectorul financiar, precum și ale părților terțe care le furnizează servicii legate de TIC” (tehnologii ale informației și comunicațiilor), cum ar fi platformele cloud sau serviciile de Big Data .

„Furnizorii de servicii TIC din țări terțe vor trebui să-și înființeze filiale pe teritoriul UE, pentru a se putea realiza supravegherea în mod corespunzător” [1].

„Aceste schimbări vor necesita să fie reglementate la nivel național în fiecare stat membru al UE. În același timp, autoritățile europene de supraveghere bancară vor elabora standarde tehnice care vor trebui respectate de toate instituțiile din domeniul serviciilor financiare” [1].

Realitatea anului 2023 arată că „este nevoie de un alt nivel, mai înalt, de colaborare între sectorul public și cel privat pentru o raportare mai exhaustivă a problemelor și cazurilor înregistrate în domeniul atacurilor cibernetice, a riscurilor identificate și a planificării recuperării pierderilor în caz de materializare a riscurilor”.

„Atacurile cibernetice au impact mai mare decât costul financiar direct generat de acesta, prejudiciile unor astfel de evenimente au dus la pierderea clienților, pierderea datelor clienților și daune aduse reputației sau mărcii” [1].

Digital Trust Insights a chestionat entitățile financiare din UE vis-a-vis de atacurile cibernetice. „Conform rezultatelor sondajului, mai puțin de 40% dintre directorii chestionați afirmă că au atenuat complet expunerea la riscurile de securitate cibernetică într-o serie de domenii critice, precum munca la distanță și hibridă (38% spun că riscul cibernetic este pe

DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

deplin atenuat), adoptarea accelerată a cloud-ului (35%), utilizarea IOT (34%), digitalizarea lanțului de aprovizionare (32%) și a operațiunilor de back-office (31%)" [8].

„Entitățile trebuie să-și evalueze expunerile la riscurile cibernetice, să-și fortifice capacitățile de reacție la amenințări, să asigure protecție prin parole sigure, să utilizeze patch-urile de securitate și să facă backup la date. Un rol important îl va constitui formarea continuă a personalului privind prevenirea atacurilor cibernetice și raportarea acestora la organele de supraveghere" [8].

Atacurile cibernetice sunt tot mai frecvente în ultima perioadă, dar și băncile sunt mai „mature" și mai pregătite pentru a gestiona riscurile. Majoritatea băncilor elaborează strategii și alocă investiții pentru prevenirea lor. Spre regret, multe din aceste strategii sunt de protecție împotriva evenimentelor și nu de anticipare, iar rezultatele nu sunt neapărat cele așteptate.

Orice proces de gestiune a riscurilor trebuie să presupună mai multe scenarii de manifestare a pericolelor sau a oportunităților. Dar oricâte scenarii nu ar fi luate în analiză, capacitatea de a prognoza toate datele, rămâne oarecum insuficientă și limitată din cauza că entitățile au structuri organizatorice și procese diferite, comunicarea pe interior uneori e deficientă, anevoioasă sau tardivă, tehnologiile sunt diverse și ingeniozitatea și inventivitatea hackerilor nu are limite.

„Astfel, reieșind din cele menționate, băncile, de rând, cu alte companii din domeniul serviciilor financiare, sunt obligate să corespundă cerințelor privind reziliența operațională. Pentru aceasta se vor implementa strategii de securitate cibernetică care să facă față tuturor provocărilor. Toate se vor rezuma la formarea resurselor financiare și umane de speță, găsirea celor mai eficiente procese de identificare și gestiune a riscurilor ce țin de securitatea cibernetică" [1].

„DORA se bazează pe patru piloni:

- gestiunea riscurilor legate de tehnologia informației și comunicații (TIC);
- raportarea incidentelor;
- testarea operațională și de reziliență digitală;
- managementului riscului generat de furnizorii TIC" [1].

Denunțarea oricărui atac cibernetic este la îndemâna oricărui membru al societății, iar organele abilitate trebuie să le monitorizeze, sistematizeze și, ulterior, să le poată anticipa. Un rol important în acest proces îl constituie și cooperarea specialiștilor din breaslă, a companiilor IT și a autorităților competente la nivel național și internațional.

„Organizațiile active în industria serviciilor financiare încep să înregistreze progrese semnificative în implementarea Legii privind reziliența operațională digitală (*Digital Operational Resilience Act* – DORA), în acest context o treime dintre acestea (29%) au început să se pregătească încă din 2022 și, dintre acestea, 29% au finalizat deja, până în februarie 2023" [10].

„Raportul Deloitte evidențiază faptul că companiile sunt în urmă în ceea ce privește *evaluarea riscului generat de terți,* în condițiile în care șapte din zece organizații participante la studiu (69%) le efectuează doar o dată pe an, insuficient pentru a respecta cerințele DORA, în timp ce doar 13% le efectuează în mod continuu, așa cum cere noul regulament. Respectarea acestor cerințe implică, de asemenea, revizuirea periodică a strategiei privind riscul generat de furnizorii de soluții TIC, luând în considerare strategia de a distribui serviciile pe furnizori multipli" [10].

Pe parcursul implementării DORA, s-a observat că a devenit o provocare conectarea furnizorilor TIC cu cei ce oferă tehnologii critice. „Studiul evidențiază faptul că funcțiile considerate critice și importante sunt autorizarea (14%) și autentificarea

DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

tranzacțiilor de plată (12%), urmate de operațiunile IT și tranzacțiile efectuate de clienți prin intermediul canalelor digitale (12% fiecare)" [10].

Pentru a se conforma cerințelor DORA, entitățile vor trebui să-și determine punctele critice, a căror impact ar afecta serviciilor lor și rezultatele, și să-și actualizeze permanent lista furnizorilor TIC.

„Instituțiile financiare vor trebui să dezvolte metode de testare a scenariilor de reziliență și strategii multi-furnizor pentru toate sistemele care susțin funcții critice și importante". „DORA obligă instituțiilor financiare să efectueze anual *teste ale planului de răspuns la incidente* și să efectueze *teste de penetrare bazate pe amenințări (TLPT)* asupra tuturor sistemelor și aplicațiilor TIC critice și asupra funcțiilor importante, în mediul de producție" [1].

CONCLUZII

Putem concluziona că nevoia de protecție a tehnologiei informației crește în fiecare an pe măsură ce crește numărul și calitatea atacurilor hackerilor.

Relevanța problemei securității informațiilor este confirmată de statisticile atacurilor hackerilor. Multe organizații, în primul rând băncile, sunt victime ale programelor malware phishing sau furt de identitate.

Rezultatele DESI 2022 arată că, deși majoritatea statelor membre UE înregistrează progrese în transformarea digitală, însă întreprinderi bazate pe tehnologii digitale cheie: cloud-ul, inteligența artificială (AI) și Big Data, este încă destul de scăzută.

Competențele digitale insuficiente împiedică dezvoltarea, sporesc decalajul digital și deoarece majoritatea serviciilor sunt transferate online, cresc riscurile de securitate cibernetică.

Este necesară implementarea pe scară largă a infrastructurii de conectivitate (în special 5G), pentru a putea oferi și/sau beneficia de servicii bazate pe aplicații de ultimă generație.

Statele membre UE continuă să-și îmbunătățească nivelul de digitalizare, de aceeași dinamică se bucură și statele candidate la UE: Republica Moldova și Ucraina, care încearcă treptat și să recupereze până vor ajunge în urmă statele de top digitalizate.

BIBLIOGRAFIE

1. Regulamentul (UE) 2022/2554 al Parlamentului European și al Consiliului din 14 decembrie 2022 privind reziliența operațională digitală a sectorului financiar și de modificare a Regulamentelor (CE) nr. 1060/2009, (UE) nr. 648/2012, (UE) nr. 600/2014, (UE) nr. 909/2014 și (UE) 2016/1011 [online]. [Accesat 6 noiembrie 2023]. Disponibil: <https://Publications Office (europa.eu)>
2. UNDP. *63% of Ukrainians use state e-services, user numbers grow for third year in row – survey* [online]. [Accesat 6 noiembrie 2023]. Disponibil: <https://63% of Ukrainians use state e-services, user numbers grow for third year in row – survey | United Nations Development Programme (undp.org)>
3. Comisia Europeană. *Deceniul Digital al Europei* [online]. [Accesat 6 noiembrie 2023]. Disponibil: <https://Deceniul digital al Europei | Shaping Europe's digital future (europa.eu)>
4. Consiliul Uniunii Europene. *Finanțele digitale* [online]. [Accesat 8 noiembrie 2023]. Disponibil: <https://Finanțele digitale - Consilium (europa.eu)>

DOI: https://doi.org/10.53486/escst2023.06
International Conference, December 07-08, 2023, Chișinău, Moldova

5. Digital Economy and Society Index (DESI) 2022. Thematic chapters [online]. [Accesat 6 noiembrie 2023]. Disponibil: <https://The Digital Economy and Society Index (DESI) | Shaping Europe's digital future (europa.eu)>
6. Payment systems and methods in Ukraine [online]. [Accesat 8 noiembrie 2023]. Disponibil: https://Payment systems and methods in Ukraine [2022] (fin.do).
7. Internet use frequency in Ukraine in 2022. [online]. [Accesat 6 noiembrie 2023]. Disponibil: <https://Internet use frequency Ukraine 2022 | Statista>
8. PWC. *Băncile, asigurătorii și societățile de investiții trebuie să-și adapteze strategiile de securitate cibernetică la noile norme privind reziliența operațională digitală, adoptate de UE* [online]. [Accesat 18 noiembrie 2023]. Disponibil: <https://Băncile, asigurătorii și societățile de investiții trebuie să-și adapteze strategiile de securitate cibernetică la noile norme privind reziliența operațională digitală, adoptate de UE (pwc.ro)>
9. Sondaj Național Anual 2022. *Percepția, asimilarea și susținerea de către populație a e-Guvernării și modernizării serviciilor guvernamentale.* [online]. [Accesat 18 noiembrie 2023]. Disponibil: <https://raport_sondaj_anual_2022_rom_.pdf (egov.md)>
10. Studiu Deloitte: organizațiile din domeniul serviciilor financiare încep să înregistreze progrese în implementarea noului regulament UE privind reziliența operațională digitală, DORA. 31 iulie 2023 [online]. [Accesat 6 noiembrie 2023]. Disponibil: <https:// Studiu Deloitte: organizațiile din domeniul serviciilor financiare încep să înregistreze progrese în implementarea noului regulament UE privind reziliența operațională digitală, DORA>
11. Women in Digital Scoreboard 2022. Country profiles. [online]. [Accesat 18 noiembrie 2023]. Disponibil: <https://digital-strategy.ec.europa.eu/en/policies/desi>

Economic Security in the Context of Systemic Transformations
DOI: https://doi.org/10.53486/escst2023.07
International Conference, December 07-08, 2023, Chișinău, Moldova

LIMBA ROMÂNĂ – SIMBOL AL IDENTITĂȚII NAȚIONALE ȘI FACTOR DE SECURITATE STATALĂ

ROMANIAN LANGUAGE - SYMBOL OF NATIONAL IDENTITY AND FACTOR OF STATE SECURITY

Lucia CEPRAGA
PhD, Associate Professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0003-4253-2753
E-mail: cepragalucia@ase.md

Svetlana BÎRSAN
PhD, Associate Professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0001-8349-2714
E-mail: birsan.svetlana@ase.md

Abstract: *According to international standards, the official language of a nation state represents an element of national security, as well as the symbolism of the state, along with the flag, coat of arms, anthem and other national symbols. Language is the guarantor of a company's functionality. The current reality demonstrates the increasing degree of state involvement in the most diverse processes: social, cultural, economic, educational, etc. The language policy of a state is represented by a set of laws, rules and guidelines adopted by the state authorities in relation to the language or languages existing or used on the territory of that country. This includes the adoption of an official language, determines its learning, the status of minority languages as well as the attitude of reporting and protecting the language against the influence of foreign cultures. In this vein, language has become for the political domain of a state an object, resource and means of control. Through language policies, adopted as administrative measures, the State administers linguistic pluralism.*

Keywords: *language policy, Romanian language, state security, national identity, hybrid war.*

UDC: *811.135.1:342.31(478)*

JEL Classification: *F52, I21, I25, P36*

INTRODUCERE

Limba este garantul funcționalității unei societăți. Totodată, limba este factorul care stă la baza dezvoltării socioculturale a macro/microsocietăților, precum și factorul lingvistic ce duce la consolidare lexicului unui sistem terminologic. Aderând la ideea că viața economică reprezintă temelia materială a unei societăți, susținem și dezvoltarea calitativă a unei societăți economice este de neimaginat fără stabilirea clară a identității termenilor economici. In grosso modo, se poate spune că interesul specialiștilor din varia domenii, sistemul economic, în acest sens nu este o excepție, este unul adânc implantat în timp. Încă renumitul Adam Smith, supranumit părintele economiei, abordează, în lucrarea *Teoria sentimentelor morale*, problema limbii, mai exact facultatea vorbirii ca instrument al „al conducerii și al orientării judecăților și comportării celorlalți oameni.” [1]

Profesorul Vasile Bahnaru, într-un interviu acordat Agenției de presă IPN, susține „ Limba constituie un însemn fundamental indispensabil al patrimoniului cultural dintr-un stat, întrucât statele s-au constituit, în principiu, în baza comunității de limbă, cu alte cuvinte limba, tradițiile, cultura populară sunt elementele constituente fundamentale ale

DOI: https://doi.org/10.53486/escst2023.07
International Conference, December 07-08, 2023, Chișinău, Moldova

unui stat, iar celelalte însemne ale statului (sigiliul, drapelul, imnul, stema, distincțiile, moneda etc.) au un caracter derivat și cunosc o succesiune cronologică posterioară limbii. Prin urmare, limba este de o importanță decisivă, chiar definitorie pentru existența statului, întrucât ea este liantul social și înglobează, exprimă și prin ea se manifestă toate aspectele, chintesența culturală a unui popor, constituit din ansamblul bunurilor materiale și spirituale, din ansamblul preceptelor cutumiare și tradițiilor milenare ale majorității naționale. Este, prin urmare, un fapt incontestabil că elementul principal de constituire a unu stat și al culturii unui popor este limba lui." [2]

„Odată ce a devenit clar că limba este unul dintre cei mai importanți factori determinanți ai identității și un factor puternic în unirea popoarelor, limba a început să fie studiată pe scară largă cu scopul unificării și standardizării acesteia."[4] Mai mult, realitatea actuală demonstrează creșterea gradului de implicare a statului în cele mai diverse procese: sociale, culturale, economice, educaționale etc. Potrivit cercetătorilor Fishman, Grillo, „limba a devenit pentru domeniul politic al unui stat obiect, resursă și mijloc de control".[4] Prin politicile lingvistice, adoptate drept măsuri administrative, statul gestionează pluralismul lingvistic.

REZULTATELE CERCETĂRII

Apărut în anii 70 ai secolului al XX-lea, conceptul de *politică lingvistică* este definit drept „o serie de proceduri prin care instituții, grupuri sau indivizi dintr-o societate influențează în mod indirect sau direct limbajul, utilizarea limbii și situația lingvistică într-un segment al societății, al întregii societăți sau în mai multe societăți sincrone".[5] Cercetătorul Škiljan abordează conceptul de politică lingvistică ca pe niște „activități raționale și, în mare parte, instituționalizate, prin care o societate influențează formele lingvistice de comunicare publică și formarea conștientizării participanților săi despre aceste forme".[6]

Premergătorul lexical, cu circa un deceniu, al termenului *politică lingvistică* este considerat conceptul *planificare lingvistică*. „Termenul planificare lingvistică (language planning) a fost introdus în circulație de Einar Haugen, lingvist american de origine norvegiană, în anul 1959, cu ocazia prezentării activităților de standardizare lingvistică efectuate în Norvegia".[3]

Cercetătorul Sue Wright susține că „stimularea convergenței lingvistice a fost o parte a dezvoltării statului național. Limba unificată promovează coeziune care permite statului să dezvolte o cultură comună. Lideri politici au devenit conștienți că o comunitate de comunicare unificată este calea spre construirea unui stat-națiune".[3]

Politica lingvistică statală se materializează printr-un cadru normativ riguros care reflectă direcțiile adoptate de factorii de decizie în raport cu limba sau limbile ce funcționează pe teritoriul respectivei țări. Politica lingvistică vizează și adoptarea unei limbi oficiale, care motivează și încurajează învățarea acesteia. Politica lingvistică are un impact direct asupra statutului pe care îl obțin limbile minoritare, totodată, determinând și atitudinea în raport cu protejarea unei limbi față de înrâuririle culturilor străine.

Politica lingvistică poate fi interpretată și ca un ansamblu de măsuri de stat, ce vin să garanteze funcționalitatea unei limbi, prin anumite reglementări, pentru țara respectivă. De asemenea, politica de limbă se poate referi nu doar la un stat, dar și la anumite asociații/parteneriate etc. de organizațiile internaționale, precum este, spre exemplu, Uniunea Europeană.

DOI: https://doi.org/10.53486/escst2023.07
International Conference, December 07-08, 2023, Chișinău, Moldova

Regretatul profesor Gh. Moldovanu, în studiul *Politică și planificare lingvistică*: *abordare teoretică și aplicativă*,[6] supune atenției cititorului o analiză a mai multor tipuri de politici lingvistice, precum:

- *politica lingvistică liberală*, specifică Australiei, Austriei, Japoniei, Cubei, SUA, Germaniei etc.;
- *politica lingvistică dirijistă*, atestată în Iran, Afganistan, Vietnam, Grecia, Irak, Turcia, precum și în regiunea Transnistria din RM, politică susținută de autoproclamata guvernare locală.

În categoria *politică lingvistică dirijistă* se pot distinge un șir de subcategorii (vezi tabelul 1).

Tabelul 1: Subcategorii ale politicii lingvistice dirijiste

Subcategoria de politică dirijistă		**Țările care aplică PL**
Politica de asimilare		Iranul, Grecia, Irakul, Afganistanul Brazilia, Indonezia, , Turcia, Vietnamul etc.
Politica de valorificare a limbii oficiale		Algeria, SUA, Croația, Țările Baltice, Italia, România, Albania, etc.
Politica lingvistică pe domenii de activitate		Franța, Alaska, Luiziana, Corsica, Arizona, Monaco, Marea Britanie în Scoția etc.
Politica statului juridic diferențiat		Slovacia, Olanda, Albania, China, Țările Baltice, România, Bulgaria, Suedia etc.
Politica bilingvismului oficial (PBO):		
A	*PBO bazat pe drepturile personale fără limită teritorială*	Ciad, Kenya, Burundi, Irlanda, Norvegia, Malta, Canada, Bielorusia, etc.
B	*PBO bazat pe drepturile personale limitate la anumite regiuni*	Hawai (SUA), Scoția, Catalonia, Galiția, Țara Bascilor, Țara Galilor (Marea Britanie) și altele
C	*PBO bazat pe drepturile teritoriale*	Belgia, Canada (Québec) Elveția, etc.
Politica plurilingvismului strategic		Slovenia, Luxemburg, Ungaria, Africa de Sud, Australia, Moldova, Nigeria, India
Politica lingvistică mixtă		Germania, Irlanda de Nord, Panama, Cehia etc

Sursa: elaborat de autoare în baza informațiilor din referința [7]

Având în vedere caracterul social al limbii, considerăm pe deplin întemeiat rolul determinant al statului de „...distribuitor al bunului lingvistic”. [9] Cu atât mai îndreptățite sunt intervențiile statului în condițiile actuale de maximă instabilitate sociopolitică în regiune și de război hibrid. Potrivit directorului adjunct al Institutului pentru Politici și Reforme Europene, Mihai Mogîldea, un război hibrid e diferit față de cel despre care am învățat la școală la lecțiile de istorie... Nu este vorba de războaiele de cândva cu mecanisme tehnice, ci, mai curând, ne referim la acele instrumente care au capacitatea de a conduce la atingerea aceluiași scop, adică înfrângerea adversarului. „De cele mai multe ori, ținta unui război hibrid este un stat care se află în vizorul unui alt stat agresor, deci avem un stat agresor pe de o parte, care încearcă prin mai multe metode să slăbească, să

DOI: https://doi.org/10.53486/escst2023.07
International Conference, December 07-08, 2023, Chișinău, Moldova

vulnerabilizeze, să minimizeze reziliența belică a celuilalt stat. Aceasta este prima diferență când auzim termenul de război hibrid – trebuie să înțelegem că el este diferit de unul convențional.

Un alt moment relevant vizează faptul că termenul *hibrid* este orientat spre o paletă largă de elemente valorificate de către statul agresor. În acest caz, putem avea atacuri cibernetice, putem avea instrumente de dezinformare, putem avea, de exemplu, sistări de energie, de gaz, curent electric, putem avea inclusiv alte mecanisme cu care operează statul agresor, precum, de exemplu, finanțarea unor partide politice care, prin intermediul alegerilor – organizate de altfel într-un mod democratic – ar trebui să preia puterea și să răspundă comenzilor statului agresor. Deci, războiul hibrid, dacă dorim să-l observăm cum arată în realitate, trebuie să ne uităm la experiența noastră din ultimii ani și vom vedea că acesta se manifestă pe mai multe fronturi și că, de altfel, a reușit mai mult sau mai puțin să vulnerabilizeze statul nostru care, în ultimul an, cel puțin încearcă să-și recapete din capacitatea de răspuns, de luptă, încearcă să-și consolideze mai multe capacități care în trecut îi lipseau." [10]

Mihai Mogîldea, în dialogul cu Ana Sârbu, pe portalul *Mediacritica - primul portal de educație mediatică,* subscrie opiniei mai multor analiști, experți, atunci când susține că „astăzi unul din grupurile - țintă care a căzut victimă a acestui război este populația Republicii Moldova. Nu atât guvernarea, nu atât instituțiile care conduc statul, ci mai degrabă populația, pentru că statul agresor (nr. Federația Rusă) dorește să influențeze gândirea, deciziile, opțiunile de vot ale populației." [10]

În acest context de instabilitate sociopolitică din țară, securitatea populației Republicii Moldova devine un imperativ. Informația socială a unui stat constituie expresia tuturor particularităților naționale, psihosociale, a intereselor și necesităților acestuia. În conjunctura acestei informații sociale, un caracter specific comportă informația cu conținut social-politic, ideologic, care este elaborată și aleasă de pe anumite poziții – politice, ideologice. Bunăoară, e cunoscut faptul că, în circumstanțele unor abordări social-politice, filosofice, „omul este un fenomen social, deoarece constitui un consumator al informației sociale a statului, grupului social, națiunii din care face parte." [11]

Mai marii statului, guvernarea, dețin instrumentele necesare de securizare a națiunii. Indiscutabil, s-au întreprins măsuri de alfabetizare politică, alfabetizare mediatică, lingvistică etc.

În ultimul an, am putut observa activizarea Guvernului la capitolul promovarea imaginii RM pe plan internațional, atragerea fondurilor financiare întru dezvoltarea infrastructurii naționale și regionale, întru susținerea păturilor vulnerabile, precum și în ceea ce privește lupta împotriva dezinformării de către sursele media pro ruse.

Implicații substanțiale a demonstrat Guvernul Republicii Moldova și la nivel de implementare a politicilor lingvistice. Or, în temeiul prevederilor art. 10 din Codul educației al Republicii Moldova nr.152 din 17 iulie 2014 (Monitorul Oficial al Republicii Moldova, 2014, nr. 319-324, art. 634) și în conformitate cu Programul de guvernare „Moldova vremurilor bune", Guvernul Republicii Moldova a aprobat la 07.03.2023 *Programul național privind învățarea limbii române de către minoritățile naționale, inclusiv populația adultă, pentru anii 2023-2025*, oferit gratuit de către Ministerul Educației și Cercetării al RM.

Elaborat în conformitate cu următoarele documente: Strategia națională de dezvoltare „Moldova 2030", Programul de guvernare „Moldova vremurilor bune", Obiectivele Dezvoltării Durabile „Educația 2030", Competențele-cheie pentru învățarea pe

DOI: https://doi.org/10.53486/escst2023.07
International Conference, December 07-08, 2023, Chișinău, Moldova

parcursul întregii vieți (Bruxelles, 2018), Codul educației (2014), *Programul național privind învățarea limbii române de către minoritățile naționale, inclusiv populația adultă, pentru anii 2023-2025*, a fost dictat de un șir de factori intrinseci, precum și extrinseci.
Printre factorii intrinseci ai documentului menționat supra, amintim:

- ✓ „necesitatea de a dezvolta un sistem de educație lingvistică sustenabilă pentru toate părțile interesate, fără deosebire de vârstă și profesie;
- ✓ necesitatea creării unui mecanism de asigurare a competitivității limbii române la cel mai înalt nivel sociolingvistic;
- ✓ necesitatea promovării patrimoniului cultural național ca un element definitoriu al identității naționale;
- ✓ necesitatea consolidării instituționale prin adoptarea unui cadru normativ, raliat la nevoile comunității".[12]

Factorii extrinseci care au dictat elaborarea și aprobarea *Programului național privind învățarea limbii române de către minoritățile naționale, inclusiv populația adultă, pentru anii 2023-2025* sunt:

- ✓ „necesitatea ralierii politicilor educaționale naționale la documentele și acordurile internaționale care vizează și R. Moldova, la documentele elaborate de ONU, Consiliul Europei, Uniunea Europeană, OECD și alte organisme internaționale, la Obiectivele de Dezvoltare Durabilă (ODD), la prevederile Acordului de Asociere cu Uniunea Europeană și Parteneriatul Global pentru Educație, la Cadrul European Comun de Referință pentru Limbi;
- ✓ necesitatea transferului și implementării în sistemul de educație lingvistică al Republicii Moldova a unor experiențe, inovații și bune practici internaționale." [12]

Totodată, experții își exprimă speranța că, odată cu dezvoltarea Programului național privind studierea gratuită a limbii române, autoritățile vor depune eforturi pentru ca școală deja să aducă cunoștințe elevilor, inclusiv acelor alolingvi, la nivelul încât aceștia să poată să-și realizeze potențialul pe care îl au de la natură în societate. [13]

CONCLUSIONS

În concluzie, din cele sus-menționate, derivă statutul ***limbii române*** atât ca **simbol de stat, simbol al identității naționale și instrument de coeziune socială**, cât și **factor de securitate națională**.

Or, „în condiții de război hibrid, este important să știm cine suntem, pentru a nu ne trezi alții... Prezervarea și valorificarea patrimoniului cultural și natural, precum și încurajarea responsabilă a domeniilor de excelență, ca modalitate de promovare a propriei identități, reprezintă obiective naționale de securitate. Între timp, lângă noi, în Ucraina, dreptul internațional umanitar, convențiile internaționale, drepturile culturale nu sunt respectate." [14]

Potrivit cercetătorului Wright „răspândirea cu succes a limbii naționale a fost ajutată de presiunea industrializării și a comerțului. Acolo unde industrializarea și construirea națiunii a avut loc mai târziu, Wright scrie că și răspândirea alfabetizării a fost întârziată; numai jumătate din populația românească a fost alfabetizată în anul 1920. Wright susține că scopul achiziției lingvistice este „socializarea tinerilor membri ai grupului în limba națiunii și discursul național".[3]

Și dacă anterior, formele industriale de producție au necesitat schimbări în educație, atunci actualmente, securitatea națională a populației reclamă adoptarea mai multor măsuri strategice de securitate, inclusiv în domeniul politicii lingvistice. E adevărat, „Statul

DOI: https://doi.org/10.53486/escst2023.07
International Conference, December 07-08, 2023, Chișinău, Moldova

Republica Moldova demonstrează un interes deosebit pentru afirmarea individului și a comunităților minorităților naționale prin sporirea gradului de implicare a acestora în viața socială, culturală, economică și politică a țării. Integrarea individului în societate, participarea sa activă la viața comunității reclamă respectarea unor condiții de bază privind asigurarea drepturilor și libertăților omului".[12]

Astfel, limba română, limba oficială a statului Republica Moldova se prezintă ca un cod lingvistic de procesare și gestionare a informațiilor, ca un instrument de integrare socioprofesională și culturală, iar drept urmare de coeziune socială și bună conviețuire într-un stat de drept, unde limba este catalizatorul societății și factorul de securitate culturală.

BIBLIOGRAFIE

1. MUNTEANU, C., Comunicare și leadership. De la Adam Smith la R.G. Collingwood. În *Revista „Limba Română". Revistă de știință și cultură*. Chișinău, nr. 2, anul XXIX, 2019. ISSN 0235-9111 [văzut decembrie 2023]. Disponibil: https://limbaromana.md/index.php?go=articole&n=3712
2. BAHNARU, Vasile. Limba este de o importanță definitorie pentru existența statului. Interviu IPN. În *IPN. Agenție de presă independentă.* Chișinău. [văzut decembrie 2023]. Disponibil: https://www.ipn.md/ro/limba-este-de-o-importanta-definitorie-pentru-existenta-statului-interviu-7978_1029311.html#ixzz8QQncGyNs
3. OLUJIĆ, V., RADOSAVLJEVIĆ, P., *Politică și planificare lingvistică: varietăți ale limbii române în Europa de sud-est.* Zagreb. 2021 [văzut noiembrie 2023]. // Disponibil: https://repozitorij.unizg.hr/islandora/object/ffzg%3A3629/datastream/PDF/view
4. OTEANU, E. *Politica lingvistică și construcția statală în Republica Moldova*, 2021 [văzut noiembrie 2023]. Disponibil: https://ro.scribd.com/document/199315691/Cap-1-Politica-Lingvistica
5. RAJIĆ, Lj., apud OLUJIĆ, V., RADOSAVLJEVIĆ, P. *Politică și planificare lingvistică: varietăți ale limbii române în EUROPA de sud-est*. p. 4. 2021 [văzut decembrie 2023]. Disponibil: https://repozitorij.unizg.hr/islandora/object/ffzg%3A3629/datastream/PDF/view
6. ŠKILJAN, D., apud OLUJIĆ, V., RADOSAVLJEVIĆ, P. *Politică și planificare lingvistică: varietăți ale limbii române în EUROPA de sud-est.* p. 5. 2021 [văzut decembrie 2023]. Disponibil: https://repozitorij.unizg.hr/islandora/object/ffzg%3A3629/datastream/PDF/view
7. Politica lingvistică. Temei juridic. 2021 [văzut decembrie 2023]. Fișe tehnice UE – 2017 Disponibil: https://www.europarl.europa.eu/RegData/etudes/fiches_techniques/2013/051306/04A_FT(2013)051306_RO.pdf
8. MOLDOVANU, Gh., *Tipologia politicilor lingvistice.* În *Revista „Limba Română". Revistă de știință și cultură*. Chișinău, nr. 1-3, anul XV, 2005. ISSN 0235-9111 [văzut decembrie 2023]. Disponibil: https://www.scribd.com/document/383411192/308142915-Moldovanu-G-Politica-Lingvistica-doc
9. KLINKENBERG, J-.M., *Les politiques linguistiques: pour qui? pour qoui?, în Français de l'avenir, avenir du français*, Paris, Didier, 2000, p. 105

DOI: https://doi.org/10.53486/escst2023.07
International Conference, December 07-08, 2023, Chișinău, Moldova

10. SÂRBU, A., Ce este un război hibrid și cum afectează Republica Moldova. Podcast-CuMINTE. În *„MEDIACRITICA. Primul portal de educație mediatică”,* Chișinău. 2023 [văzut noiembrie 2023]. Disponibil: https://mediacritica.md/podcast/ce-este-un-razboi-hibrid-si-cum-afecteaza-republica-moldova/ [văzut noiembrie 2023].
11. BUTUC M. Limba oficială, factor decisiv al securității naționale. *Revista Militară. Studii de securitate și apărare.* Chișinău, nr. 2 (16)/2016, pp. 78-82 [văzut noiembrie 2023]. Disponibil: https://ibn.idsi.md/sites/default/files/imag_file/79_82_Limba%20oficiala%2C%20factor%20decisiv%20al%20securitatii%20nationale.pdf
12. Programul național privind învățarea limbii române de către minoritățile naționale, inclusiv populația adultă, pentru anii 2023-2025 [văzut noiembrie 2023]. Disponibil: https://gov.md/sites/default/files/document/attachments/subiect-03-nu-32-mec.pdf
13. BOȚAN, I. Programul național gratuit pentru învățarea limbii române este unul întârziat. În *IPN. Agenție de presă independentă.* Chișinău, 04.09.2023 [văzut noiembrie 2023]. Disponibil: https://www.ipn.md/ro/igor-botan-programul-national-gratuit-pentru-invatarea-limbii-romane-8004_1099201.html
14. TODORAN, M. *Vulnerabilități, riscuri și amenințări la adresa identității naționale. „Geopolitica”. Revistă de geografie politică și Geostrategie.* [văzut noiembrie 2023]. Disponibil: https://www.geopolitic.ro/2022/08/vulnerabilitati-riscuri-si-amenintari-la-adresa-identitatii-nationale/

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.08
International Conference, December 07-08, 2023, Chișinău, Moldova

VENITURILE, CHELTUIELILE DE CONSUM ȘI CONSUMUL ALIMENTAR

INCOME, CONSUMPTION EXPENDITURE AND FOOD CONSUMPTION

Profira CRISTAFOVICI

PhD, Associate professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0001-5582-0231
E-mail: cristofprof@gmail.com

Abstract: *In the current socio-economic context of crisis, accompanied by the significant increase in prices, major concerns are imposed to ensure the well-being of the population, both in the Republic of Moldova and in other states. The well-being of the population, in turn, is determined by the interconnection between income and consumption. A higher level of the population's income leads to higher consumption, and the discrepancies between the incomes of different social categories affect their security and quality of life. The security and quality of people's lives also depends on the purchasing power of households, the quantitative value of consumption, its structure and quality, as well as the assimilated and promoted conceptions of consumption, the social policy of the state. In this paper, the income and consumption expenditure situation of the population in the Republic of Moldova is analyzed based on documentation from statistical sources, as well as other secondary sources of information. Also, the analysis of food consumption of basic products in the Republic of Moldova in comparison with Romania is carried out. The research showed that in the Republic of Moldova the incomes of the population, compared to neighboring countries, are at a lower level, 41% being spent, according to the family budget research, for food consumption. In general, the level of provision of the population with basic food products is appreciated as satisfactory, but there are significant gaps between different categories of consumers, which requires the support of these categories by the state and society.*

Keywords: *income, consumption expenditure, food consumption, security.*

UDC: *330.564.2:330.567.22(478)*

JEL Classification*: I16, I31, I32, I38.*

INTRODUCERE

Viața este singura valoare inestimabilă, care este posibilă doar satisfăcând nevoile existențiale prin consum. Consumul calitativ nu este un scop în sine al vieții omului, dar este condiția existențială a lui. Conștientizarea acestui fapt de însăși om, în calitatea sa de consumator/prosumator, precum și în calitate de furnizor a experiențelor de consum, determină calitatea vieții într-o societate. Totodată, se cunoaște faptul că orice persoană, familie, firmă sau chiar și stat, indiferent de nivelul său de dezvoltare, sunt limitați în posibilitățile sale de satisfacere a necesităților din cauza insuficienței resurselor (limitelor bugetare), precum și alte motive, de exemplu, de timp [1, p.16]. Atât consumul în general, cât și consumul alimentar, în particular, depind de veniturile populației, direcționarea acestora spre procurarea diferitor tipuri de produse și servicii, precum și de gestionarea problemelor legate de consum de către factorii de decizie la nivel de întreprinderi și societate. Consumul are un impact considerabil asupra economiei și societății. O consecință esențială a dezvoltării consumului o reprezintă creşterea cererii agregate pe piaţă. Aceasta, la rîndul său, determină volumul de producere şi, respectiv, conduce la creşterea cererii de forţă de muncă şi veniturilor cetăţenilor. Pe lângă impactul economic,

DOI: https://doi.org/10.53486/escst2023.08
International Conference, December 07-08, 2023, Chișinău, Moldova

consumul are şi o profundă semnificaţie socio-culturală, efectele sale fiind resimţite pe diferite planuri: competitivitatea produselor, deprinderile și obiceiurile de consum, instruirea şi educaţia populaţiei ţării, conservarea tradiţiilor şi culturii locale, utilizarea timpului liber, creşterea calităţii vieţii. Un nivel înalt al calității vieții populației presupune consumul bunurilor calitative, sigure, în concordanță cu normele fiziologice și normele raționale de consum, într-un mediu de viață sănătos.

SITUAȚIA VENITURILOR, CHELTUIELILOR DE CONSUM ȘI CONSUMULUI ALIMENTAR

Nivelul de trai al populației unei țări își găsește reflectare (condiționat) în indicatorul macroeconomic Produsul intern brut (PIB). Analiza evoluției acestui indicator în perioada anilor 2010-2022 (tabelul 1) denotă o creștere continuă, cu excepția anilor 2020 și 2022 (91,7% și 95% respectiv, în comparație cu perioada precedentă) [2]. În anul 2022 acest indicator a atins cifra de 274207 milioane lei în prețuri curente, „consumul final al gospodăriilor populației" constituind 83,6% din PIB, iar investițiile fiind în descreștere. PIB pe cap de locuitor în anul 2022 a constituit 5713 $ USD (în prețuri curente) [3].

Pentru comparație, conform calculelor Băncii Mondiale, cel mai înalt PIB pe cap de locuitor (PPC) - 234,3 mii $ SUA, a fost înregistrat în anul 2021 de țara Monaco, urmând Luxemburgul cu 133,7 mii $, Irlanda -101,1 mii $, SUA - 69,2 mii $, Germania -51,1 mii $, Japonia - 39,6 mii $, Spania - 30,1 mii $, Polonia-17,7 mii $, România-14,7 mii $, Bulgaria și Rusia -12,2 mii $, Turcia - 9,7 mii $, Ucraina - 4,6 mii $, Moldova - 4468 dolari (5274 $ conform datelor statistice ale țării), iar cel mai scăzut nivel s-a înregistrat în Yemen - 302 $, Burundi - 311$, Afganistan - 373$ [4]. Este evident nivel scăzut al acestui indicator al Republicii Moldova, comparativ cu țările din regiune, precum și amplitudinea enormă dintre cele mai sărace și cele mai dezvoltate state.

În anul 2022, câștigul salarial mediu lunar brut a constituit 10529,11 lei și s-a mărit față de anul 2021, în valoare nominală, cu 15,5%, iar în valoare reală (ajustat la indicele prețurilor de consum) s-a micșorat cu 10,3%. Din toți salariații, aproximativ 42% au avut salarii mai mici de 7 mii lei, iar cumulativ, 66% au avut salarii mai mici 10 mii lei; 19% – au avut salarii între 10 și 15 mii lei, 15% au avut salarii între 15-20 mii lei și 0,3 % peste 20 mii lei, amplitudinea extinzându-se de la 6850 până la 26537 lei (salariații în domeniul Informații și telecomunicații) [3, p. 11]. Salariul minim pe țară în anul 2022 a alcătuit 3500 lei, iar în anul 2023 - 4000 lei sau circa 200 euro [5].

O astfel de stratificare a populației după veniturile disponibile arată că marea majoritate (salariați + pensionari) fac parte din păturile social vulnerabile, inflația accentuând și mai mult nivelul scăzut de trai al gospodăriilor. De asemenea, există mari discrepanțe între grupurile sociale în ceea ce privește consumul. Pentru a atenua impactul inflaționist, majoritatea țărilor UE au majorat salariile minime pe țară. Republica Moldova, în concordanță cu Directiva UE, optează, de asemenea, pentru majorarea salariului minim de la 4000 lei în 2023 până la 5000 lei, începând cu anul 2024. Pentru comparație, salariile minime în UE în iulie 2022 variau între valoarea maximă 2313 euro în Luxemburg și valoarea minimă 363 de euro în Bulgaria. Salariu minim peste 1700 de euro îl aveau Belgia, Irlanda, Țările de Jos, Germania, 1646 euro avea Franța. Salariu minim sub 1.000 de euro a fost înregistrat în 13 dintre statele membre UE, inclusiv și România - 516 euro, iar în țările candidate și potențial candidate - 269 de euro în Albania și 532 de euro în Muntenegru [7]. Nivelul scăzut al veniturilor populației este unul din factorii principali care determină emigrarea populației apte de muncă către țările cu un nivel de trai mai înalt, ceea ce se confirmă și prin tendința de micșorare continuă a numărului populației (tabelul 1).

DOI: https://doi.org/10.53486/escst2023.08
International Conference, December 07-08, 2023, Chișinău, Moldova

Tabelul 1. Evoluția PIB, PIB pe cap de locuitor și a câștigului salarial în Republica Moldova

Indicatori	2010	2015	2017	2018	2019	2020	2021	2022
Produsul Intern Brut (PIB), mil.lei, în prețuri curente	86275, 4	145754	178881	192509	206256	199734	242079	274207
Produsul Intern Brut, (în preț. comp.), mil lei	...	133030 ,1	168358, 0	197616, 6	195779	189187	227557	219937
Indicele deflator al PIB,100=anul precedent, %	102.3	109,6	106,3	104.1	103.6	91,7	113,9	95,0
PIB, prețuri curente, mil $SUA	6976, 6	7746,2	9674, 4	11176,0	11736,o	11532, 0	13691, 0	14 506
PIB, prețuri curente, mil Euro	5260, 9	6974,5	8588,4	9955,9	10484,0	10116, 0	11569, 0	13 781
Populația stabilita la 1 ianuarie, mii pers.	3561,6	3555,2	3550,9	3371,3	2664,9	2635,3	2616,5	2565,0
PIB pe locuitor, prețuri curente, $SUA	1 959	2 180	2 724	3315	4405	4376	5274	5713
Câștigul salarial mediu lunar brut, lei	2971,7	4610,9	5697,1	6268,0	7356,1	8107,5	9115,9	10529, 1
Indicele câștigului salarial mediu lunar brut al unui lucrător din economie, %	108,2	110,5	112,1	113,2	108,2	110,2	112,4	115,5

Sursa: elaborat în baza datelor statistice: [2], [3, p.22].

Conform datelor statistice, veniturile disponibile lunare ale populației din Republica Moldova au constituit în anul 2022 (tabelul 2), în medie pe o persoană, 4252,7 lei (5355,3 în mediul urban și 3528,4 în mediul rural), ceea ce este cu 21,2% mai mult comparativ cu anul precedent, în condițiile unui indice anual cumulativ al inflației de 130,2 %, inclusiv 132 % pentru produsele alimentare. Sursele bănești constituie 97,2% pentru mediul urban și 89,8% pentru mediul rural. Salariul formează 61,1 % din veniturile totale în mediul urban și 40,3 în mediul urban, iar prestațiile sociale – 20,3 % și transferurile bănești -12,1% [3, p.12].

Tabelul 2. Veniturile medii lunare pe o persoană în anul 2022, lei

Indicatori	Total	Mediul urban	Mediul rural
Veniturile disponibile totale, medii lunare pe o persoană, lei	4 252,7 5	5 355,3	3528,4
Inclusiv în % pe surse de venit			
Activitatea salarială	50,7	61,1	40,3
Activitatea individual agricolă	7,8	0,6	15,1
Activitatea individual agricolă non-agricolă	6,2	6,8	5,6
Prestațiile sociale	20,3	16,8	23,8
Alte venituri, inclusiv transferuri din afara țării	15,0 12,1	14,7 10,4	15,2 13,7

Sursa: [3, p.12]

DOI: https://doi.org/10.53486/escst2023.08
International Conference, December 07-08, 2023, Chișinău, Moldova

Cea mai mare parte din veniturile disponibile ale gospodăriilor este îndreptată spre cumpărarea produselor alimentare și băuturilor nealcoolice - 41,1%,inclusiv 36% în mediul urban și 46,4% în mediul rural, urmând cheltuielile pentru locuință , apa, electricitate și gaze – 16,3%, îmbrăcăminte și încălțăminte - 8,4%, transport -7,4%, mobilier , dotare și întreținerea locunței – 5,8%, sănătate – 5,1% ș.a. (Figura 1).

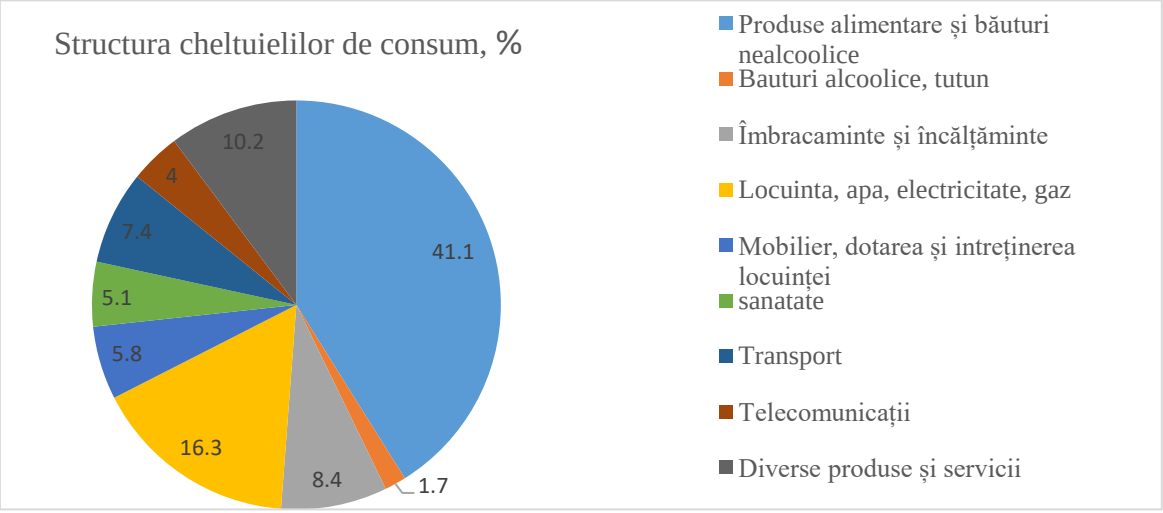


Figura 1. Structura cheltuielilor de consum în anul 2022
Sursa: [3, p.13]

Vulnerabilitatea populației este și mai mare, dacă vom lua în considerare mărimea gospodăriei, cheltuielile medii a unei familii cu 5 și mai multe persoane fiind aproape de două ori mai mici, comparativ cu gospodăria cu o persoană, cheltuielile principale fiind legate de alimente (45,8% din totalul cheltuielilor) [3, p.13]. Pentru comparație, venitul disponibil al gospodăriilor cheltuit pentru produsele alimentare și băuturi nealcoolice în România a alcătuit în anul 2021 34,4%, în țările UE-27- în mediu 14,7 %, iar în țările dezvoltate acest indicator variază între 10-15% [7].

Cercetările arată că o treime din populația terei trăiește în sărăcie, polarizarea societăților aprofundându-se. În Republica Moldova nivelul sărăciei extremale în anul 2021 a constituit 2095 lei în mediul urban și 1689,7 lei în mediul rural, nivelele sărăciei extremale înregistrate fiind 24,5 % media pe țară , 11,9% în mediul urban și 32,8% în mediul rural [8, p.5].

Tabelul 3. Evaluarea produselor alimentare incluse în coșul alimentar al minimului de existență prin prizma criteriilor de securitate alimentară

Grupe de produse	Disponibilitate	Accesibilitate	Stabilitate
Pâine și produse de panificație	satisfăcător	satisfăcător	nesatisfăcător
Carne și produse din carne, inclusiv carne de pasăre	satisfăcător/ parțial satisfăcător	satisfăcător/ parțial satisfăcător	parțial satisfăcător
Lapte și produse lactate	nesatisfăcător	nesatisfăcător	parțial satisfăcător
Pește și produse din pește	nesatisfăcător	parțial satisfăcător	satisfăcător

DOI: https://doi.org/10.53486/escst2023.08
International Conference, December 07-08, 2023, Chișinău, Moldova

Ouă	satisfacător	satisfacător	satisfacător
Grăsimi	satisfacător	satisfacător	parțial satisfăcător
Zahăr și produse de cofetărie	satisfacător	satisfacător	nesatisfacător
Cartofi	satisfacător	satisfacător	parțial satisfăcător
Legume	satisfacător	satisfacător	parțial satisfăcător
Culturi de bostănărie	satisfacător	satisfacător	parțial satisfăcător
Fructe, pomușoare, struguri	satisfacător	satisfacător	parțial satisfăcător
Alte produse (ceai, sare, drojdie, frunză de dafin)	partial satisfacător	partial satisfacător	partial satisfacător

Sursa: adaptat după [8,p.33-39];[9]

Evaluarea produselor alimentare incluse în coșul alimentar al minimului de existență prin prizma criteriilor de securitate alimentară, la nivel de țară, relevă o situație relativ satisfăcătoare, cu excepția produselor lactate și produselor și a cărnii de gainăși bovine, care au o disponibilitate mai scăzută, însă accesibilitatea este mai problematică pentru păturile cu venituri scăzute și există probleme de stabilitate în asigurarea cu produse ce țin de condiții climaterice, exportul sau importul produselor ș.a.

Tabelul 4. Consumul anual pe cap de locuitor, kg

Categorii de produse	**Consumul în Republica Moldova, 2021**	**Nivel de autoaprovizionare, %**	**Consumul în România, 2020**
Cereale și produse din cereale, echivalent cereale (grâu, porumb și derivate)	205	165	204,4
Cartofi	78	89,1	93,4
Leguminoase/ boabe	5,7	165,5	3,6
Legume și produse din legume, echivalent legume proaspete	88	96,1	167,8
Fructe si produse din fructe in echivalent fructe proaspete	31consum populatie /115consum industrie mere , pere, gutui	156,7	107,6
Zahar si produse din zahar in echivalent zahar (inclusiv miere)	16,3 zahar populatie+ 16.3 zahar industrie	105,8	25,5
Carne si produse din carne in echivalent carne proaspătă	57	75	74,4
Lapte si produse din lapte in echivalent lapte 3,5% grăsime (exclusiv unt)	170	66,2	260,2
Ouă	183-populație/ 220- industrie	100,5	360 Finlanda
Peste și produse din peste în echivalent peste proaspăt	5,3	39,4 în raport cu norma recomandată	6,3
Vin si produse din vin (litri)	29	>100	21,1

Sursa: [3, p.33-39], [7, p.45]

DOI: https://doi.org/10.53486/escst2023.08
International Conference, December 07-08, 2023, Chișinău, Moldova

Analiza comparativă a consumului alimentar anual pe cap de locuitor a principalelor categorii de produse în Republica Moldova și România indică diferențe semnificative în consumul: *legume și produse din legume* - de aproape două ori mai mult în România; *zahăr și produse din zahăr* – cu 7 kg/persoană mai mult în Republica Moldova; *carne și produse din carne* - cu 17 kg mai mult în România; cu 90 kg *lapte și produse din lapte echivalent lapte 3,5% grăsime* mai mul în România, cu 8 litri de vin mai mult în Republica Moldova.

CONCLUZII

Veniturile populației din Republica Moldova indică un nivel scăzut al acestora comparativ cu țările învecinate, 66 la sută din salariați având un câștig salarial sub câștigul mediu salarial. Nivelul sărăciei extremale pe țară a alcătuit în anul 2021 24,5% din numărul total al populației. Ponderea salariului în veniturile disponibile în mediul urban constituie 61,1%, iar în mediul rural 40,3%. Veniturile disponibile ale gospodăriilor sunt îndreptate spre cumpărarea produselor alimentare și băuturilor nealcoolice în proporție de 41,1%, inclusiv 36% - mediul urban și 48,5 - mediul rural, ceea ce denotă orientarea majorității populației spre satisfacerea necesităților în produse alimentare de bază și produse de igienă. Deși, în general, se apreciază ca satisfăcător nivelul de asigurare al populației cu produsele alimentare de bază, există decalaje semnificative între diferite categorii de consumatori, precum și decalaje în raport cu alte țări, spre exemplu, România. In vederea creșterii nivelului de bunăstare al populației sugerăm următoarele acțiuni: transparentizarea veniturilor și o politică a salarizării responsabilă la nivel de antreprenoriat și țară; dezvoltarea pieței muncii, creșterea veniturilor și a autoconsumului populației rurale prin diversificarea activităților de antreprenoriat și responsalizarea factorilor de decizie locali (menținerea pășunilor, iazurilor, grădinăritului s.a.); politică de susținere a afacerilor micro și mici; politică socială responsabilă de susținere a celor nevoiași etc.

BIBLIOGRAFIE

1. STRELEȚ,I.A.; STANCOVSCAIA, I.C. Economicescaia teoria. Polnâi curs MBA (tmk.edu.ee). -M: ООО «Рид Групп», 2011. ISBN 978-5-9614-2947-3. [accesat 02 decembrie 2023]. Disponibil: <https://materjalid.tmk.edu.ee/tatjana_moroz/Ek_teoria_Stankovskaya_Strelets.pdf>.
2. Anuarul statistic al Republicii Moldova.– Chișinău: Biroul Național de Statistică al Republicii Moldova, 2019 ;– Statistica Moldovei, ISBN 978-9975-53-418-5). – ISBN 978-9975-53-928-9.2019,472 p.[accesat 02 decembrie 2023]. Disponibil:< https://statistica.gov.md/public/files/publicatii_electronice/Anuar_Statistic/2019/Anuarul_statistic_2019.pdf >.
3. Moldova în cifre: Breviar statistic / Biroul Național de Statistică al Republicii Moldova ; – Chișinău : 2023. – (Statistica Moldovei / Biroul Naţional de Statistică al Republicii Moldova, p.22. ISBN 978-9975-53-418-5). – ISBN 978-9975-3629-0-0.[accesat 02 decembrie 2023]. Disponibil:< https://statistica.gov.md/files/files/publicatii_electronice/Moldova_in_cifre/2023/Moldova_cifre_rom_2023.pdf>
4. GDP per Capita by Country.World Bank.[accesat 05 decembrie]. < https://worldpopulationreview.com/country-rankings/gdp-per-capita-by-country>.

DOI: https://doi.org/10.53486/escst2023.08
International Conference, December 07-08, 2023, Chișinău, Moldova

5. Salariul minim pe țară în anul 2024. [accesat 05 decembrie 2023]. Disponibil:< https://gov.md/ro/content/salariul-minim-pe-tara-anul-2024-va-constitui-5000-lei-mai-mare-cu-1000-de-lei-decat-2023>.
6. Servet Yanatma. Minimum wages have declined because of soaring inflation. This is how things stand across Europe. [accesat 02 decembrie 2023]. Disponibil: <https://www.euronews.com/next/2023/02/08/minimum-wages-have-declined-because-of-soaring-inflation-this-is-how-things-stand-across-e>.
7. LUCA, L. (coordonator); ALEXANDRI C.; IONEL, I.; LEONTE, Marie-Jacqueline-Cosette. Securitatea alimentară, ca element al politicii agricole comune și agriculturii României în context european. Provocări 2023 – 2027. ISBN online: 978-606-8202-71-6, p.43 [accesat 02 decembrie 2023]. Disponibil: <http://ier.gov.ro/wp-content/uploads/2023/01/Studiul-1_SPOS-2022_Securitatea-alimentara_Final.pdf>.
8. STRATEGIA securității alimentare a Republicii Moldova pentru anii 2023-2030. [accesat 05 decembrie 2023]. Disponibil: <https://cancelaria.gov.md/sites/default/files/document/attachments/531_0.pdf>.
9. ROJCO, Anatolii, HEGHEA, Ecaterina. Inegalitatea nivelului și condițiilor de trai ale populației urbane și rurale din Republica Moldova și măsurile de reducere a acesteia. In: *Creşterea economică în condiţiile globalizării*, Ed. 15, 15-16 octombrie 2021, Chișinău. Chisinau, Moldova: INCE, 2021, Ediția 15, Vol.2, pp. 324-331. ISBN 978-9975-3529-7-0 [accesat 05 decembrie 2023]. Disponibil: <https://ibn.idsi.md/sites/default/files/imag_file/materiale_conferinta_vol_II_versiunea_electronic_2021.pdf>.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

IMPLICAȚII MANAGERIALE ASUPRA SUSTENABILITĂȚII POLITICILOR ENERGETICE

MANAGERIAL IMPLICATIONS FOR THE SUSTAINABILITY OF ENERGY POLICIES

Dana-Claudia COJOCARU

PhD Student,
Alexandru Ioan Cuza University of Iași, România,
ORCID 0000-0002-2533-6729
E-mail: claudia.cojocaru82@yahoo.com

Mihaela ONOFREI

PhD, Professor,
Alexandru Ioan Cuza University of Iași, România,
ORCID 0000-0002-9521-9210
E-mail: onofrei@uaic.ro

Abstract: *In the 21st century, society is characterised by innovation, complexity and numerous challenges with multiple implications for citizens' lives. Political, economic, financial, environmental and social issues are constantly influencing the development trend of society. The most recent global events have demonstrated the weaknesses of contemporary societal arrangements, one of which is the dependence of economies on non-renewable energy sources.*

Today, in many economies, oil is the main energy resource and the reason for cooperation between certain countries, but also the reason for disputes between players in the international system. In this context, two interrelated concepts emerge - energy security and the managerial implications for decision-makers. These two concepts, which we have at our disposal at all times, are designed to achieve an integrated energy market, managing the resources at our disposal efficiently. Accordingly, the main purpose of our paper is to analyse two of the most important mechanisms we have at our disposal to ensure security and the climate for sustainable development.

According to our results, policy makers have a major role to play in developing sustainable and quality energy policies. Despite the fact that policy makers often faced challenges in choosing the most appropriate and effective energy policy for their countries, they faced multiple challenges related to the energy sector and highlighted the importance of ensuring energy security.

Keywords: *energy security, sustainable resources, energy policies, environmental protection.*

UDC: *620.9:504.06*

JEL Classification: *O13, Q56.*

INTRODUCERE

Începând cu perioada anilor `50, poluarea mediului înconjurător a constituit principalul impediment în realizarea Obiectivelor de Dezvoltare Durabilă, deoarece au avut loc o multitudine de evenimente negative asupra Pământului (schimbări climatice, defrișări masive, creșterea temperaturii medii globale, etc.). Totodată, consumul excesiv de combustibili fosili, dar și cerința de creștere continuă au cauzat daune majore asupra planetei și a ecosistemului.

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

Pentru o economie durabilă și prosperă este esențială elaborarea unor măsuri riguroase de eliminare a emisiilor de gaze cu efect de seră (GES) generate de sursele energetice neregenerabile (petrol, cărbune, gaze naturale). În acest sens, în cadrul conferinței de mediu din Egipt (COP28) economiile lumii au fost încurajate să-și diminueze nivelul emisiilor antropogene și să-și impună termene riguroase în ceea ce privește elaborarea planurilor de acțiune pentru combaterea încălzirii globale. Având în vedere acest context, economiile globale încearcă să finalizeze un acord în domeniul mediului pentru a putea depăși provocările la adresa acestuia.

O strategie ideală pentru a aborda problemele privind deficitul de energie, bunăstarea energetică și reducerea efectelor negative produse de consumul de surse neregenerabile este obținerea securității energetice [1]. Într-adevăr, în prezent asigurarea securității energetice reprezintă o provocare complexă la nivelul oricărei economii. Mai mult decât atât, politicile energetice depind foarte mult și de gradul de disponibilitate a resurselor energice ale unui stat, cât și de capacitatea tehnică și economică de a le exploata [2] ceea ce îngreunează puțin atingerea securității energetice. Însă, pe lângă strategiile și măsurile implementate de către diverse economii, literatura de specialitate se lovește de o problemă majoră în ceea ce privește conceptul de securitate energetică. În viziunea unor cercetători, „securitatea energetică" sau în forma largă „securitatea aprovizionării cu energie" nu pare a fi foarte clar definită [3], [4]. Prin urmare, confuzia cu privire la acest concept se reflectă și în acțiunile politice [5] făcând acest proces de asigurare a securității energetice din ce în ce mai dificil. De exemplu, în Statele Unite ale Americii securitatea energetică s-a axat în mod tradițional pe reducerea vulnerabilității la șantajul politic, ceea ce i-a determinat pe politicieni să ceară independența energetică și creșterea ponderii energiei regenerabile. Potrivit acestora, atunci când se abordează conceptul de securitate energetică opiniile se împart în două tabere. Pe de o parte, securitatea energetică are un singur obiectiv, respectiv cel de a proteja economiile mai puțin dezvoltate de instabilitatea prețurilor la produse de bază. Pe de altă parte, unii consideră că prin securitatea energetică este protejată economia de întreruperile furnizării de servicii energetice.

Într-o societate globalizată, aflată într-un continuu proces de expansiune și dependentă de energie, apar o multitudine de dificultăți. Însă, pentru a putea face față acestor provocări, implicațiile manageriale asupra sustenabilității politicilor energetice sunt un factor esențial ce poate ajuta, atât la asigurarea energiei în mod continuu, cât și la asigurarea stabilității economice și ecologice. Așadar, obiectivul cercetării noastre este de a analiza două dintre cele mai importante mecanisme pe care le avem la îndemână pentru a ne asigura securitatea și climatul favorabil dezvoltării durabile, politicile energetice și implicațiile manageriale ale factorilor de decizie.

Mai departe, lucrarea se structurează astfel: în secțiunea 2 aprofundăm literatura de specialitate cu privire la contextul securității energetice. În secțiunea 3 discutăm despre piața energiei și utilitatea politicii energetice, fiind urmată de partea de concluzii și recomandări.

CONTEXTUL SECURITĂȚII ENERGETICE

Asigurarea securității energetice reprezintă unul dintre factorii cheie utilizați în determinarea poziției actuale a unui stat și a orientării viitoare a dezvoltării acestora. *Dar totuși, ce este securitatea energetică?* Potrivit Agenției Europene de Mediu securitatea energetică, denumită în literatura de specialitate și securitatea aprovizionării este definită ca fiind *„... disponibilitatea neîntreruptă a surselor de energiei la prețuri accesibile"* [6].

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

În prezent, majoritatea economiilor se confruntă cu o provocare majoră – resurse energetice limitate și, mai mult decât atât, distribuite într-un mod inegal. Ca urmare a acestei situații, economiile în curs de dezvoltare sugerează faptul că securitatea energetică este o problemă prioritară pentru dezvoltarea oricărei economii. Energia este principala resursă pentru ca economiile să își producă bunuri și servicii și, în cele din urmă, să îmbunătățească bunăstarea umană, socială și economică [7], [8].

Deși securitatea energetică este un concept relativ nou în literatura de specialitate, aceasta are în spatele său o istorie fabuloasă datorită importanței pe care a demonstrat-o de-a lungul anilor.

În pofida faptului că energia a fost dintotdeauna o parte esențială a vieții umane, cele mai vechi încercări de conceptualizare, măsurare și abordare a securității energetice în accepțiunea sa modernă au fost făcute abia în secolul al XX-lea, moment în care securitatea energetică a primit o atenție sporită în domeniul politicii energetice [9]. Noțiunea de „securitate energetică" este strâns legată de furnizarea combustibililor pentru armată încă din timpul celui de-al Doilea Război Mondial [4], [10]. Ca urmare a evenimentelor din acea perioadă, cea de-a doua conflagrație globală a reliefat și mai mult importanța securității energetice. Potrivit lui Downs, schimbările geopolitice evidențiază faptul că securitatea energetică face parte din securitatea națională, fiind considerată parte integrantă a acesteia [11].

Originile noțiunii de „securitate energetică" datează încă din perioada anilor 1970, moment în care membrii arabi ai Organizației Țărilor Exportatoare de Petrol (OPEC) au suspendat exportul de petrol către Statele Unite ale Americii, declanșând astfel prima „criză energetică", așa cum o numesc contemporanii [12]. Acest fapt s-a datorat susținerii Israelului de către Statele Unite ale Americii în timpul războiului arabo-israelian (denumit în literatura de specialitate și Războiul Yom-Kippur) din perioada anilor `70, creând astfel un embargo petrolier arab [12] care a durat până în anul 1974. Acest eveniment a scos la iveală dependența unor state față de importurile de petrol. Totodată, Henry Kissinger spunea în acea perioadă „controlează petrolul și poți controla toate continentele". De asemenea, un susținător de-al acestuia afirma că „dacă vrei să conduci întreaga lume, trebuie să controlezi petrolul. Tot petrolul, indiferent de unde locul unde se află".

La acel moment, embargoul petrolier a zdruncinat puternic economia americană care devenea încet-încet tot mai dependentă de petrolul străin. Totodată, membrii arabi ai Organizației Țărilor Exportatoare de Petrol au extins embargoul și în state precum Portugalia, Țările de Jos și Africa de Sud, ca urmare a sprijinii Israelului la acel moment. Un aspect foarte important de menționat se referă la faptul că Organizația Țărilor Exportatoare de Petrol nu a deținut niciodată monopolul asupra pieței petrolului. Interesul Organizației Țărilor Exportatoare de Petrol a fost manipularea prețului petrolului, în cooperare cu firmele private și de stat petroliere.

Criza petrolieră din 1970 a dus în mod automat la o majorare substanțială a prețului petrolului. Potrivit Administrația Informațiilor Energetice barilul de petrol era 2,90 USD înainte de embargou, iar ulterior, în ianuarie 1974, prețul acestuia s-a cvadruplat, ajungându-se la 11,65 USD. Ca urmare a evenimentelor petrecute în perioada anilor 1970-1974 considerăm că acești ani i-am putea descrie ca insecuritate energetică.

Aceste întreruperi trebuie tratate cu maximă seriozitate, deoarece economia oricărui stat se bazează pe astfel de resurse pentru furnizarea diferitelor servicii sociale. De exemplu, de-a lungul anilor au avut loc la nivelul Uniunii Europene mai multe întreruperi majore în aprovizionare cu gaze, iar acestea au îngreunat activitatea economică a statelor membre.

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

Politica energetică și politica de mediu au apărut în tandem în anii 1970 [13]. Degradarea mediului din acea perioadă a fost un subiect dezbătut intens de factorii de decizie și activiștii mediului. Prin urmare, energia a fost principalul subiect abordat în cadrul dezbaterilor privind mediul înconjurător, unde s-a concluzionat faptul că are două mari efecte negative asupra mediului. În primul rând, se consideră că unele moduri de utilizare a energiei au fost responsabile pentru deteriorarea mediului și, în al doilea rând, energia atomică prezintă riscuri substanțiale.

Astfel, în anul 1972, Jorge Randers publică o carte intitulată *„Limits to growth”* unde abordează subiecte precum protejarea mediului înconjurător și preocupările legate de energie. Autorul a arătat faptul că poluarea și consumul de energie se aflau pe o traiectorie nu tocmai sustenabilă. Ca răspuns la cele demonstrate de Jorge Randers, scriitorul american Lovins a prezentat două căi energetice: o cale ușoară și o cale dificilă [14]. În acest context, calea ușoară se baza pe tehnologii alimentate de surse de energii regenerabile și eficiență energetică, în timp ce calea dificilă se baza pe politici ce promovau sisteme energetice care utilizau surse de energie neregenerabile. Conform celor menționate de Lovins, Statele Unite ale Americii ar putea renunța la dependența sa de petrol și cărbune dacă factorii de decizie ar alegea calea ușoară propusă de acesta.

La nivel global, numeroși factori au provocat apariția unor astfel de șocuri ale prețului petrolului. Printre aceștia se includ schimbările majore în cerere sau ofertă, indiferent unde în lume, întrucât petrolul este considerat o marfă globală. Totodată, se pot produce șocuri din cauza unor evenimente geopolitice, a unor perioade de creștere economică accelerată în țările importatoare de petrol, inclusiv modificările politice ale Organizației Țărilor Exportatoare de Petrol. Figura 1 reliefează trendul oscilant al prețurilor petrolului pe perioada 1970-2022, tendința fiind una în creștere. Aceste șocuri petroliere nu sunt noi pentru societate, ele fiind o parte integrantă a dinamicii pieței petrolului.

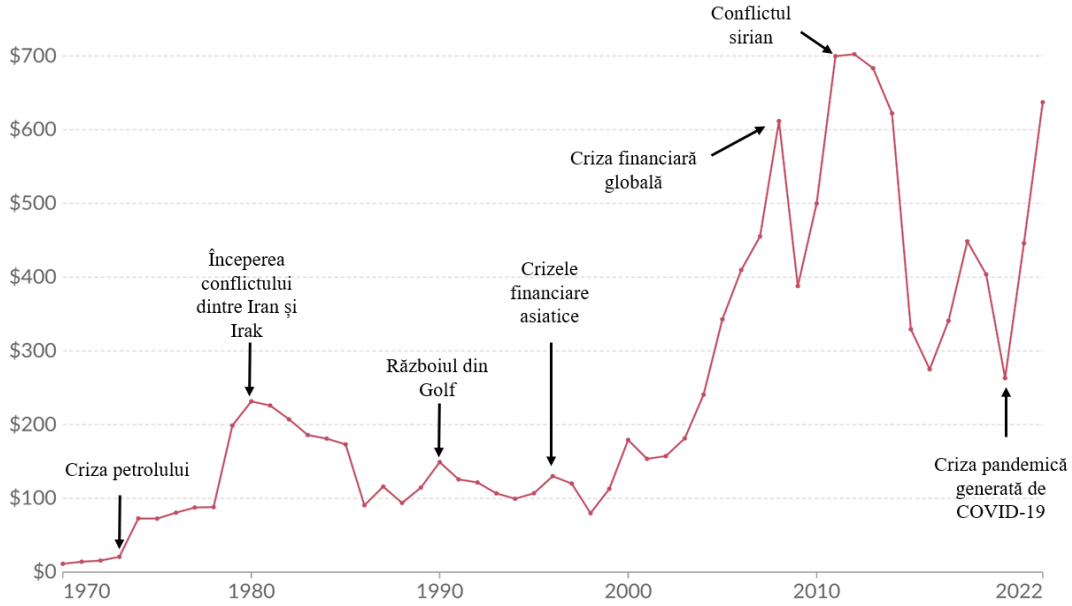


Figura 1. Evoluția prețurilor petrolului

Sursa: Energy Institute Statistical Review of World Energy based on S&P Global Platts (2023)

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

Imaginea atașată reliefează 53 de ani de suișuri și coborâșuri. După impunerea embargoului petrolier, prețurile au început să înregistreze un tren ascendent până în perioada anului 1980, moment în care acestea au crescut de la 13 dolari pe baril la 34 [15]. Având în vedere prețurile foarte ridicate ale petrolului, proiectele cu privire la sursele de energie alternativă s-au extins, fiind finanțate de Occidental Petroleum și Exxon. Însă, odată ce prețul petrolului a început să scadă începând cu anul 1981, proiectele privind sursele de energie alternativă au fost, fie anulate, fie suspendate până la următoarele creșteri.

Potrivit imaginii atașate, observăm că în anul 2012 se înregistrează cea mai mare creștere a prețului la petrol. Potrivit unor autori, aceste creșteri au fost anticipate încă din perioada anului 1990 [16]. Agenția Internațională de Energetice susține că principalii factori care au dus la aceste creșteri substanțiale sunt: (1) sancțiunile impuse de Statele Unite ale Americii și Europa asupra Iranului, (2) creșterea producției de petrol din Statele Unite și (3) întreruperile aprovizionării cu petrol [17].

După o perioadă de „stabilitate", prețul petrolului înregistrează o scădere bruscă în iunie 2016, fiind considerată de către Banca Mondială ca cea mai mare scădere a petrolului din istoria modernă. Principala cauză a fost reprezentată de oferta excedentară determinată de producția de petrol de șist din Statele Unite.

În anul 2020, piața petrolului este zguduită iarăși de un eveniment ce își lasă amprenta asupra întregii economii. Pandemia generată de COVID-19 a lovit industria petrolului, ducând la o scădere semnificativă a prețurilor petrolului în prima jumătate a anului.

Volatilitatea prețurilor petrolului ne arată faptul că foarte mulți producători de petrol s-au lovit de diverse provocări în momentul proiectării și implementării politicilor energetice. Este foarte important să se înțeleagă proprietățile statistice ale prețurilor petrolului pentru a putea elabora politici eficiente [18].

PIAȚA ENERGIEI ȘI UTILITATEA POLITICII ENERGETICE

În contextul unei societății ce se află într-un proces continuu de schimbare, securitatea energetică este considerată ca fiind un pilon fundamental al dezvoltării economiilor globale. Evenimente precum creșterea inflației, criza climatică, respectiv perspectivele geopolitice reprezintă adevărate provocări pentru guvernele ce s-au angajat în atingerea obiectivului net zero și dezvoltarea sistemului energetic pe bază de resurse regenerabile. Russell Wells, liderul global al companiilor din domeniul energiei și managerul secundar al grupului de tranziție energetică, a menționat în cadrul unui eveniment faptul că „reducerea emisiilor de CO_2 generate de energie este crucială în vederea limitării efectelor nocive ale schimbărilor climatice. Anul 2023 va fi caracterizat de inovație și dezvoltare în mai multe domenii, dar provocările competitive legate de securitatea energetică și de accesibilitatea prețurilor, împreună cu problemele legate de lanțul de aprovizionare la nivel mondial, generează obstacole".

Din punct de vedere istoric, piața energiei a suferit numeroase transformări din cauza modificărilor frecvente a politicilor energetice, dezvoltarea noilor tehnologii care au fost adoptate pe scară largă și a preocupărilor îndreptate tot mai mult spre schimbările climatice. În acest context, Figura 2 reliefează o parte din evenimentele ce au adus modificări majore asupra pieței energetice.

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

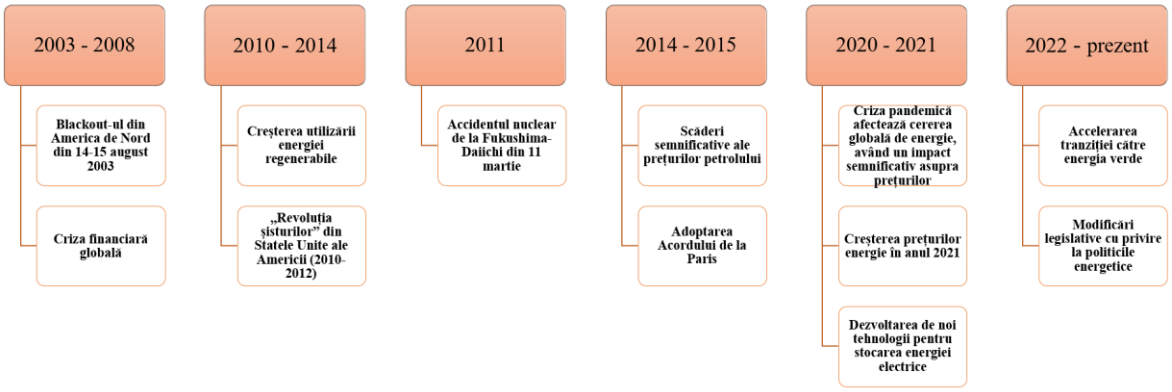


Figura 2. Evoluția pieței energetice
Sursa: reprezentarea autorilor.

Un studiu foarte interesant realizat de Consiliul Global al Energiei este cel de identificare a statelor care vor să realizeze o tranziție energetică de la combustibilii fosili la sursele de energie regenerabile. Pentru a clarifica ce presupune tranziția energetică ne îndreptăm spre definiția oferită de Grunwald, unde susține faptul că această noțiune implică „un program de politică cuprinzător ce reprezintă o reconstrucție a aprovizionării cu energie regenerabilă, o modernizare a infrastructurii rețelei electrice și dezvoltarea de noi tehnologii pentru stocarea acesteia" [19]. Tranziția energetică este „o cale de transformare a sectorului energetic mondial de la o energie bazată pe combustibili fosili la o energie fără emisii de carbon" [20]. Astfel, Consiliul Global al Energiei a măsurat durabilitatea mediului înconjurător, securitatea energetică și echitatea energetică în fiecare teritoriu al lumii. Rezultatele au reliefat faptul că Suedia, Elveția, Danemarca, Finlanda, Marea Britanie și Canada sunt primele cinci state cu siguranță energetică ale căror sisteme energetice robuste și sigure gestionează eficient cererea și oferta de energie [21]. Atunci când discutăm despre echitate energetică clasamentul se schimbă puțin, iar primele cinci state care îndeplinesc acest criteriu sunt Luxemburg, Bahrain, Qatar, Kuweit și Emiratele Arabe [21].

Totodată, în realizarea acestui studiu, Consiliul Global al Energie oferă câteva argumente despre fiecare teritoriu. De exemplu, la nivelul Uniunii Europene se susține faptul că actualele angajamente de atenuare a efectelor negative generate de criza energetică nu îi vor permite să își îndeplinească obiectivele în materie de energie durabilă, deoarece prețurile foarte ridicate afectează accesibilitatea. În schimb, America de Nord dispune de o puternică securitate energetică bazată pe un istoric îndelungat de dezvoltare a diverselor resurse energetice, iar echitatea energetică este puternică și rămâne un factor relativ puțin mediatizat în regiune [21]. Factorul principal care a dus America de Nord spre acest succes sunt sursele de energie regenerabile adoptate pentru satisfacerea nevoile interne. La nivelul Africii au fost identificate progrese notabile în privința accesului la energie, însă, în continuare, securitatea energetică este o provocare uriașă.

Luând în considerare aceste argumente aduse fiecărui teritoriu, reiese importanța implementării și gestionării politicilor energetice la nivelul economiilor. Cu toate acestea, unii autori [22] au realizat un studiu asupra unui număr de 42 de economii din regiunea Asia-Pacific. Autorii menționează că au ales studierea acestui eșantion, deoarece este responsabil pentru mai mult de jumătate din consumul global al energiei. De asemenea, această regiune a adoptat un număr mare de politici energetice și, totuși, progresul în tranziția energiei verzi

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

rămâne lent, subliniază autorii. Rezultatele acestora au evidențiat faptul că politicile energetice au contribuit la îmbunătățirea accesului la energia electrică cu doar 3%, în timp ce, în cazul eficienței energetice, cu doar 1,4%. Mai mult decât atât, pentru capacitatea de energie electrică regenerabilă, politicile energetice au contribuit la îmbunătățirea acestora cu 6,9%. De asemenea, [23] analizează securitatea energetică a Asociației Națiunilor din Asia de Sud-Est (ASEAN) în perioada 2005-2010. În urma analizelor efectuate de autori, s-a constat faptul că ASEAN a înregistrat puține progrese în privința stabilirii securității energetice. În acest caz ne apare în minte următoarea întrebare: *de ce este nevoie de politici energetice?*

Politicilor energetice cuprind reguli cu privire la sursele de energie, prețurile energiei pe piață, eficiența energetică, infrastructura energetică și toate aspectele climatice și de mediu ale producției, utilizării și tranzitului energiei [24]. Aceste politici se caracterizează la ora actuală prin patru elemente fundamentale, prezentate sub formula celor „4A”: „disponibilitate (**a**vailability), acces la energie (**a**ffordability), accesibilitate din punct de vedere financiar (**a**ccessibility) și acceptabilitate (**a**cceptability)” [25], [26]. Dar cu toate acestea, în literatura de specialitate unii cercetători [27], [28] consideră că cele patru elemente nu sunt suficiente pentru a răspunde la problemele de securitate și ar trebui completate. Prin urmare, [27] și [28] au considerat că este necesar să răspundă la un set de întrebări: *„Securitatea pentru cine?”*, *„Securitatea pentru ce valori?”* și *„Securitatea față de ce amenințări?”*.

Hughes a introdus pentru prima dată conceptul celor patru „R” [29]. Pentru a clarifica conceptul de securitate energetică, autorul explică faptul că ar trebui introduse politici energetice care să se bazeze pe „revizuire (**r**ewiew), reducere (**r**educe), înlocuire (**r**eplace) și restricție (**r**estrict)”.

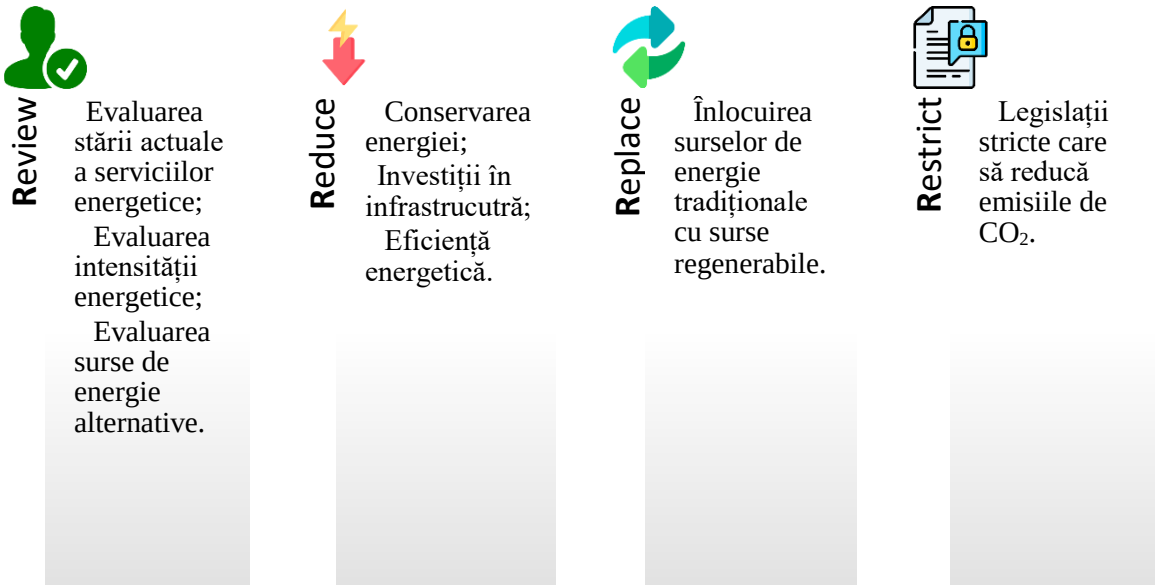


Figura 3. Cei 4 R ai securității energetice

Sursa: adaptare după Hughes, L. (2009). The four 'R's of energy security. Energy policy.

Energia este esențială pentru oricine și în orice moment. Fie că vorbim despre realizarea unor activități obișnuite din viața de zi cu zi, fie că vorbim despre dezvoltarea economiei prin susținerea activităților de producție, energia este omniprezentă. Am observat că încă din perioada Primului Război Mondial s-au căutat surse alternative de energie, iar al Doilea Război Mondial a întărit și mai mult această dinamică. Astfel, în

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

funcție de timp, spațiu și condițiile pieței, politicile energetice și-au relevat progresiv natura multiformă. Prin urmare, căutarea de noi resurse energetice devine un subiect discutat la scară largă [30].

Mulți cercetători [31], [32] și [33] susțin că sursele de energie regenerabile sunt un factor-cheie în diminuarea emisiilor de gaze cu efect de seră. Raihan analizează efectele consumului de energie și inovațiile tehnologice asupra emisiilor de gaze cu efect de seră din Coreea de Sud [32]. Folosind date pentru perioada 1990-2021, rezultatele au reliefat faptul că utilizarea energiilor regenerabile și inovațiile tehnologice ajută la îmbunătățirea mediului înconjurător, atât pe termen scut, cât și pe termen lung. Rezultate similare au obținut și [34], [35] și [36]. Având în vedere aceste aspecte, foarte multe state au implementat diverse politici energetice pentru a promova sursele de energie regenerabilă, deoarece ar putea acoperi o mare parte din nevoile energetice ale oricărei economii.

În acest domeniu de politici, în special în contextul european, problema majoră se referă la compromisurile dintre energie accesibilă, sigură și curată. Politica energetică este un domeniu de politică intersectorială sau de extindere a limitelor [37], [38]. Natura intersectorială a politicii energetice se reflectă în modul în care este propusă, adoptată, pusă în aplicare și evaluată [24].

La nivelul Uniunii Europene, pilonii politicii energetice sunt: economisirea energiei, diversificarea aprovizionării cu energie și producerea de energie curată [39]. Unii autori au identificat, în urma analizelor efectuate, faptul că majoritatea statelor membre ale Uniunii Europene și-au îmbunătățit mult securitatea energetică ca urmare a numeroasele directive pe care le-au adoptat [40]. Am putea contrazice acest aspect pe baza unor argumente bine fundamentate. În primul rând, statele membre ale Uniunii Europene sunt dependente de importurile de combustibili fosili, iar această dependență are ca rezultat o securitate energetică scăzută. Mai mult decât atât, la nivelul Uniunii Europene încă există state ce se confruntă cu o infrastructură energetică slabă (de exemplu: România, Grecia, Bulgaria).

Într-adevăr, de-a lungul anilor Uniunea Europeană a implementat diverse măsuri în materie de politici energetice, dar cu toate acestea, ne aflăm într-o criză energetică care poate fi rezolvată printr-un plan de acțiune bine fundamentat și prin adoptarea unor politici riguroase în privința resurselor de energie regenerabilă.

O mică parte din directivele adoptate de către Uniunea Europeană care vizează eficiența energetică sunt analizate în continuare.

Statele membre ale Uniunii Europene au adoptat în octombrie 2003 Directiva 2001/77/EC cu privire la promovarea electricității produse din surse de energie regenerabile. De asemenea, un număr de zece state ce urmau să adere la Uniunea Europeană în acea perioadă aveau obligația de a îndeplini această condiție până la data aderării. Majoritatea statelor au înregistrat progrese considerabile.

La data de 8 mai 2003, Uniunea Europeană a adoptat Directiva 2003/30/CE privind promovarea utilizării combustibililor din surse regenerabile care a prevăzut ca statele membre să asigure, până la finalul anului 2005, o pondere de cel puțin 2% de biocombustibili în totalul benzinei și al motorinei vândute pe piața lor și de 5,75% până în decembrie 2010 [41].

În acest context, începând cu 1 iulie 2004, statele membre ale Uniunii Europene erau obligate să raporteze Comisiei Europene următoarele aspecte:

- măsurile întreprinse în vederea promovării combustibililor regenerabili pentru a înlocui vehiculele cu motoare termice;

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

- vânzările totale de carburanți pentru transporturi și ponderea biocarburanților;
- resursele interne alocate pentru producția de biomasă.[1]

Cartea verde a Uniunii Europene din anul 2006, intitulată *„O strategia europeană pentru o energie durabilă, competitivă și sigură”* a reprezentat o etapă importantă în dezvoltarea politicii energetice. Comisia Europeană a stabilit pentru statelor membre ale Uniunii Europene trei obiective prioritare: *competitivitatea, securitatea aprovizionării și sustenabilitate* [42]. În acest context, Comisia Europeană a ținut să sublinieze că cele trei obiective fac parte din aceiași strategie, iar „munca pentru a realiza unui obiectiv din cele trei trebuie să contribuie la realizarea celorlalte”. Ulterior, la data de 8-9 martie 2007, prim-miniștrii Uniunii Europene au aprobat o nouă politică energetică. De data aceasta, noua politică a prevăzut, printre altele, un angajament ferm de creștere a energiei din surse regenerabile la 20% din aprovizionarea cu energie primară până în 2020. Totodată, prim-miniștrii au stabilit reducerea cu 30% a emisiilor de gaze cu efect de seră până la finele anului 2020. Pentru prima dată în istorie, Comisia Europeană a propus un obiectiv obligatoriu pentru energia regenerabilă și nu doar pentru electricitate sau biocombustibili din surse regenerabile [43].

În 2016, Comisia Europeană a prezentat un nou pachet de propuneri legislative intitulat „Energie curată pentru toți europenii” pentru a transpune strategia în realitate [44]. În acest context, Consiliul Uniunii Europene a stabilit obiective ce prevăd majorare cu 32,5% a eficienței energetice prin reducerea consumului de energie și creșterea cu circa 32% a energiei din surse regenerabile.

În septembrie 2023, a fost adoptată Directiva 1791/2023 privind eficiența energetică, prin care au fost adoptate o serie de măsuri pentru a accelerarea acesteia. Printre acestea se regăsesc: finanțarea eficienței energetice, atenuare sărăciei energetice, încurajarea companiilor să fie mult mai eficient din punct de vedere energetic.

Totalitatea directivelor și politicilor prezentate anterior au avut un impact favorabil în reducerea emisiilor de gaze cu efect de seră. În acest sens, Agenția Internațională pentru Energie subliniază faptul că politicile energetice europene sunt pregătite pe baza unor consultări ample cu factorii de decizie, inclusiv consumatorii și companiile, precum și organizațiile neguvernamentale [45]. Totodată, este primordial să recunoaștem faptul că securitatea energetică la nivelul Uniunii Europene este influențată în continuare de o dependență semnificativă de importurile de combustibili fosili, subliniind astfel nevoia permanentă de inovare și de strategii durabile pentru a diminua vulnerabilitățile și pentru a asigura independența pe o perioadă îndelungată.

CONCLUZII

Securitatea energetică este un subiect cu implicații largi, influențând într-un mod semnificativ politicile și reglementările adoptate de către guvernele din întreaga lumea. În vederea intensificării procesului de tranziție către o economie bazată pe energie curată, este necesar să se cunoască îndeaproape dinamica politicii globale și considerentele care stau la baza adoptării și difuzării acestora.

Scopul acestei cercetări a fost acela de a ilustra implicațiile manageriale ale factorilor de decizie pentru a implementa cele mai eficiente politici energetice. De

[1] Jurnalul Oficial al Uniunii Europene, DIRECTIVA 2003/30/CE A PARLAMENTULUI EUROPEAN ȘI A CONSILIULUI din 8 mai 2003 privind promovarea utilizării biocombustibililor sau a altor combustibili regenerabili în transporturi.

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

asemenea, scoatem în evidență faptul că politicile energetice trebuie adaptate în funcție de evenimentele ce se petrec la nivel global și de nivelul de dezvoltare al fiecărui stat, deoarece nicio politică nu se potrivește tuturor statelor.

Sistemul energetic modern constituie o componentă fundamentală a societății contemporane. Acest sistem facilitează prestarea unor servicii multiple care pot îmbunătăți calitatea vieții umane, sociale, economice și de mediu. Totuși, actualul sistem energetic nu este deloc sustenabil din cauza dependenței uriașe de petrol care generează emisii de gaze cu efect de seră. Astfel, pentru a îmbunătăți calitatea vieții umane și a ne îndrepta către o societate durabilă, serviciile energetice trebuie distribuite într-o manieră accesibilă, sigură și, cel mai important, ecologică. Desigur, pentru îndeplinirea acestui obiectiv sunt necesare schimbări radicale în domeniul tehnologiilor, al infrastructurii și al comportamentului uman. Această schimbare necesită modificări profunde, astfel încât autoritățile guvernamentale și liderii din domeniul afacerilor trebuie să se folosească de toate instrumentele de care dispun pentru a putea a-și putea îndeplini obiectivele propuse. Aceste schimbări ar trebui începute de la nivel de mentalitate și deschidere către nou, până la acorduri solide între toate statele lumii, bazate pe încredere și colaborare, dar mai important conduse de dorința unanimă de a progresa.

BIBLIOGRAFIE

1. SHITTU, W. [et al.]. An investigation of the nexus between natural resources, environmental performance, energy security and environmental degradation: Evidence from Asia. *Resources Policy* [online]. 2021, **73**, 102227. ISSN 0301-4207 [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301420721002385>.
2. BERZAN, V. [et al.]. Tendințele funcționării sistemului energetic și securitatea energetică. [online]. 2015. [viewed 30 November 2023]. Available from: <https://ibn.idsi.md/vizualizare_articol/35887>.
3. LÖSCHEL, A. [et al.]. Indicators of energy security in industrialised countries. *Energy Policy* [online]. 2010, **38**(4), 1665–1671. ISSN 0301-4215 [viewed 13 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421509002262>.
4. CHESTER, L. Conceptualising energy security and making explicit its polysemic nature. *Energy Policy* [online]. 2010, **38**(2), 887–895. ISSN 0301-4215 [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421509007861>.
5. WINZER, C. Conceptualizing energy security. *Energy Policy* [online]. 2012, **46**, 36–48. ISSN 0301-4215 [viewed 30 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421512002029>.
6. AGENȚIA EUROPEANĂ DE MEDIU. Security of supply. *European Environment Agency* [online], 2004. [viewed 22 November 2023]. Available from: <https://www.eea.europa.eu/help/glossary/eea-glossary/security-of-supply>.
7. BOMPARD, E. [et al.]. National energy security assessment in a geopolitical perspective. *Energy* [online]. 2017, **130**, 144–154 [viewed 24 January 2024]. ISSN 0360-5442. [viewed 24 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0360544217306746>.

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

8. CONSILIUL GLOBAL DE ENERGIE. Energy security risk index. *Global Energy Institute* [online]. 2018. [viewed 12 November 2023]. Available from: <https://www.globalenergyinstitute.org/energy-security-risk-index>.
9. NOVIKAU, A. Energy security: evolution of a concept. *SpringerLink* [online]. 2020. [viewed 12 November 2023]. Available from: <http://link.springer.com/10.1007/978-3-319-74336-3_491-1>.
10. CHERP, A., JEWELL, J. The concept of energy security: Beyond the four As. *Energy Policy* [online]. 2014, **75**, 415–421. ISSN 0301-4215 [viewed 21 November 2023] Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421514004960>.
11. DOWNS, E. The chinese energy security debate. *The China Quarterly* [online]. 2004, **177**, 21–41. ISSN 1468-2648. [viewed 12 November 2023]. Available from: <https://www.cambridge.org/core/product/identifier/S0305741004000037/type/journal_article>.
12. JONES, T. „Energy security": Genealogy of a term. *No. 271, Summer 2014, FUEL & WATER: THE COMING CRISES* [online]. 2014. [viewed 30 November 2023]. Available from: <https://www.jstor.org/stable/24426552>.
13. GRAF, R. Energy history and histories of energy. [online]. 2004. [viewed 05 November 2023]. Available from: <https://zeitgeschichte-digital.de/doks/frontdoor/index/index/docId/2616>.
14. LOVINS, Amory B. Energy strategy: the road not taken? *Foreign Affairs* [online]. 1976, **55**(1), 65. ISSN 0015-7120 [viewed 13 November 2023]. Available from: <https://heinonline.org/HOL/Page?handle=hein.journals/fora55&id=67&div=&collection=>
15. MONTGOMERY, Scott L. Oil price shocks have a long history, but today's situation may be the most complex ever. *The Conversation* [online]. 2022. [viewed 30 November 2023]. Available from: <http://theconversation.com/oil-price-shocks-have-a-long-history-but-todays-situation-may-be-the-most-complex-ever-178861>.
16. CIUPAGEA, C., CÂMPEANU, V. Energia în cursa competitivitate-încălzire globală. Editura Expert, București. 2007. pp.188-212, ISBN 978-973-7885-92-0.
17. AGENȚIA INTERNAȚIONALĂ DE ENERGIE. 2012 Brief: Average 2012 crude oil prices remain near 2011 levels - U.S. Energy Information Administration (EIA). *Homepage - U.S. Energy Information Administration (EIA)* [online]. 2013. [viewed 22 November 2023] Available from: <https://www.eia.gov/todayinenergy/detail.php?id=9530>.
18. BARNETT, S., OSSOWSKI, R. Operational aspects of fiscal policy in oil-producing countries. [online]. *International Monetary Fund*. IMF Working Paper 2002/177. [viewed 30 November 2023]. Available from: <https://econpapers.repec.org/paper/imfimfwpa/2002_2f177.htm.>.
19. GRUNWALD, A. [et al.]. Die Energiewende verstehen - orientieren - gestalten - Nomos eLibrary. *Nomos eLibrary* [online]. 2017. [viewed 05 November 2023]. Available from: <https://www.nomos-elibrary.de/index.php?doi=10.5771/9783845278957-1>.
20. VAN DE GRAAF, T. A new world: the geopolitics of energy transformation. *Ghent University Academic Bibliography* [online]. 2019. [viewed 30 November 2023]. Available from: <http://hdl.handle.net/1854/LU-8588274>.

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chişinău, Moldova

21. Consiliul Global al Energiei. Trilemma Index 2022. [online]. 2022. [viewed 30 November 2023]. Available from: < https://trilemma.worldenergy.org/reports/main/2022/World%20Energy%20Trilemma%20Index%202022.pdf>
22. CHEN, P. [et al.]. The heterogeneous role of energy policies in the energy transition of Asia–Pacific emerging economies. *Nature Energy* [online]. 2022. ISSN 2058-7546 [viewed 21 November 2023]. Available from: <https://www.nature.com/articles/s41560-022-01029-2>.
23. TONGSOPIT, S. [et al.]. Energy security in ASEAN: a quantitative approach for sustainable energy policy. *Energy Policy* [online]. 2016, **90**, 60–72. ISSN 0301-4215 [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S030142151530197X>.
24. TOSUN, T. Energy Policy. *Oxford Research Encyclopedia of Politics* [online]. 2017. [viewed 22 November 2023]. Available from: <https://oxfordre.com/politics/view/10.1093/acrefore/9780190228637.001.0001/acrefore-9780190228637-e-174>.
25. CHERP, A., JEWELL, J. The concept of energy security: Beyond the four As. *Energy Policy* [online]. 2014, **75**, 415–421. ISSN 0301-4215 [viewed 21 November 2023] Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421514004960>.
26. HUGHES, L. The four 'R's of energy security. *Energy Policy* [online]. 2009, **37**(6), 2459–2461. ISSN 0301-4215 [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421509001414>.
27. JEWELL, J. [et al.]. Energy security under de-carbonization scenarios: an assessment framework and evaluation under different technology and policy choices. *Energy Policy* [online]. 2014, **65**, 743–760. ISSN 0301-4215 [viewed 22 November 2023]. Available from: <https://www.sciencedirect.com/science/article/pii/S0301421513010744>.
28. WINZER, C. Conceptualizing energy security. *Energy Policy* [online]. 2012, **46**, 36–48. ISSN 0301-4215 [viewed 30 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421512002029>.
29. HUGHES, L. The four 'R's of energy security. *Energy Policy* [online]. 2009, **37**(6), 2459–2461. ISSN 0301-4215 [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421509001414>.
30. ZHANG, Z. [et al.]. Overview of the development and application of wind energy in new zealand. *Energy and Built Environment* [online]. 2022. ISSN 2666-1233 [viewed 30 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S2666123322000459>.
31. LIMA, M. [et al.]. Renewable energy in reducing greenhouse gas emissions: Reaching the goals of the Paris agreement in Brazil. *Environmental Development* [online]. 2020, **33**, 100504. ISSN 2211-4645 [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S2211464520300191>.
32. RAIHAN, A. Nexus between greenhouse gas emissions and its determinants: The role of renewable energy and technological innovations towards green development in South Korea. *Innovation and Green Development* [online]. 2023, **2**(3), 100066. ISSN 2949-7531 [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S2949753123000346>.

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

33. SHAAHID, S., EL-AMIN, I. Techno-economic evaluation of off-grid hybrid photovoltaic–diesel–battery power systems for rural electrification in Saudi Arabia-A way forward for sustainable development. *Renewable and Sustainable Energy Reviews* [online]. 2009, **13**(3), 625–633. ISSN 1364-0321 [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S1364032107001694>.
34. PANWAR, N. [et al.]. Role of renewable energy sources in environmental protection: a review. *Renewable and Sustainable Energy Reviews* [online]. 2011, **15**(3), 1513–1524. ISSN 1364-0321 [viewed 22 November 2023] Available from: <https://linkinghub.elsevier.com/retrieve/pii/S1364032110004065>.
35. CHEN, X. [et al.]. Assessing the environmental impacts of renewable energy sources: A case study on air pollution and carbon emissions in China. *Journal of Environmental Management* [online]. 2023, **345**, 118525. ISSN 0301-4797. [viewed 22 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301479723013130>.
36. ISLAM. R. [et al.]. Alternative fuels to reduce greenhouse gas emissions from marine transport and promote UN sustainable development goals. *Fuel* [online]. 2023, **338**, 127220. ISSN 0016-2361 [viewed 30 November 2023]. Available from: <https://www.sciencedirect.com/science/article/pii/S0016236122040443>.
37. ARO, T. Preconditions and tools for cross-sectoral regional industrial GHG and energy efficiency policy-A Finnish standpoint. *Energy Policy* [online]. 2009, **37**(7), 2722–2733. ISSN 0301-4215. [viewed 22 November 2023]. Available from: https://doi.org/10.1016/j.enpol.2009.03.005>.
38. BEHNKE, N., HEGELE Y. Achieving cross-sectoral policy integration in multilevel structures-Loosely coupled coordination of „energy transition" in the German „Bundesrat". *Review of Policy Research* [online]. 2023. ISSN 1541-1338. [viewed 22 November 2023]. Available from: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/ropr.12551>.
39. COMISIA EUROPEANĂ. REPowerEU: politica energetică în planurile de redresare și reziliență ale țărilor UE. [online]. 2023. [viewed 22 November 2023]. Available from: <https://www.consilium.europa.eu/ro/policies/eu-recovery-plan/repowereu/>.
40. MATSUMOTO, K. [et al.]. Historical energy security performance in EU countries. *Renewable and Sustainable Energy Reviews* [online]. 2018, **82**, 1737–1748. ISSN 1364-0321 [viewed 30 November 2023]. Available from: <https://www.sciencedirect.com/science/article/pii/S1364032117309966>.
41. JURNALUL OFICIAL AL UNIUNII EUROPENE. Directiva 2003/30/CE a Parlamentului European și a Consiliului din 8 mai 2023 de promovare a utilizării biocombustibililor și a altor combustibili regenerabili pentru transport. [online]. 2003. [viewed 28 November 2023]. Available from: <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32003L0030&from=CS>
42. PARLAMENTUL EUROPEAN. Politica energetică: principii generale. Fișe descriptive despre Uniunea Europeană. [online]. 2023. [viewed 28 November 2023]. Available from: <https://www.europarl.europa.eu/factsheets/ro/sheet/68/politica-energetica-principii-generale>.
43. FOUQUET, D., JOHANSSON, T. European renewable energy policy at crossroads—Focus on electricity support mechanisms. *Energy Policy* [online]. 2008, **36**(11), 4079–

DOI: https://doi.org/10.53486/escst2023.09
International Conference, December 07-08, 2023, Chișinău, Moldova

4092. ISSN 0301-4215. [viewed 20 November 2023]. Available from: <https://linkinghub.elsevier.com/retrieve/pii/S0301421508003078>.

44. CONSILIUL UNIUNII EUROPENE. Energie curată pentru toți: Consiliul adoptă dosarele rămase referitoare la piața energiei electrice și la Agenția pentru Cooperarea Autorităților de Reglementare din Domeniul Energiei. [online]. 2019. [viewed 24 November 2023]. Available from: <https://eur-lex.europa.eu/legal-content/RO/TXT/HTML/?uri=CELEX:52016DC0860(01)&from=SL>.
45. AGENȚIA INTERNAȚIONALĂ PENTRU ENERGIE. Better energy efficiency policy with digital tools. [online]. 2021. [viewed 22 November 2023]. Available from: <https://www.iea.org/articles/better-energy-efficiency-policy-with-digital-tools>.

Economic Security in the Context of Systemic Transformations
DOI: https://doi.org/10.53486/escst2023.10
International Conference, December 07-08, 2023, Chișinău, Moldova

ASPECTE ALE MANAGEMENTULUI RESURSELOR UMANE ÎN INSTANȚELE JUDECĂTOREȘTI DIN REPUBLICA MOLDOVA

ASPECTS OF HUMAN RESOURCES MANAGEMENT IN THE COURTS OF THE REPUBLIC OF MOLDOVA

Ion CUPCEA
PhD Student,
Doctoral Scool of the Academy of Economic Studies of Moldova, Moldova,
ORCID 0009-0004-8030-3139
E-mail: cupceaion11@gmail.com

Abstract: *This paper analyses some aspects of human resources management in the courts of the Republic of Moldova. Taking into account the fact that human resources management is important for all categories of organizations, it has become an even more important topic for the courts of the Republic of Moldova, as a result of the reform of the justice system in this area. One of the key elements in the effective management of human resource management in the courts is to ensure a fair workload leading to an increase in institutional performance. In this context, some indicators related to human resources management and judges' workload have been analysed. Thus, the following were analysed: the coverage rate of judges' posts, the workload expressed in cases registered for a judges' post and the workload in relation to the actual number of judges. These indicators are calculated at court level. The reports of the Court Administration Agency were used as statistical data. The results show that there are disproportions in terms of workload per judge.*

Keywords: *human resource management, workload, courts, workload indicators.*

UDC: *005.96:347.97/.99(478)*

JEL Classification: *M12; M54.*

INTRODUCERE

Managementul resurselor umane acționează într-un mediu organizațional și național ce se caracterizează prin schimbarea permanentă a relațiilor dintre factorii de mediu și resursele umane. În ceea ce privește factorii de mediu ai instanțelor judecătorești, există schimbări în procedurile de muncă, precum și în normele și modelele politice și sociale care influențează activitatea personalului. Acestea, la rândul său, influențează comportamentul, ideile, atitudinile și chiar valorile acestora.

Managementul resurselor umane poate fi definit ca fiind acea parte a managementului care se ocupă de toate deciziile, strategiile, factorii, principiile, operațiunile, practicile, funcțiile, activitățile și metode legate de administrarea forței de muncă în orice tip de organizație. Instanțele judecătorești reprezintă organizațiile în cadrul cărora activează mai multe categorii de personal: judecători, asistenți judiciari, grefieri, interpreți personal administrativ etc., care printr-o cooperare eficientă poate asigura performanța acestora pe termen lung. De asemenea, activitatea eficientă a categoriilor de personal menționate mai sus pot schimba în bine reputația instanțelor judecătorești și creșterea încrederii societății în instituțiile judiciare.

ADMINISTRAREA RESURSELOR UMANE ÎN INSTANȚELE JUDECĂTOREȘTI

Resursele umane nu au fost niciodată mai necesare în sectorul judecătoresc din Republica Moldova, urmare a reformei judiciare inițiată. Angajații instanțelor judecătorești

DOI: https://doi.org/10.53486/escst2023.10
International Conference, December 07-08, 2023, Chișinău, Moldova

trebuie să remodeleze comportamentele și atitudinile pentru a se adapta noilor rigori, pentru a asigura excelența organizațională. În vederea atingerii excelenței este nevoie de o concentrare din partea tuturor angajaților pe: procesul învățării continue, munca în echipă, precum și pe reingineria resurselor umane. Astfel prin proiectarea unui rol și a unei agende noi va avea ca rezultat îmbogățirea valorii instanței judecătorești atât pentru toți angajații, cât și pentru societate.

Responsabilitatea pentru transformarea resurselor umane din instanțele judecătorești revine Consiliului Superior al Magistraturii care coordonează toate activitățile legate de managementul resurselor umane, adoptând politici, proceduri, instrumente etc. Acestea, la rândul său, permit resurselor umane din instanțele judecătorești să gestioneze procesele în mod inteligent și eficient, urmare a angajamentului angajaților și al contribuției maxime a acestora la atingerea obiectivelor instituționale.

Unul din elementele esențiale ale managementului resurselor umane în instanțele judecătorești se referă la volumul de muncă și complexitatea sarcinilor ce trebuie exercitate de către angajații acestora. Atât volumul de muncă, cât și complexitatea sarcinilor ce revin spre exercitare sunt elemente ale structurilor organizaționale care trebuie abordate cu mare atenție, pornind de la specificul activităților desfășurate în cadrul instanțelor judecătorești. Aceasta este important deoarece chiar și în cadrul aceleiași organizații cerințele privind sarcinile angajaților variază, iar angajații de același rang pot avea sarcini inegale. Discrepanțele înregistrate în volumul de muncă pot fi, în mare măsură, influențate de calificarea profesională, domeniul de specializare sau vechimea în muncă pe postul respective. Potrivit lui Sravani (2018), percepția unui angajat cu privire la echilibrul sau dezechilibrul sarcinilor de muncă, ca urmare a discrepanțelor percepute între volumul său de muncă și cel al altor membri ai organizației, poate provoca insatisfacție [8]. Conform teoriei echității, un angajat se va simți tratat incorect dacă percepe că colegii care depun eforturi similare ca și acesta câștigă mai mult sau în cazul în care câștigă la fel ca cei care depun un efort mai mic.

Volumul de muncă al angajaților este un factor determinant care reflectă performanța organizațională, în cazul nostru performanța instanței judecătorești. Dacă volumul de muncă este peste volumul standard, există tendința ca angajatul să fie suprasolicitat ceea ce ar putea duce la epuizarea emoțională, în primul rând, apoi la epuizarea fizică. În cazul judecătorilor, epuizarea emoțională are un impact direct asupra activității ulterioare a acestuia, luând în considerație și circumstanțele și riscurile în care își desfășoară activitatea profesională.

Volumul de muncă al angajaților se referă la intensitatea sarcinilor postului [2]. Altfel spus, volumul de muncă este cantitatea de muncă alocată sau așteptată de la un angajat într-o anumită perioadă de timp. Potrivit lui Hart și Staveland, (1988), volumul de muncă al angajaților a fost definit ca relația percepută între de capacitate de procesare mentală sau resursele necesare pentru a îndeplini o sarcină [3].

Din punct de vedere statistic prin volum de muncă al unei instanțe se înțelege gradul de solicitare al acelei instanțe prin luarea în considerare a numărului de dosare existente pe rol (stoc existent la sfârșitul anului anterior + număr de cauze înregistrate în anul în curs), la care se adaugă dosarele suspendate [9].

Având în vedere tendința privind variația sarcinilor de muncă între angajații din diferite instanțe judecătorești sau chiar în cadrul aceleiași instanțe, necesitatea gestionării sarcinilor de muncă devine foarte importantă. În acest context, Van den Bossche et al., (2010) susțin că managementul volumului de muncă este ajustarea volumului de muncă al

DOI: https://doi.org/10.53486/escst2023.10
International Conference, December 07-08, 2023, Chișinău, Moldova

angajaților pentru a minimiza discrepanța dintre volumul de muncă real și cel potențial [1], [6]. Printre altele, managementul volumului de muncă ajută la reducerea nevoilor de competențe specializate și tehnice, precum și la facilitarea organizării, gestionării și monitorizării volumului de muncă în conformitate cu obiectivele organizaționale. De asemenea, managementul volumului de muncă oferă resursele necesare pentru a planifica schimbările în volumul de muncă, făcând instanțele judecătorești mai adaptabile și mai receptive la mediile în schimbare [2]. Pe de altă parte, managementul volumului de muncă trebuie să caute să minimizeze discrepanța dintre sarcinile de muncă alocate și capacitatea angajatului, astfel încât acesta să nu fie copleșit de volumul de muncă. În acest scop, obiectivul principal al managementului volumului de muncă este de a minimiza dezechilibrul sarcinilor de muncă în organizații.

În acest context, performanța angajatului poate fi îmbunătățită atât timp cât volumul de muncă este menținut. Un volum mare de muncă poate afecta starea fizică și psihologică a angajatului [6], [7]. Cu toate acestea, atunci când managementul volumului de muncă este bine gestionat, acesta va influența pozitiv performanța angajaților [8].

INDICATORI DEFINITORII AI VOLUMULUI DE MUNCĂ AI JUDECĂTORILOR

Volumul de muncă poate afecta și mai mult performanța angajaților, în cazul în care există o suprasolicitare mai mare din cauza neacoperirii tuturor posturilor de muncă. În instanțele judecătorești din Republica Moldova se observă un anumit grad de neacoperire a posturilor de judecător în toate instanțele judecătorești teritoriale (Figura 1).

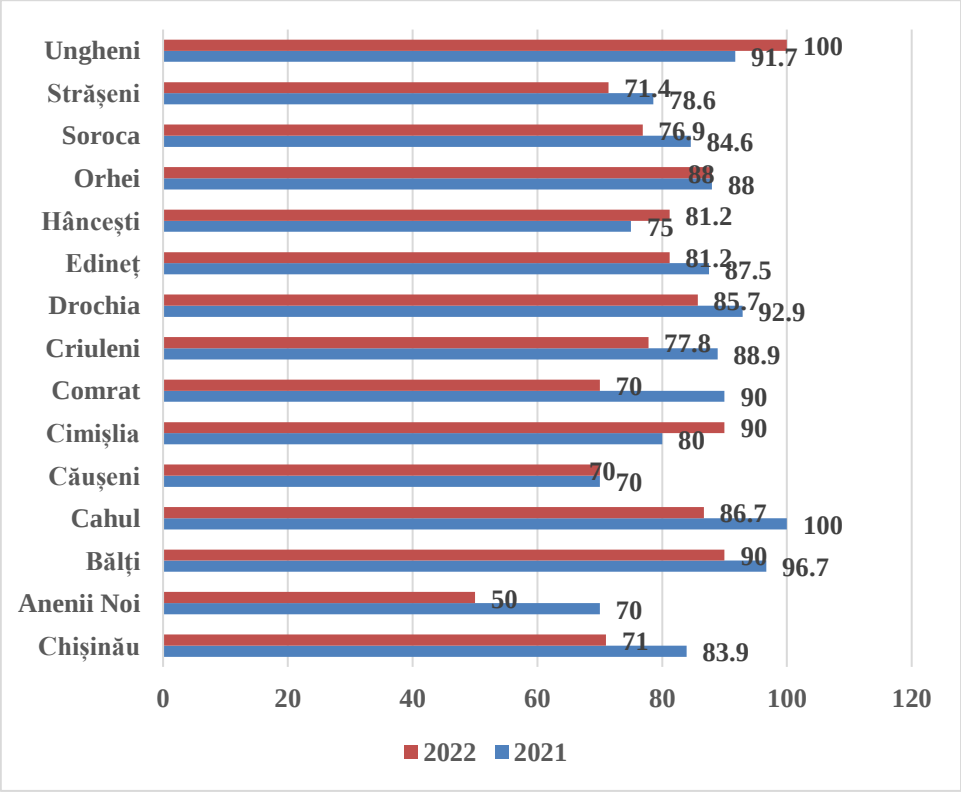


Figura 1. Rata de acoperire a posturilor de judecător în instanțele judecătorești teritoriale

Sursă: Elaborat de autor.

DOI: https://doi.org/10.53486/escst2023.10
International Conference, December 07-08, 2023, Chișinău, Moldova

Din Figura 1, constatăm un dezechilibru al volumului de muncă în instanțele judecătorești teritoriale, urmare al neacoperirii posturilor vacante. În perioada analizată, în doar două judecătorii teritoriale rata de acoperire a posturilor de judecător a fost de 100%. În anul 2021, această situație a fost valabilă pentru judecătoria Cahul, iar în anul 2022 – pentru judecătoria Ungheni.

Cea mai critică situație este în judecătoria Anenii Noi. Dacă în anul 2021, rata de acoperire a posturilor vacante de judecător a fost de 70%, în anul 2022, aceasta s-a redus până la 50%. Aceasta înseamnă că volumul de muncă per judecător s-a dublat, în anul 2022. La fel, putem constata că în unele judecătorii teritoriale (Chișinău, Căușeni, Comrat), rata de acoperire a posturilor vacante a fost mai mica de 75%, în anul 2022. Aceasta determină ca automat volumul de muncă al judecătorilor în funcțiune să crească cu 25%.

Fluctuațiile pe posturile de judecător determină ca volumul de muncă să varieze de la an la an. Aceasta crează și mai mari impedimente în rândul judecătorilor legate, în primul rând, de modificarea volumului de muncă. Urmare a creșterii volumului de muncă, crește și durata de soluționare a cauzelor aflate în cadrul judecătoriilor, ceea ce face să crească și mai mult nemulțumirea clienților.

Volumul de muncă al judecătorilor diferă de la o judecătorie la alta, ceea ce face ca judecătorii să se afle în condiții inechitabile, din cauza numărului de dosare care trebuie soluționate într-o anumită perioadă de timp. Or, aceasta cauzează mai mult stres și nemulțumiri din partea judecătorilor. În Figura 2 este prezentat nivelul de solicitare al judecătorilor raportat la numărul posturilor stabilite pe judecătorie exprimat prin volumul de muncă ce trebuie realizat la un singur post de muncă.

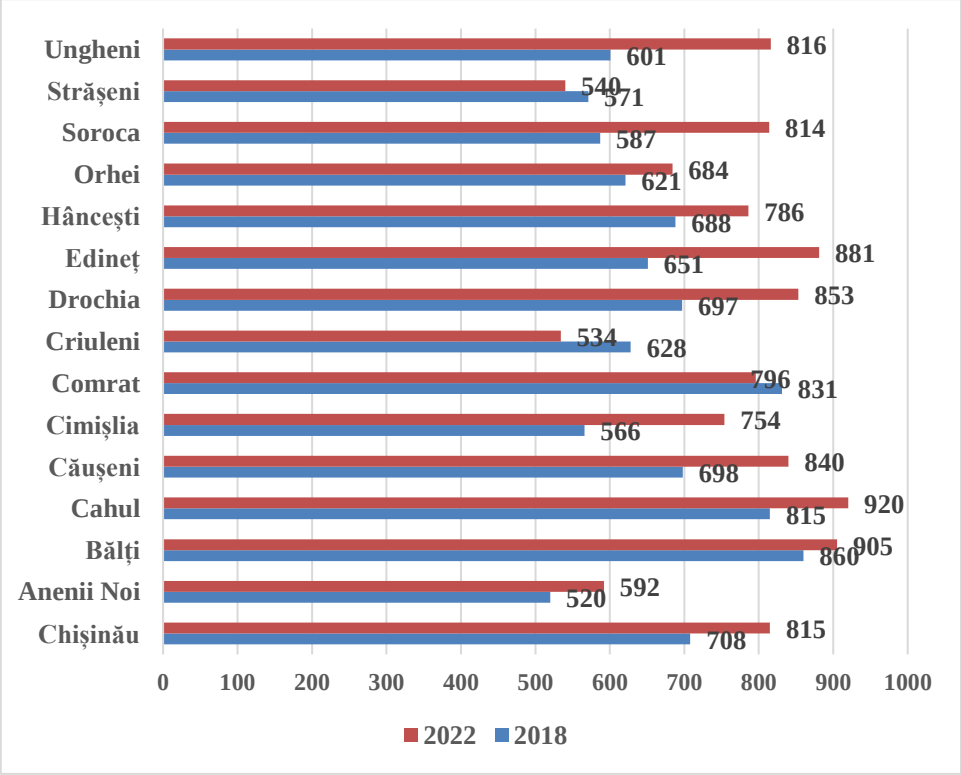


Figura 2. Volumul de muncă exprimat în numărul de cauze înregistrate în medie la un post de judecător

Sursa: Elaborat de autor.

DOI: https://doi.org/10.53486/escst2023.10
International Conference, December 07-08, 2023, Chișinău, Moldova

Din Figura 2 observăm că volumul de muncă exprimat prin numărul de cauze înregistrate variază de la o judecătorie la alta și de la un an la altul. Trebuie remarcat faptul că volumul de muncă la un post de judecător a crescut în toate judecătoriile, în perioada analizată, cu excepția judecătoriilor din Strășeni, Criuleni și Comrat. Cel mai mult, volumul de muncă la un post de judecător a crescut în judecătoriile Ungheni, Soroca și Edineț. În aceste judecătorii, volumul de muncă la un post de judecător a crescut cu peste 200 de cauze înregistrate. În majoritatea judecătoriilor, unui post de judecător îi reveneau peste 800 de cauze înregistrate, în anul 2022. Acest număr este și mai mare în cazul în care raportăm la numărul efectiv de judecători din judecătoriile teritoriale (Figura 3).

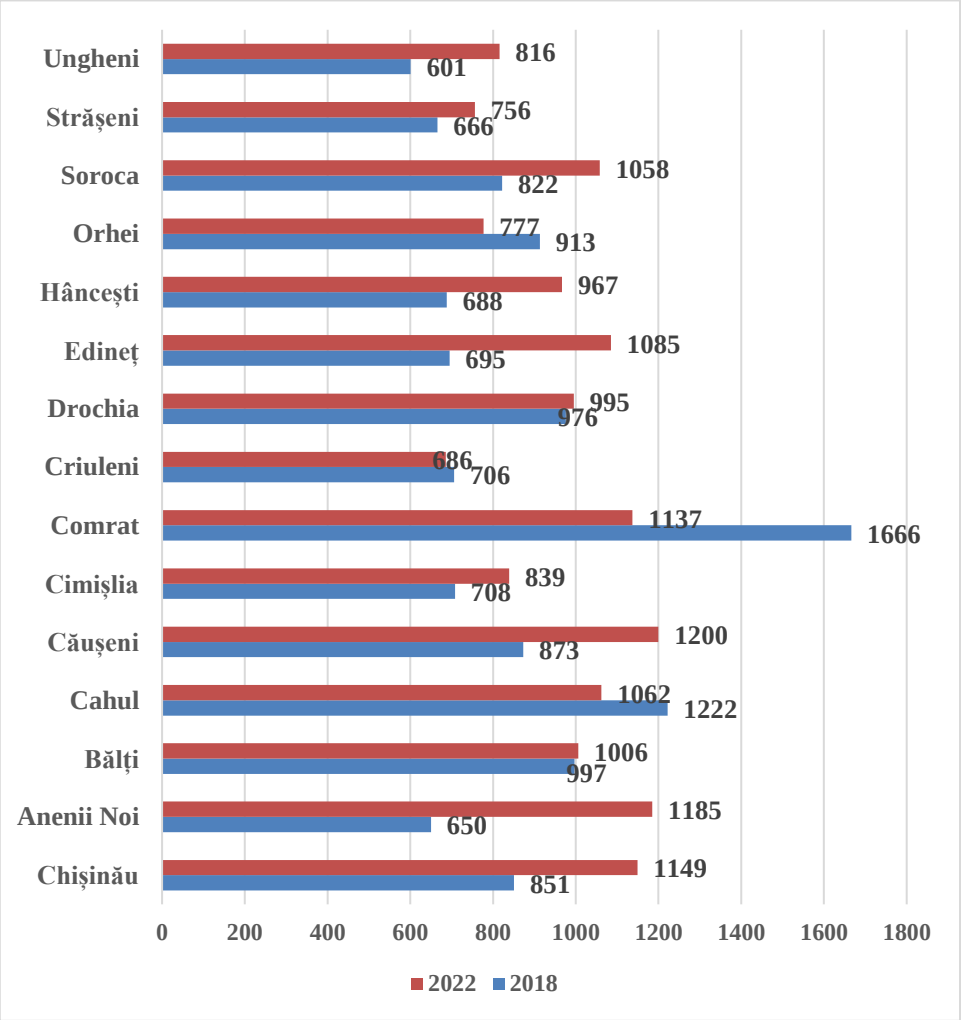


Figura 3. Nivelul de solicitare exprimat prin volumul de muncă raportat la numărul efectiv de judecători

Sursa: Elaborat de autor.

Rezultatele obținute în Figura 3 demonstrează faptul că nivelul de solicitare al judecătorilor este direct corelat cu nivelul de acoperire a posturilor de judecător. Un alt element important care a condus la creșterea nivelului de solicitare al judecătorilor este creșterea numărului de cauze înregistrate în cadrul judecătoriilor. În anul 2022, în mai multe judecătorii (Chișinău, Anenii Noi, Bălți, Căușeni, Cahul, Comrat, Edineț, Soroca), numărul e cauze înregistrate ce reveneau în medie unui judecător efectiv angajat era mai

DOI: https://doi.org/10.53486/escst2023.10
International Conference, December 07-08, 2023, Chișinău, Moldova

mare de 1000. Luând în considerație numărul efectiv de zile lucrătoare într-un an calendaristic, prin excluderea și a zilelor de concediu anual de odihnă, unui judecător din judecătoriile menționate mai sus îi reveneau mai mult de 5 cauze înregistrate pe zi. În același timp, în unele judecătorii, cum ar fi cea din Strășeni și Criuleni, mai bine de 3 cauze pe zi reveneau unui judecător.

Cu toate că există deosebiri evidente în ceea ce privește volumul de muncă revenit, în medie unui judecător, activitatea acestora este reglementată prin metodologia Consiliului Superior al Magistraturii care evidențiază mai multe criterii ce stau la determinarea numărului de posturi pentru judecători și anume:

1. Volumul de muncă pe judecător în ultimii 3 ani.
2. Numărul de dosare pe an înregistrate în instanța judecătorească.
3. Complexitatea cauzelor care trebuie soluționate.
4. Numărul de judecători pe cap de locuitori.
5. Numărul de locuitori pe circumscripția instanței de judecată.
6. Numărul de dosare specifice instanței și circumscripției respective [4].

Criteriile prezentate mai sus reprezintă repere pentru stabilirea numărului de judecători la nivelul instanței judecătorești. Chiar și prin luarea în considerație a criteriilor susmenționate observăm dezechilibre legate de numărul de dosare, în medie, la un judecător. Aceasta oricum creează nemulțumiri în rândul judecătorilor legate de efortul necesar ce urmează a fi depus pentru realizarea volumului de muncă per ansamblul judecătoriei. Transferul dosarelor de la o judecătorie la alta este o soluție pentru asigurarea echilibrului volumului de muncă între judecători în cadrul unei instanțe judecătorești, însă, în același timp, cauzează nemulțumiri în rândul clienților, urmare a distanței care trebuie parcursă.

Schimbarea rapidă a cadrului legal în toate sferele vieții în Republica Moldova, inclusiv adaptarea legislației la cerințele Uniunii Europene, în contextul aderării Republicii Moldova la această comunitate, solicită din partea judecătorilor mai mult timp pentru documentare și informare pentru luarea unor decizii judicioase. Aceasta face ca timpul de pregătire pentru pregătirea unei decizii judecătorești să crească, respectiv numărul cauzelor soluționate în instanțele judecătorești să se diminueze.

CONCLUZII

Managementul resurselor umane reprezintă un element important în administrarea eficientă a instanțelor judecătorești. În contextul demarării reformei justiției în Republica Moldova, managementul resurselor umane în instanțele judecătorește trece printr-o transformare profundă, fapt ce creează nemulțumiri în rândul personalului care activează în acest domeniu de activitate. Analiza volumului de muncă reprezintă un element esențial al managementului resurselor umane în instanțele judecătorești, deoarece felul cum acesta este repartizat în rândul judecătorilor depinde performanța instituțională.

Rezultatele cercetării demonstrează că există dezechilibre al volumului de muncă în instanțele judecătorești. Un prim factor care conduce la creșterea volumului de muncă per judecător îl constituie neacoperirea în totalitate a posturilor vacante de judecător. Astfel, am constatat că în unele instanțe judecătorești rata de acoperirea a posturilor vacante este la nivelul de 50% și 70%. Situația creată conduce, în mod direct, la creșterea volumului de muncă per judecător. Neacoperirea la timp a posturilor vacante de judecător pune o presiune mai mare pe judecătorii aflați în funcțiune, prin creșterea numărului de cauze care trebuie să le soluționeze într-o anumită perioadă de timp.

DOI: https://doi.org/10.53486/escst2023.10
International Conference, December 07-08, 2023, Chișinău, Moldova

BIBLIOGRAFIE

1. BRUGGEN, A. (2015). *An empirical investigation of the relationship between workload and performance*, *Management Decision*, Vol. 53 No. 10, p. 2377-2389. ISSN 0025-1747
2. DASGUPTA, P. R. (2013). *Volatility of workload on employee performance and significance of motivation: IT sector*. *Science Journal of Business and Management*, *1*(1), 1-7. ISSN 2331-0626.
3. HART, S. G., & STAVELAND, L. (1988). *Development of the NASA task load index (TLX): Results of empirical and the-oretical research*. In P. A. Hancock & N. Meshkati (Eds.), Human mental workload (pp. 139–183). Amsterdam:North-Holland *(3) (PDF) Subjective Task Complexity and Subjective Workload: Criterion Validity for Complex Team Tasks*. Disponibil la: https://www.researchgate.net/publication/240237178_Subjective_Task_Complexity_and_Subjective_Workload_Criterion_Validity_for_Complex_Team_Tasks [accesat 29. 11. 2023].
4. HOLDEN, R. J., SCANLON, M. C., PATEL, N. R., KAUSHAL, R., ESCOTO, K. H., BROWN, R. L., ... & KARSH, B. T. (2011). *A human factors framework and study of the effect of nursing workload on patient safety and employee quality of working life*. *BMJ quality & safety*, *20*(1), 15-24. ISSN 2044-5415
5. Hotărârea Consiliului Superior al Magistraturii nr. 175/7 din 26 februarie 2013 cu privire la aprobarea Regulamentului privind criteriile de stabilire a numărului de judecători în instanțele judecătorești. Disponibil la: https://www.legis.md/cautare/getResults? doc_id=4504&lang=ro Accesat la: 13. 11. 2023
6. INEGBEDION, H., INEGBEDION, E., PETER, A., & HARRY, L. (2020). *Perception of workload balance and employee job satisfaction in work organisations. Heliyon, 6(1), e03160. ISSN* 2405-8440.
7. NOELLE CHESLEY (2010) *Technology use and employee assessments of work effectiveness, workload, and pace of life*, *Information, Communication & Society*, 13:4, 485-514.
8. SRAVANI, A. (2018). *Managing the distribution of employee workload of the hospital staff*. IJRDO Journal of Business Management, *4*(1), 40-50. ISSN 2329-3284.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.11
International Conference, December 07-08, 2023, Chișinău, Moldova

MECANISME DE GESTIONARE A RISCURILOR FINANCIARE ÎN DOMENIUL RELAȚIILOR BUGETARE ȘI FISCALE ÎN CONTEXTUL TRANSFORMĂRILOR DIGITALE A PROCESULUI BUGETAR

FINANCIAL RISK MANAGEMENT MECHANISMS IN THE FIELD OF BUDGETARY AND FISCAL RELATIONS IN THE CONTEXT OF DIGITAL TRANSFORMATIONS OF THE BUDGETARY PROCESS

Mariana PRUTEANU

PhD Student,
Doctoral Scool of the Academy of Economic Studies of Moldova, Moldova,
ORCID 0009-0003-6039-7329
E-mail: mariana.pruteanu.md@gmail.com

Abstract:*The digital transformation of all spheres of the contemporary social-economic reproduction process, accentuated by the COVID-19 pandemic, has gained unprecedented scope in the last period of time. Remote work, e-commerce and online banking have become quite common in people's daily lives. Contemporary systemic transformations have amplified the penetration of digital tools in the private sector of the world's states, but in the public sector of national economies.*

The purpose of the article is to analyze the impact of digital transformations on the national budgetary and fiscal field in order to highlight the financial risks in the field and determine effective mechanisms to mitigate them.

The study is based on the hypothesis that determining the impact of digital transformation in the field of budgetary and fiscal relations can contribute to the adjustment of state and municipal program documents in the field of the digital economy, which will allow highlighting the mechanisms for mitigating the financial risks of not achieving key indicators performance of the budget process.

The methodological basis of the research includes general scientific methods of analysis and synthesis, induction, deduction, comparison, methods of scientific abstraction, grouping, generalization, formalization, systematization.

Keywords: *digital economy, budget process, systemic transformations, digitalization, mechanism of the digital budget process.*

UDC: *[330.131.7:336.1/.22]:004.78*

JEL classification: *H61, H69, O31, O33*

INTRODUCERE

Pandemia COVID – 19 care a cuprins întreaga lume în anul 2020 și a generat o criză economică fără precedent, a accentuat necesitatea și a demonstrat eficiența digitalizării în toate domeniile activității social – economice și politice. Republica Moldova a accelerat transformările digitale inclusiv și în sectorul public la general cât și în domeniul relațiilor bugetar – fiscale în particular. În baza analizei transformării digitale în domeniul relațiilor bugetare și fiscale pot fi identificate tendințele actuale în digitalizarea procesului bugetar în Republica Moldova, precum și evidențiate riscurile transformării digitale ale acestuia.

REZULTATE ȘI DISCUȚII

Termenul „economie digitală” a devenit atât de uzual încât a fost inclus în titlurile documentelor de planificare strategică guvernamentală. Cu toate acestea, în cercurile

DOI: https://doi.org/10.53486/escst2023.11
International Conference, December 07-08, 2023, Chișinău, Moldova

științifice și aplicativ - practice nu există o definiție general acceptată a acestui fenomen. Conceptul de economie digitală se schimbă în funcție de specificul unei anumite perioade istorice și a tendințelor globale în domeniul tehnologiilor informaționale. Astfel, prima definiție a economiei digitale a fost propusă de Don Tapscott în 1996 [3, p.145]. În lucrarea sa autorul a accentuat necesitatea utilizării tehnologiilor informaționale în toate domeniile vieții social – economice. În anii 90 ai secolului XX este evidențiată prima abordare, considerată astăzi destul de limitată, a conceptului de economie digitală, care s-a rezumat la prezentarea economiei digitale ca o economie bazată pe producția de bunuri și prestarea de servicii cu utilizarea pe scară largă a tehnologiilor digitale. O abordare mai extinsă a conceptului apare în secolul XXI și reflectă economia digitală ca și sistem economic complex în care sunt produse bunuri și prestate servicii cu utilizarea predominantă a tehnologiilor digitale iar datele în formă digitală reprezintă un factor determinant în producția de produse și prestarea de servicii. Astfel, putem concluziona că economia digitală ca categorie economică este supusă transformărilor conceptuale determinate de apariția și dezvoltarea noilor tehnologii digitale. În această ordine de idei, conceptul de economie digitală este un atribut al timpului, și nu o caracteristică esențială a unei noi etape în dezvoltarea relațiilor economice. Pe măsură ce utilizarea tehnologiilor digitale se extinde în procesul reproducției, prin economie digitală înțelegem o economie în care relațiile economice sunt construite exclusiv pe utilizarea tehnologiilor digitale.

Putem evidenția următoarele caracteristici definitorii ale economiei digitale:

1. fundamentarea relațiilor economice pe tehnologii digitale care contribuie la optimizarea structurii economiei;
2. informația și cunoașterea sunt factorii de producție determinanți;
3. rețelele moderne de informații, dispozitivele de acces, sistemele informaționale și funcționalitatea pe care acestea le oferă (prelucrarea și analiza unor cantități mari de date, calcule) sunt componentele integrante ale relațiilor economice;
4. rezultatul producției este un produs digital sau un serviciu digital;
5. digitalizarea modelelor de afaceri ale entităților economice;
6. un număr infinit de mare și în continuă creștere de relații economice interconectate pe mai multe nivele (numite și platforme digitale), care permit accesul direct utilizatorului prin mai multe canale, făcând astfel dificilă excluderea anumitor jucători, de exemplu, concurenți;
7. predominarea formelor de plată fără numerar, apariția noilor forme de plată și dezvoltarea de noi forme de bani digitali sau electronici.

Digitalizarea economiei are un șir de avantaje și dezavantaje:

Avantajele digitalizării economiei:

- reducerea cheltuielilor tranzacționale;
- apariția unor noi forme și modele de afaceri în legătură cu transmutarea lor în sfera media;
- reducerea numărului de intermediari în afaceri, interacțiunea directă și rapidă între vânzător și cumpărător, etc.

Dezavantajele digitalizării economiei:

- cerc limitat de beneficiari ai rezultatelor activității economice. În economia digitală beneficiarii sunt considerați în special producătorii de semiconductori și sisteme de control digital bazate pe acestea. Întreprinderile din Republica Moldova nu dețin tehnologii proprii pentru producția de

DOI: https://doi.org/10.53486/escst2023.11
International Conference, December 07-08, 2023, Chișinău, Moldova

semiconductori și/sau sisteme de control digital, prin urmare, nu pot fi considerați beneficiari deplini ai economiei digitale;
- atenuarea concurenței pe piața tehnologiei digitale. Companiile de locomotive ale economiei digitale urmăresc să absoarbă sau să distrugă concurenții prin repetarea funcțiilor produsului unui concurent;
- reducerea numărului de locuri de muncă, creșterea șomajului, devastarea sectoarelor conexe ale economiei;
- vulnerabilitatea și protecția insuficientă a informațiilor și a drepturilor din cauza utilizării tehnologiilor digitale perturbatoare care apar în mod constant și a creșterii numărului de atacuri cibernetice.

Avantajele transformării digitale ale economiei sunt atractive pentru toate industriile și domeniile de activitate. Tot din acest motiv, economia digitală nu se limitează la sectorul companiilor de înaltă tehnologie, pentru care „*digitalul*" este atât un obiect, un mijloc, cât și un produs de producție. În cursa conducerii, transformarea digitală este un dopaj general recunoscut care poate asigura victoria și, într-o anumită măsură, destul de legitim. Avantajele digitalizării sunt relevante și pentru domeniul relațiilor bugetare și fiscale. [3] În Republica Moldova, în diferite perioade, au fost făcute o serie de încercări de a accelera acest proces, ca parte a reformelor administrative din 2010, 2014 și 2021. Au fost supuse digitalizării mai multe niveluri ale administrației publice și al relațiilor bugetare și fiscale, care, în primul rând, au avut drept scop dezvoltarea și creșterea eficienței acestora precum și a randamentului cheltuielilor bugetare. [2]

Relațiile bugetare și fiscale în Republica Moldova au înregistrat rate accelerate de digitalizare odată cu înființarea, în 2010, a Centrului de Guvernare Electronică (în prezent Agenția de Guvernare Electronică). În continuare au fost dezvoltate și implementate o serie de platforme digitale reutilizabile, inclusiv platforma tehnologică guvernamentală comună (MCloud), serviciul electronic guvernamental de autentificare și control al accesului (MPass), serviciul guvernamental de plăți electronice (MPay), platforma de interoperabilitate (MConnect), Portalul Guvernamental al Datelor Deschise etc. [2]

Gestionarea eficientă a riscurilor financiare în domeniul relațiilor bugetare și fiscale în contextul transformărilor digitale a procesului bugetar se axează pe următoarele elemente fundamentale. [4] Primul element este ***suportul instituțional*** care reprezintă totalitatea de instituții, obiecte, subiecte, etc. ce interacționează conform odinii stabilite în contextul transformării digitale a procesului bugetar. Sub aspect instituțional, transformarea digitală a domeniului relațiilor bugetare și fiscale presupune interacțiunea subiecților procesului bugetar preponderent prin intermediul unui sistem unificat de interacțiune electronică interdepartamentală. În acest sens în Republica Moldova în anul 2010 a fost lansat procesul de e-Transformare a guvernării și creată instituția publică Centrul de Guvernare Electronică. Scopul CGE este facilitarea actelor de guvernare prin intermediul aplicării intensive a tehnologiilor informaționale. În 2018 CGE este restructurat în Agenția de Guvernare Electronică.

Al doilea element fundamental al transformărilor digitale a procesului bugetar este ***baza legală și normativă*** a digitalizării. Acesta prevede existența unui cadru normativ adecvat, ce include documente care reglementează procedura transformării digitale a tuturor proceselor în administrația publică precum și a procesului bugetar (de formare și executare a bugetului public național prin intermediul instrumentelor digitale și interacțiune a participanților acestuia).

DOI: https://doi.org/10.53486/escst2023.11
International Conference, December 07-08, 2023, Chișinău, Moldova

Al treilea element a procesului digitalizării domeniului relațiilor bugetare și fiscale este ***suportul informațional***, care se caracterizează prin prezența tehnologiilor digitale, a sistemelor informatice și analitice și a tehnologiilor de protecție a datelor care permit executarea sigură și eficientă a procesului bugetar. În contextul gestionării eficiente a riscurilor în domeniul relațiilor bugetare și fiscale în condițiile digitalizării este necesar să evidențiem impactul tehnologiilor de protecție a datelor. Asigurarea securității informațiilor în contextul utilizării tehnologiilor digitale inovatoare (care apar cu o regularitate constantă) a devenit sarcină prioritară a guvernelor statelor lumii în era globalizării. Această tendință se datorează creșteri numărului și a intensității riscurilor atacurilor cibernetice a domeniului bugetar - fiscal, a încălcării integrității și a continuității funcționării instituțiilor din sectorul public și, în consecință, a incapacității de furnizare a serviciilor bugetare calitative și eficiente populației și, drept rezultat, a creșterii tensiunii sociale în stat. Gradul de complexitate a metodelor și a strategiilor de desfășurare a atacurilor cibernetice necesită utilizarea noilor tehnologii de protecție a datelor în domeniul relațiilor bugetare și fiscale, în special protecția datelor atunci când se efectuează transferuri de fonduri bugetare. Tehnologiile de protecție a datelor fac posibilă crearea și introducerea sistemului dublului control (sau a așa numitului sistemu de coridor: „verde” și „roșu”) la prelucrarea informațiilor în toate etapele procesului bugetar, obținând confirmarea suplimentară a tranzacțiilor financiare de către principalii manageri ai fondurilor bugetare și destinatarii fondurilor bugetare.

În baza celor expuse anterior putem evidenția următoarele perspective de transformare digitală a procesului bugetar în Republica Moldova:

1. elaborarea unui model de interacțiune digitală între participanții procesului bugetar, inclusiv a unui mecanism de interacțiune între instituțiile publice la toate nivelurile sistemului bugetar;
2. implementarea sistemului de formare a personalului care vizează utilizarea noilor tehnologii digitale în activitatea lor precum și crearea un sistem de suport de înaltă calitate a procesului bugetar în condițiile digitalizării continue;
3. crearea unui mediu digital accesibil, sigur și incluziv.

CONCLUZII

În concluzie putem afirma, că transformările digitale a domeniului relațiilor bugetare și fiscale în Republica Moldova sunt determinate de noi forme de organizare a elaborării proiectelor de buget, a aprobării și executării, a raportării modului de execuție a bugetului, etc. bazate pe utilizarea pe scară largă a tehnologiilor informaționale pentru integrarea și interacțiunea tuturor participanților la diferite etape ale procesului bugetar. Digitalizarea s-a manifestat în mecanismul procesului bugetar digital, o trăsătură distinctivă a căruia este disponibilitatea suportului informațional care ajută la eliminarea costurilor tranzacționale și la creșterea eficienței cheltuielilor bugetare. Esența componentelor rămase ale mecanismului procesului de buget digital rămâne aceeași, doar forma existenței lor s-a schimbat. Evaluarea eficacității transformării digitale a procesului bugetar permite nu doar determinarea gradului de digitalizare a domeniului bugetar și fiscal, ci și identificarea principalelor riscuri și amenințări ale digitalizării sistemului atât la nivel național, cât și cel regional, municipal și local.

DOI: https://doi.org/10.53486/escst2023.11
International Conference, December 07-08, 2023, Chișinău, Moldova

BIBLIOGRAFIE

1. *Cadrul bugetar pe termen mediu al Republicii Moldova (2024-2026) [online]*. [Accesat 22 decembrie 2023] Disponibil: <https://www.mf.gov.md/sites/default/files/1.%20Proiect%20HG%20privind%20aprobarea%20CBTM%202024-2026.pdf>
2. *Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030*, (2023), [online]. [Accesat 22 decembrie 2023]. Disponibil: <https://mded.gov.md/transparenta/64373-2/>
3. TAPSCOTT, D. *The digital economy: promise and peril in the age of networked intelligence*. McGraw-Hill, 1996.
4. VAN GORP, N., BATURA, O., (2015). *Challenges for competition policy in a digitalised economy*. Brussels European Parliament [online]. [Accesat 22 decembrie 2023]. Disponibil: <https://www.europarl.europa.eu/RegData/etudes/STUD/2015/542235/IPOL_STU(2015)542235_EN.pdf>

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.12
International Conference, December 07-08, 2023, Chișinău, Moldova

RISK ASSESSMENT AND HEDGING AS THE BASIS OF FINANCIAL SECURITY OF THE ENTERPRISE

Liudmila LAPIȚKAIA

PhD, Associate professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0001-9739-0495
E-mail: liudmila@ase.md

Abstract: *Financial security is the basis for the effective development of any economic agent; it is especially important for enterprises, since their financial security underlies the security of both households and the state. This article examines the risks that can lead to the loss of the financial security of an enterprise, which the author classified into: general economic, industry- specific and risks of a particular enterprise. Hedging financial security risks will be most effective if the management of the enterprise evaluates the risks, using the classification proposed by the author. The financial security of an enterprise depends on the financial resources necessary for its normal condition, ensuring their placement and efficient use, financial stability with other legal entities and individuals, solvency and financial stability, as well as on the efficiency of the operating, financial and other activities of the enterprise. By the financial condition one can judge the solvency, liquidity and financial stability of the enterprise. In a market economy, defining the boundaries of an enterprise's financial security is one of the most important economic problems, since insufficient financial stability can lead to a shortage of funds for enterprises, and to their insolvency and, ultimately, bankruptcy, as well as "excessive" stability will slow down development, burdening the enterprise with excess inventories and reserves. Financial security should be considered taking into account the risks that arise both at the level of the economy as a whole, and at the level of the industry and at the level of the enterprise itself.*

Keywords: *risk assessment, hedging, financial security.*

UDC: *[330.131.7:336]:334.72*

JEL Classification: *D61, G32.*

INTRODUCTION

Financial security is the basis for the effective development of any economic agent, starting from the household and ending with the state. In this model, enterprises play a significant role in maintaining the financial security of both households and the state. Various definitions and concepts of financial security are considered in the economic literature, as I. Blank defines financial security as a quantitatively and qualitatively determined level of the financial condition of an enterprise [2]. While Papekhin R. defines the financial security of an enterprise as a complex concept reflecting such a state of finance in which the enterprise is able to develop steadily while maintaining its financial security in conditions of additional risk [3].Alexandr Cauia considers financial security as a concept that includes a set of measures, methods and means to protect the economic interests of the state at the macro level, corporate structures, financial activities of business entities at the micro level [1].

According to the author, financial security is the ability of an economic agent, using resources, primarily financial, to withstand risks.

DOI: https://doi.org/10.53486/escst2023.12
International Conference, December 07-08, 2023, Chișinău, Moldova

PAPER BODY

Analyzing the economic literature, we can state the fact that the risks faced by the enterprise are mainly classified as internal and external. The author offers a classification of the risks faced by the enterprise into:

- *General economic,*
- *Industry-specific,*
- *Risks of a particular enterprise.*

In turn, the general economic risks faced by the enterprise can be represented as follows:

- *Unstable economy, economic crisis or stagnation,*
- *hyperinflation,*
- *unfavorable macroeconomic indicators,*
- *the crisis of the country's financial and credit system,*
- *political crises,*
- *frequent changes in legislation, in terms of taxation, lending, insurance, customs legislation*

Industry-specific risks that affect the financial security of an enterprise can be presented as follows:

- *negative changes occurring in the economic sector in which the enterprise operates,*
- *disloyal competition from competitors,*
- *legislative prohibitions for enterprises in a particular industry to export their products,*
- *frequent changes in regulations and legislation for the industry in which the enterprise operates,*
- *government restrictions on the selling price of goods or products*.

The company itself may face the following types of risks, which can significantly affect its financial security:

- *unfavorable financial performance,*
- *aspects related to disruption of business continuity or liquidity of the enterprise;*
- *development and offering to the market new types of goods or services or transition to a new spectrum of the economy;*
- *weak marketing and pricing policy,*
- *lack of strategic planning and budgeting,*
- *lack of trained, qualified personnel,*
- *changes in the structure of the enterprise, including reorganization,*
- *poor organization of the enterprise's internal control system;*
- *discrepancy between information and entrepreneurial strategy;*
- *changes in the information environment of the enterprise;*
- *transactions or events that lead to estimation uncertainty, including accounting;*
- *litigation.*

Analyzing general economic risks, it can be stated that one of the main indicators affecting the activities of an enterprise is inflation. Figure 1 shows the dynamics of inflation in the Republic of Moldova from 2018 to 2022, it should be noted that in 2022 it amounted to 30.2%.

DOI: https://doi.org/10.53486/escst2023.12
International Conference, December 07-08, 2023, Chişinău, Moldova

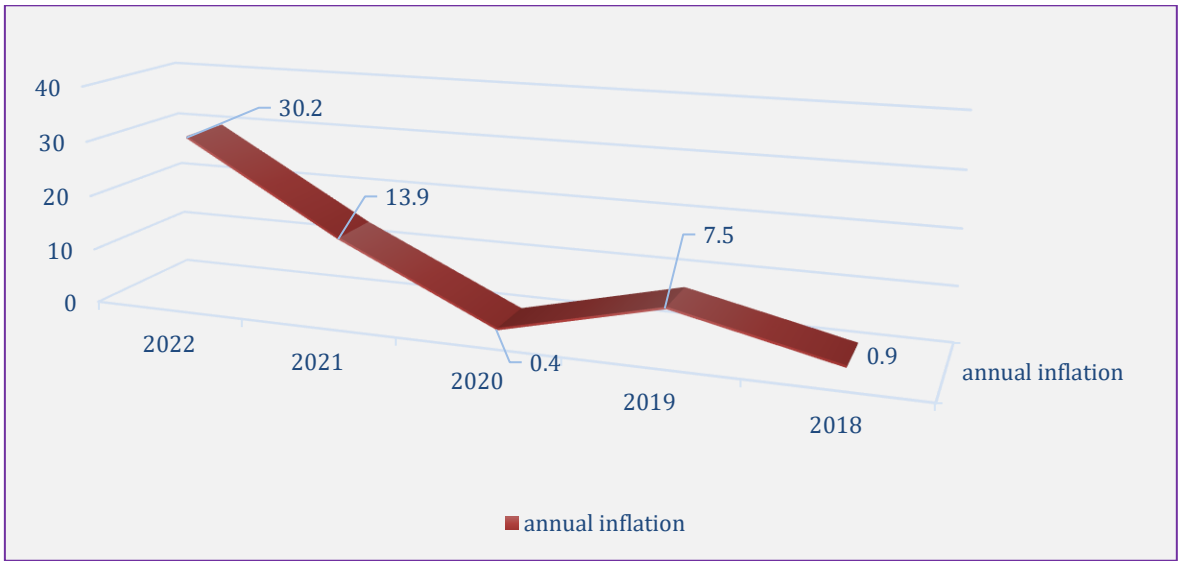
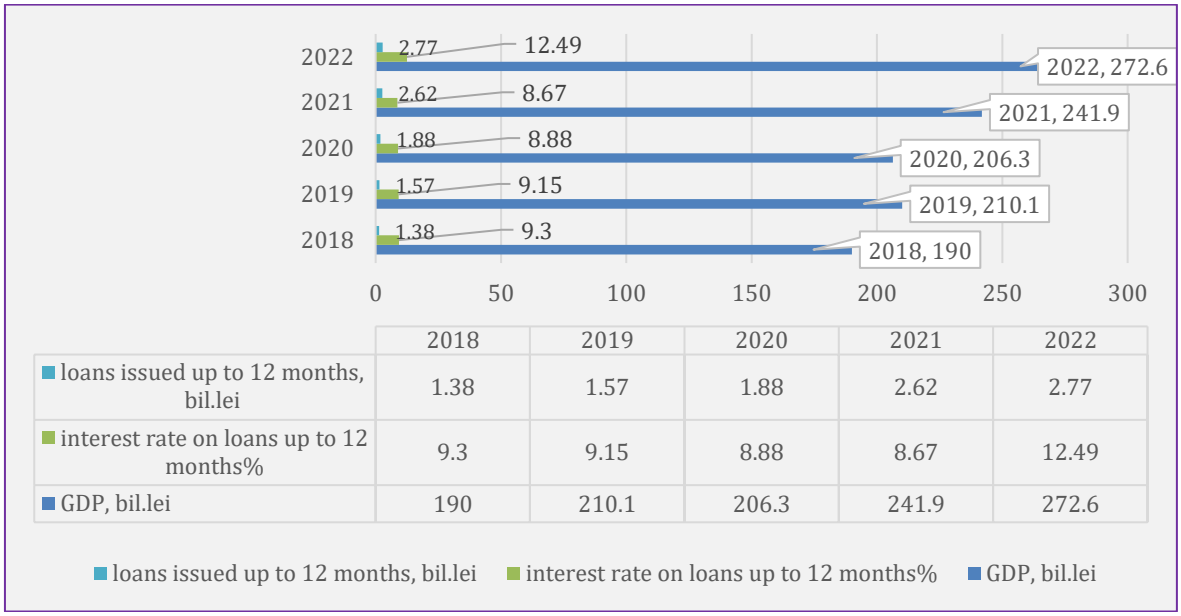


Figure 1. Annual inflation in the Republic of Moldova in dynamics
Source: Elaborated by the author according to the NBM' s data https://www.bnm.md/ro/content/rata-inflatiei-0

Analyzing the macroeconomic indicators and their impact on the financial security of the enterprise, presented in Fig. 2, we can note the following:

- *over the period 2018-2022, GDP has steadily grown and in 2022, compared to 2018, the growth rate was 143.4%*
- *there is an increase in loans issued to enterprises, the growth rate in 2022 compared to 2018 was 195.6%.*



	2018	2019	2020	2021	2022
loans issued up to 12 months, bil.lei	1.38	1.57	1.88	2.62	2.77
interest rate on loans up to 12 months%	9.3	9.15	8.88	8.67	12.49
GDP, bil.lei	190	210.1	206.3	241.9	272.6

Figure 2. Macroeconomic indicators of the Republic of Moldova in dynamics
Source: Elaborated by the author according to the NBM' s data https://www.bnm.md/bdi/pages/reports/dpmc/DPMC8.xhtml?id=0&lang=ro

DOI: https://doi.org/10.53486/escst2023.12
International Conference, December 07-08, 2023, Chişinău, Moldova

If we analyze the indicators of Fig. 2, namely, the dynamics of the interest rate on loans up to 12 months granted to legal entities, then we can state that the rate decreased in 2019 compared to 2018 by 0.3 points, respectively, in 2020 compared to 2019, a decrease of 0.27 points, in 2021 compared to 2021, a decrease by 0.21 points and a sharp increase in the loan rate in 2022 in relation to 2021 by 3.82 points.

At the same time, it is observed that the amount of loans received was not affected by the level of the interest rate, for example: in 2020, when the interest rate was 8.88%, 1.88 bil. lei of loans were taken, while in 2022, when the rate was 12.49%, 2.77 bil.lei of loans were issued.

It is necessary to analyze in more detail the trend in GDP growth and loans received by legal entities for up to 12 months, what is presented in table 1.

Table 1. Trends in economic indicators of Moldova

	2019	2020	2021	2022
GDP growth rate in relation to previous year, %	100,6	98,2	117,3	112,7
Growth rate of loans issued For legal entities up to 12 months in relation to the previous year, %	113,7	119,7	139	105,7

Source: Elaborated by the author according to the NBM' s data https://www.bnm.md/bdi/pages/reports/dpmc/DPMC8.xhtml?id=0&lang=ro

Analyzing the data in Table 1 and the information presented above, it can be stated that the amount of loans received does not depend on the growth of inflation, and the activity of the economy, changes in the quantitative indicators of GDP have a certain impact on the amount of loans received.

The financial security of an enterprise depends on the availability of financial resources necessary for its normal functioning, the appropriateness of their placement and efficiency of use, financial relationships with other legal entities and individuals, solvency and financial stability, as well as on the effectiveness of the operational, financial and other activities of the enterprise.

The financial condition of an enterprise shows the degree to which the enterprise is provided with financial resources, as well as the feasibility of investing financial resources in activities and the efficiency of their use. By the financial condition one can judge the solvency, liquidity, and financial stability of the enterprise. It is on the basis of these data that the enterprise's operating strategy is developed, performance assessments are made and decisions are made about the prospects for the enterprise's activities.

The financial condition directly depends on the performance indicators of the enterprise. The efficiency of each enterprise is expressed in financial results, such as: profit received as a result of entrepreneurial activity. The return on sales is an indicator of the financial activity and efficiency of the enterprise, this indicator shows how much gross profit per 1 lei of sales income, the indicators of return on assets and equity are also calculated.

An important condition for assessing the financial security of an enterprise is the calculation and analysis of the financial indicators of the enterprise.

Analysis of financial indicators is one of the methods for assessing the state of an enterprise and its capabilities in the future. It acts as the basis for strategic planning, helps management identify resources and directions for subsequent development of the enterprise, and find its strengths and weaknesses. Analysis of financial ratios is carried out

DOI: https://doi.org/10.53486/escst2023.12
International Conference, December 07-08, 2023, Chişinău, Moldova

in order to identify optimal ways to achieve the goals of the enterprise, such as increasing business activity - asset turnover, ensuring liquidity and financial stability, increasing the profitability of the enterprise.

Based on the content of the financial condition, we can draw the following fundamental conclusion that the financial security of an enterprise is based on:

- *rationality of the structure of assets and liabilities, that is, the enterprise's funds and their sources,*
- *efficient use of property and profitability of products,*
- *the degree of its financial stability,*
- *the level of liquidity and solvency of the enterprise.*

Analyzing the economic indicators of small and medium-sized enterprises in the dynamics in the Republic of Moldova, it should be noted that they make a significant contribution to the development of the national economy.

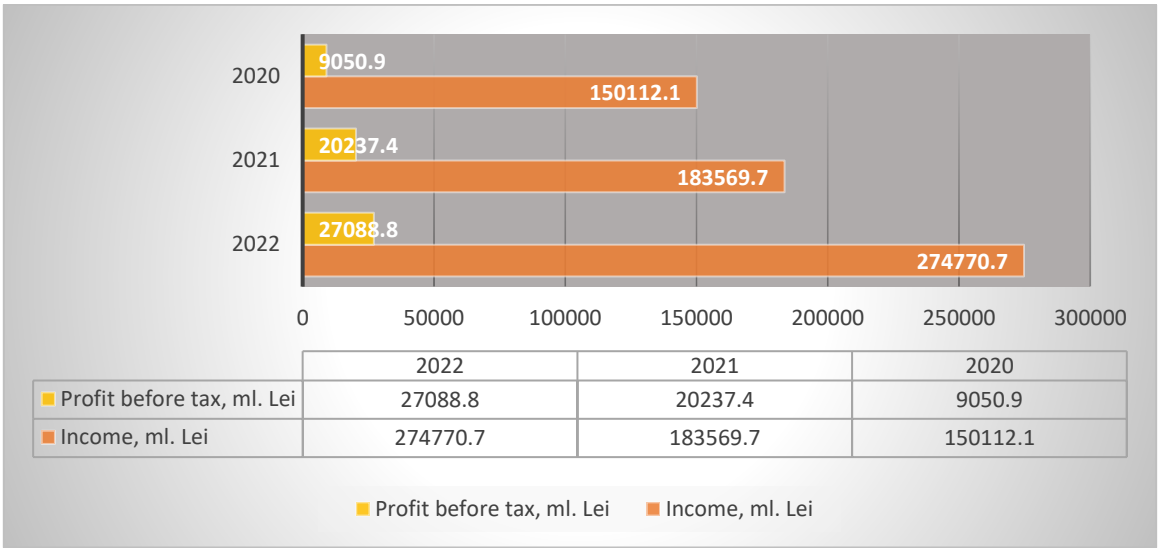


Figure 3. Economic indicators of Small and Medium-sized Enterprises of the Republic of Moldova in dynamics

Source: Elaborated by the author according to the NBS' s data
https://statistica.gov.md/ro/statistic_indicator_details/22

Based on the data presented in Figure 3, the following conclusions can be drawn:

- The profitability of sales by profit before taxation of small and medium-sized enterprises in the Republic of Moldova in 2020 amounted to 6 bani per 1 lei of sales income, in 2021 -11 bani, in 2022 - 10 bani.
- It should be noted that in the conditions of high inflation in 2022, small and medium-sized enterprises of the Republic of Moldova managed to keep the profitability of sales almost at the level of last year.
- The profitability of sales in the region of 10% of sales revenue is considered a good indicator at the level of the global economy.

Risk management is becoming more relevant every year and more and more organizations and managers are introducing risk management schemes into their activities. The main goal of neutralizing risks when implementing a new activity is to protect it from all kinds of risks that prevent it from achieving its goals.

DOI: https://doi.org/10.53486/escst2023.12
International Conference, December 07-08, 2023, Chișinău, Moldova

The process of managing activity risks involves minimizing possible risks or losses of the project related to profit, people or other problems that may arise during work.

The use of the hedging method to neutralize risks is relevant today, since this financial instrument is directly aimed either at compensating for the expected losses of the enterprise, or at insuring against unplanned low profits.

The use of a risk hedging system, on the one hand, provides a guarantee to the acquirer or investor, some kind of insurance protection against all kinds of adverse consequences, but, on the other hand, it is necessary to give part of the profit for such reliability.

In essence, hedging is somewhat similar to classical types of insurance – for the opportunity to rely on insurance protection, the policyholder will have to pay an insurance premium. In order to make the most optimal use of hedging, it is necessary to develop a clear and effective program for its implementation, which will help reduce the risk levels to the minimum.

In the process of implementing a hedging program, an analysis of the effectiveness of the strategies used in hedging should be implemented. A hedging strategy is a set of specific financial hedging instruments and methods of using them to reduce the risks.

Hedging can reduce various types of risks to a reasonable level, primarily using various derivative financial instruments, such as forwards and futures, currency swaps, which makes it possible to isolate and control the effect of managing a particular type of risk.

In addition, enterprises can use long-term contracts, transfer pricing, and the use of insurance policies as risk hedging, an enterprise can manage risks, namely avoid, prevent, and reduce.

A company is exposed to financial risk due to its dependence on market factors such as commodity prices, exchange rates and interest rates. In a civilized market economy, insurance, or hedging, of such risks is often an integral part of business planning.

The purpose of hedging is to eliminate the uncertainty of future cash flows (both negative and positive), which will allow you to have a complete picture of future income and expenses arising in the course of financial or business activities.

Thus, the main task of hedging is to transform risk from unpredictable forms into clearly defined ones.

In modern practice, the hedging process is closely interconnected with the overall management of the company's assets and liabilities and covers the entire set of actions aimed at eliminating or at least reducing financial risks.

The implementation of risk hedging strategies should be carried out with control over the implementation of decisions made in the process.

When hedging the risks of an enterprise, one should take into account the classification of risks proposed by the author: into general economic, sectoral and the enterprise itself.

To effectively hedge risks at the general economic level, enterprise management must monitor changes in the exchange rate and interest rates on loans. In situations where an enterprise has funds in foreign currency, with a favorable exchange rate for the corresponding currency, upon exchange, it is possible to receive a positive influx of funds in national currency.

The management of the enterprise must constantly promptly analyze the financial situation and performance of the enterprise in order to make the right decisions in a timely manner to overcome crisis situations.

DOI: https://doi.org/10.53486/escst2023.12
International Conference, December 07-08, 2023, Chişinău, Moldova

Despite the costs associated with hedging and the difficulties that an enterprise may encounter in developing and implementing a hedging strategy, its role in ensuring the progressive development of the enterprise is quite large and is associated with:

- the possibility of significantly reducing the price risk associated with the purchase of raw materials and the supply of finished products;
- freeing up enterprise resources and helping management focus on core aspects of the business, minimizing risks,
- the ability to increase capital, reducing the cost of using funds and stabilizing income;
- ensuring constant financial protection using market and non-market instruments;
- making it easier to attract credit resources: banks take into account hedged collateral at a higher rate; the same applies to contracts for the supply of finished products.

Types of hedging using market mechanisms can be classified as follows:

- *by type of hedging instruments (exchange and over-the-counter contracts);*
- *by type of counterparty (buyer and seller hedge);*
- *by the amount of insured risks (full or partial);*
- *in relation to the time of conclusion of the underlying transaction; (depending on the time of acquisition of the underlying asset);*
- *by asset type;*
- *under the terms of the hedging contract (one-way, two-way hedging).*

For hedging purposes, management of an enterprise can use:

1. effective management of the assets and liabilities of the enterprise; for each period of time, the amount of assets and liabilities with the corresponding repayment periods is determined. A significant advantage as a risk hedging tool is its simplicity and clarity combined with the possibility of a comprehensive analysis of assets and liabilities,
2. forward agreements,
3. futures contracts,
4. currency options,
5. swap contracts,
6. diversification of assets, that is, the distribution of free investment capital into stocks, bonds, real estate, bank deposits, precious metals,
7. purchase and sale transactions of long-term and short-term government securities.

At the same time, the disadvantages of hedging should also be considered, for example, the considered insurance mechanism is not a panacea for all risks, since it has a number of significant disadvantages:

- conscious refusal of possible additional profit;
- excess costs for opening and fulfilling obligations under hedging transactions;
- the risk of changes in legislation in economic and tax policy (introduction of taxes). In this situation, the hedge will not only not protect, but will also lead to losses;
- exchange restrictions;
- increase in the number and complexity of the structure of transactions.

DOI: https://doi.org/10.53486/escst2023.12
International Conference, December 07-08, 2023, Chişinău, Moldova

CONCLUSIONS

In market conditions, the key to survival and the basis for a stable position of an enterprise is its financial security. It also reflects the state of financial resources in which an enterprise, freely maneuvering funds, is able, through their effective use, to ensure an uninterrupted process of production and sales of products, as well as to bear the costs of its expansion and renewal.

Determining the boundaries of the financial security of an enterprise is one of the most important economic problems in a market economy, since insufficient financial stability can lead to a lack of funds for enterprises to develop production, their insolvency and, ultimately, bankruptcy, and "excessive" stability will hinder development , burdening the enterprise with excess inventories and reserves.

Financial security should be considered taking into account those risks that arise both at the level of the economy as a whole, and at the industry level and at the level of the enterprise itself.

For an enterprise to operate effectively, its management must develop a risk hedging strategy, which should include:

1. taking into account general economic risks:
- monitoring and analysis of the exchange rate, interest rates on loans, inflation rates and prices in the economy for specific raw materials, services, energy resources,
- development of response measures to optimize cash flows in terms of the acquisition of raw materials, energy, services

2. taking into account industry risks:
- it is necessary to monitor constant changes in legislation related to this industry,
- revise pricing policy, depending on market conditions,
- analyze the activities of competitors in the sale of identical goods and services

5. at the enterprise level:
- effectively manage assets and liabilities,
- promptly analyze financial indicators of an enterprise: liquidity, turnover, return on sales, assets, equity, and, above all, in case of declining of these indicators, take appropriate effective hedging measures.

BIBLIOGRAPHY

1. CAUIA, A. *Securitatea financiară — componentă fundamentală a securității naționale*. Studii Juridice Universitare. 2020 (2). ISSN 1857-4122.
2. БЛАНК, И. *Управление финансовой безопасностью предприятия*. Киев: Эльга, 2009. ISBN: 978-966-521-256-0.
3. ПАПЕХИН, Р. *Теоретические основы финансовой устойчивости предприятий.* Волгоград: Волгоградское научное изд-во. 2008. ISBN 978-5-534-13505-3.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chişinău, Moldova

THE EFFICACY OF FINANCIAL STABILITY ON ECONOMIC GROWTH: THE EXPERIENCE OF DEVELOPING COUNTRIES WITH LARGE FINANCIAL SECTORS

Mahlatse MABEBA

Affiliate member,
South African Institute of Financial Markets, South Africa,
ORCID 0000-0003-4646-679X
E-mail: mahlatsemabeba@gmail.com

Abstract: *Recent years have attracted the attention of policymakers about the effect of financial stability on economic growth. These developments raise more concern for developing countries with large financial sectors. From a recent history of financial crises, we learn that countries highly exposed to international financial markets experience adverse economic trajectories. The focal countries for this study are Brazil, India, Indonesia, Malaysia, Mexico, and South Africa. This empirical study has a sample period from 1996 to 2022, capturing the most recent quantifiable events. The study considers aggregate measures of financial stability from the financial system. We make use of the random effects panel data methodology which captures the heterogeneity associated with the developing countries in variegated continents. The implication of this study is that financial stability policies that aim to stabilize financial institutions and their functions will significantly affect economic growth. This study finds that financial stability has a significant and negative effect on economic growth.*

Keywords: *financial stability, economic growth, large financial sector, developing countries, panel data econometrics.*

UDC: *336.74.02:330.35(1-773)*

JEL Classification: *C23, E44, G10, G20.*

INTRODUCTION

In developing countries with large financial sectors, the efficacy of financial stability on economic growth takes on a unique and multifaceted significance. These nations often experience rapid expansion in their financial systems, characterized by the proliferation of banks, stock exchanges, and other financial intermediaries. While the growth of the financial sector can be a promising sign of economic development, it also introduces a set of challenges and opportunities that require careful consideration. The stability of these financial systems in such contexts becomes even more critical, as it not only influences the broader economic landscape but also determines the ability of countries to harness the full potential of their financial sectors.

We provide some insights into the financial stability of six developing countries with large financial sectors which includes Brazil, India, Indonesia, South Africa, Malaysia, and Mexico. After the 2008 global financial crisis, Brazil felt the effects of reduced global demand, affecting its trade balance and economic growth. There were disruptions in financial markets, and the country's stock market faced declines. The crisis contributed to increased volatility in currency markets. Brazil experienced currency depreciation as investors sought safe-haven assets, impacting the value of the Brazilian real (Barroso and Nechio, 2020) [1].

India's financial stability is influenced by a diverse and growing financial sector. The country has a robust banking system and a well-regulated stock market. However,

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chișinău, Moldova

India has experienced non-performing loan issues in its banking sector, and regulatory reforms are ongoing to address these concerns. The government has also introduced measures to encourage foreign investment and economic growth (Kumar et al., 2022) [2].

Indonesia's financial stability has benefited from prudent financial regulation and economic reforms. The country has seen stable economic growth, supported by strong commodity exports. Nonetheless, Indonesia faces challenges related to income inequality, infrastructure development, and managing inflation (Machdar, 2020) [3].

South Africa's financial stability is influenced by a well-developed financial sector and a relatively open economy. The country faces challenges related to high unemployment, income inequality, and political uncertainty. South Africa's fiscal situation has also been a concern, leading to credit rating downgrades in the past (Mishi & Khumalo, 2019) [4].

Malaysia has a diversified economy with a well-regulated financial sector. The country has a history of prudent financial management and has taken measures to maintain economic stability. However, challenges include addressing issues related to government debt, managing fiscal deficits, and enhancing the efficiency of state-owned enterprises (Koong et al., 2017) [5].

Mexico's financial stability is closely tied to its economic relationship with the United States, given its extensive trade ties. The country has benefited from structural reforms, such as energy sector liberalization, but it faces challenges related to high levels of informality in the labor market, income inequality, and security concerns (Gambacorta, L., & Murcia, 2019) [6].

The interplay between financial stability and economic growth in developing countries with substantial financial sectors is a topic of great importance, as it holds the potential to unlock or hinder their journey towards sustained prosperity. In this context, understanding how financial stability affects these economies is vital for policymakers, investors, and the general populace. This exploration will delve into the specific dynamics at play in such nations, examining how financial stability impacts economic resilience, and how it shapes the overall trajectory of development in these rapidly evolving financial landscapes.

The goal of the study is to estimate the effect of financial stability on economic growth in developing countries with large financial sectors. Therefore, the empirical hypothesis of this study is that "financial stability has a causal effect on economic growth in developing countries with large financial sectors." The study deploys the random effects as a panel data model to account for the heterogeneity of developing countries in different part of the world. The sample period of the study comprises annual data from 1996 to 2022. The study finds that financial stability is causal on economic growth. From the sample period, there is a negative and highly significant effect of financial stability on economic growth.

LITERATURE REVIEW

Financial stability refers to a financial system that is resilient to systemic shocks, facilitates efficient financial intermediation and mitigates the macroeconomic costs of disruptions in such a way that confidence in the system is maintained (SARB, 2015) [7]. Financial stability is the efficient allocation of economic resources through smooth savings and investment processes that enhance economic growth (Schinasi, 2011) [8]. Financial stability is affected by both exogenous and endogenous factors. Shocks and surprises are not the only components that pose a threat to the financial system, also disorderly

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chișinău, Moldova

adjustment of imbalances can cause financial instability. For example, there could be a misperception of expectation of future returns that could subsequently miss-price future price (Schinasi, 2011) [8].

Inefficient allocation of capital and mispricing of risk can cause vulnerabilities and imbalances thus threaten financial stability (Peukert, 2010) [9]. Financial stability is to protect the economy from financial crises and enabling a financial system so that it limits and addresses emergence of imbalances before they constitute a threat to stability. This may be received by self-corrective, market disciplining mechanisms that can create resilience and that can endogenously prevent development of system-wide risk (Peukert, 2010) [9]. Forces are allowed to resolve potential problems but there is room for intervention through liquidity injections.

A financial system is a system that allows the transfer of money through the savers to investors. The financial system comprises of three broad closely related concepts (Schinasi, 2011). These are financial intermediaries, financial markets, and the financial infrastructure. Financial intermediaries are financial institutes that pool funds and reallocate funds for different uses. Financial institutions are not simply limited to banking services; they include a variety of institutes, such as, hedge funds, pension funds, non-financial hybrids, that provide a range of different services. Financial markets are markets that directly serve investors and savers through the direct buying and selling of equities and bonds. Finally, the financial infrastructure, comprises of clearance, payments, and settlement systems, and regulatory, supervisory and surveillance infrastructure (Schinasi, 2011). Furthermore, private, and public persons who participate in the financial market are an essential part of the financial infrastructure (Allen and Wood, 2006) [10]. The key concepts identified here are important to grasp and monitor their activities for understanding how well a financial system works and how well they are performing.

Systemic risk is the threat of a possible collapse of the financial system; it is a risk of an event that may cause a loss of real economic value or confidence such that it may have some serious adverse effects on the economy (Taylor, 2010). Systemic risk may be an event that arise suddenly and unexpectedly, or it could be built up over time due to inappropriate policy responses (Taylor, 2010). Real economic effect of systemic risk mainly emerges from disruption to payment systems, credit flows and through destructions of asset values (Taylor, 2010) [11].

To prevent potential problems from materializing a financial stability framework requires a continuous process of monitoring and information gathering on macroeconomic conditions, financial markets, financial institutes, and financial infrastructure (Silva et al., 2017) [12]. As, the real economy is linked to the financial system (Schinasi, 2011). The process will be more useful and successful if there is a linkage between economic and financial dimensions. The framework involves a continuous process of gathering information, monitoring and assessment (Silva et al., 2017). The process requires a comprehensive and analytical approach. There is a need to develop measurement technique for detecting growing imbalances and calibrating risk and vulnerabilities to keep up to par with important monitoring phases (Silva et al., 2017). The approach also involves the process of supervision, surveillance, and regulation of financial and economic actors. Supervisory processes could be enhanced through the knowledge about the economy's position in the business and credit cycle and the overall performance of markets. The reason for this is that the macro economy and the market provide the background to which performance of individual institutes should be assessed. Finally, the purpose of information

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chișinău, Moldova

gathering is to assess if the financial system is performing its main functions well enough to be within the corridor of financial stability (Silva et al., 2017).

According to Blejer (2006) [13] financial stability is essential for economic growth because it provides a stable and predictable environment for investment, innovation, and entrepreneurship. A stable financial system helps to reduce uncertainty and risk, which encourages businesses to invest in new projects, creates jobs, and promotes economic growth. In addition, financial stability helps to maintain confidence in the financial system, which is essential for the effective functioning of financial intermediation.

Glocker (2021) [14] postulate that financial instability can result in a credit crunch, a decrease in investment, and a decline in economic activity. For example, financial crises can lead to a decrease in lending, a rise in non-performing loans, and a loss of confidence in the financial system, which can lead to a recession and long-term economic damage. Therefore, it is crucial for policymakers to ensure financial stability in developing countries with large financial sectors. This may include measures such as strengthening prudential regulation, improving risk management practices, and promoting transparency and accountability in the financial sector. Ben Ali, Intissar, and Zeitun (2018) [15] supports the existence of a stabilizing effect on concentration on financial stability for developing countries. These countries should also prioritize building resilient financial systems that can withstand shocks and prevent financial crises.

Schoenmaker (2011) [16] postulates that when a country's financial system become increasingly integrated the domestic policies become less effective. This means that high exposures of the developing country's financial system to global financial institutions and markets have the potential to inject financial instability. Therefore, financial stability is a key prerequisite for sustainable and inclusive economic growth in developing countries with large financial sectors. According to Shaw (1973) [17] a poorly regulated financial system can be prone to instability and financial crises, which can have negative effects on economic growth. In addition, a large financial sector can create incentives for excessive risk-taking and speculative investments, which can lead to financial instability and macroeconomic imbalances.

Understanding the connection between financial stability and economic growth can be justified by the semi-endogenous growth model. Both financial stability and economic growth are endogenous factors that are sensitive to exogenous factors. By including exogenous elements, the model provides a more comprehensive framework that captures the interaction between endogenous and exogenous factors in driving growth (Jones, 2005) [18]. By focusing on these factors, the model offers insights into how policies and investments can promote economic growth (Barcenilla-Visús et al., 2014) [19]. Therefore, it is important to utilize an empirical model that takes into account both endogenous and exogenous factors.

METHODOLOGY AND DATA

Our point of departure is from the Solow growth model which we utilize to understand the sources of economic growth in the long run. This is a vanilla framework the help macroeconomics scholars identify causes of growth and their process. The Solow model, also known as the neoclassical growth model, is one of the most widely used frameworks for understanding economic growth. It was developed by Robert Solow in the 1950s and 1960s and has been influential in shaping the field of macroeconomics. Economists continue to debate and refine growth frameworks, seeking to improve our

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chișinău, Moldova

understanding of economic growth and inform policy decisions. Therefore, we use this framework to include the financial stability variable as a source of growth not addressed by the basic Solow model.

According to Cooray (2009) [20] the inclusion of financial factors allows the financial augmented Solow model to explore how changes in financial conditions, such as improvements in financial markets and institutions, can affect economic growth. It recognizes that financial factors can amplify or dampen the effects of capital accumulation and technological progress on economic growth.

To show the importance of financial factors in the development of growth, Atje and Jovanovic (1993) was the first to explicitly add the financial variable to the initial Solow model as described by *Equation 1*. Thereafter, other scholars utilized the financial augmented Solow model (Cooray, 2009, 2010; Haibo, Manu, and Somuah, 2023) [21].

$$Y(t) = K(t)^{\alpha}[A(t)L(t)]^{1-\alpha}\ , \qquad 0 < \alpha < 1 \tag{1}$$

$$Y(t) = K(t)^{\alpha}H(t)^{\beta}[A(t)L(t)]^{1-\alpha-\beta}\ , \qquad 0 < \alpha, \beta < 1, \qquad \alpha + \beta < 1 \tag{2}$$

$$Y(t) = F(t)^{\alpha}K(t)^{\beta}H(t)^{\gamma}[A(t)L(t)]^{1-\alpha-\beta-\gamma}, 0 < \alpha, \beta, \gamma < 1, \qquad \alpha + \beta + \gamma < 1 \tag{3}$$

, where Y is economic growth, F is financial stability, K is capital, H is human capital, A is the level of technology, L is the labour force, α is the elasticity of economic growth with respect to financial capital, β is the elasticity of economic growth with respect to physical capital, and γ is the elasticity of economic growth with respect to human capital. *Equation 3* culminates with three forms of capital: financial, physical, and human capital.

The financial augmented Solow model enables us to study of how financial crises and disruptions can impact long-term growth. It captures the negative effects of financial crises which can have lasting consequences for economic performance. By incorporating financial factors, the model enhances our understanding of the relationship between financial stability and sustained growth.

We therefore utilize the panel data econometrics to study the effect of financial stability on economic growth. All the variables in the model have data availability and making our panel balanced. To conduct a panel data analysis of the effect of financial stability on economic growth we applied necessary panel data steps as scientifically demonstrated by Angrist and Pischke (2009) [22]. Firstly, we identified seven developing countries with large financial sectors. Secondly, we collect data on financial stability, economic growth, and control variables. Thirdly, we utilize a linear panel data model, the random effects model. According to the theoretical and empirical literature we estimate *Equation 4*, which reflects the random effect model.

$$GDP_{i,t} = \sum_{i=1}^{n} \beta_1 F_{i,t} + \sum_{I=1}^{n} \beta_2 X_{i,t} + \alpha_i + \varepsilon_{i,t} \tag{4}$$

, where $GDP_{i,t}$ is the real GDP growth for country i at time t, $F_{i,t}$ is the vector of financial stability variables, $X_{i,t}$ is the vector of control variables, α_i is the country-specific intercept that captures the unobserved heterogeneity, and $\varepsilon_{i,t}$ is the error term. According to

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chișinău, Moldova

Hausman and Taylor (1981) [23] α_i is the individual-specific intercept that is randomly distributed across individuals in the random effects model. According to Joshi and Wooldridge (2019) [24] the random effects model assumes that the coefficients of the independent variables are the same for all countries but allows for individual-specific intercepts that are randomly distributed.

Table 1 presents a list of variables for the financial stability and economic growth analysis. The main dependent variable is the real GDP growth rate. The main independent variables of interest are the Bank capital to total assets and Bank regulatory capital to risk-weighted assets which serve as proxies for financial stability. We control for the effect of recent major financial crises and include them in the model.

Table 1. Variables

Code	***Variable description***
Dependent variable: Economic growth	
gdp	Real GDP growth (annual %)
Independent variable: Financial Stability	
bcap	Bank capital to total assets (%)
breg	Bank regulatory capital to risk-weighted assets (%)
Independent variable: Control variables	
tro	Trade Openness, % of GDP
caf	Fixed capital formation, % of GDP
labgr	Total labour force, % change year-on-year
mix	Monetary policy independence index
y2001	Year dummy, 2001 Dot.com bubble burst, 1=Crisis, 0=No crisis
y2008	Year dummy, 2008 Global financial crisis, 1=Crisis, 0=No crisis
Covid	Covid-19 dummy, 1=Crisis, 0=No crisis

Source: Compiled by the author. Note: Data collected from Fitch Connect, World Bank, KAOPEN, Penn World Table, and author's own construct of dummy variables.

The 2001 Dot-com bubble burst was a major economic event that had a significant impact on economic growth in the United States and around the world. The Dot-com bubble was a period of rapid growth in the technology sector, fuelled by the growth of the internet and the proliferation of technology start-ups. According to Wheale and Amin (2003) [25] the bubble was characterized by a frenzy of speculative investment in internet-based companies, many of which had little or no revenue and were not profitable. As the bubble grew, investors became increasingly concerned about the underlying value of these companies. However, this was followed by a sharp decline in the value of technology stocks, which began in March 2000 and continued for more than a year, leading to the Dot-com bubble burst in 2001.

The 2008 Global financial crisis had a significant and far-reaching impact on economic growth in the United States and around the world. The crisis was triggered by the collapse of the U.S. housing market, which had been fuelled by a speculative bubble in the housing sector. According to Afonso and Blanco-Arana (2022) [26] when the bubble burst, it led to a widespread collapse of the housing market and a sharp decline in the value of mortgage-backed securities and other financial instruments that were tied to the housing

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chişinău, Moldova

market. This led to a major financial crisis, as banks and other financial institutions faced large losses on their investments in these securities.

Many developing countries with large financial sectors are closely tied to the global economy. The covid-19 pandemic led to a global economic downturn, affecting international trade, investment, and financial markets. The financial sectors in these countries, particularly those heavily reliant on international capital flows, experienced significant volatility. Capital flight and abrupt changes in investor sentiment contributed to financial instability (Calderon and Kubota, 2022) [27].

FINDINGS

This section provides comprehesive analysis of the efficacy of financial stabilty on economic growth in developing countries with large financial sectors. We provide an analysis of the correlations between variables and the culminates with the panel data regression results utilizing the random-effects model.

Table 2 depicts the correlation matrix of all the variables for this study. These correlations provides sentiments into what we can expect from the efficacy. We find that there is a negative and weak correlation between financial stability [*bcap and breg*] and economic growth [*gdpgr*] from 1996 to 2022. The financial stability indicators, *bcap* and *breg*, have a positive and strong correlation. While financial stability and economic growth are weakly correlated, other unobserved factors may be having an influence on this nexus. This reflects the complexity of the relationship between financial stability and economic growth. We also find that the 2001 [*y2001*] and 2008 [*y2008*] global financial crisis is negatively associated with both financial stability and economic growth. The *covid-19* pandemic [*covid*] is also negatively associated with economic growth.

Table 2. Correlation matrix

	gdpgr	*bcap*	*breg*	*tro*	*caf*	*labgr*	*mix*	*y2001*	*y2008*	*covid*
gdpgr	1.00									
bcap	-0.21	1.00								
breg	-0.20	0.82	1.00							
tro	0.12	-0.10	-0.03	1.00						
caf	0.47	0.00	-0.05	0.02	1.00					
labgr	0.58	-0.15	-0.04	0.03	0.12	1.00				
mix	0.16	0.07	0.01	-0.21	0.24	-0.15	1.00			
y2001	-0.06	-0.04	-0.06	-0.10	-0.11	-0.16	0.10	1.00		
y2008	-0.03	-0.16	-0.06	0.06	0.01	0.13	-0.05	-0.02	1.00	
covid	-0.49	0.24	0.23	-0.01	-0.04	-0.25	-0.23	-0.03	-0.09	1.00

Source: Authors' own computation

Table 3 provides panel data results from the random-effects model. Model 1 captures financial stability as represented by the Bank capital to total assets [*bcap*]. Model 2 captures financial stability as represnted by the Bank regulatory capital to risk-weighted assets [*breg*]. We find that financial stability has a negative and highly significantly effect on economic growth at 1% level. The Bank capital to total assets reduced real GDP growth by an estimated 0.233. The Bank regulatory capital to risk-weighted assets reduced real GDP growth by an estimated 0.203. This study utilizes a parsimonious model that controls for the financial crises and the covid-19 pandemic. The 2008 global finacial crisis had a

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chișinău, Moldova

negative effect in the developing countries with large financial sectors but the efficacy is not significant. In contrast, the 2001 and 2008 global finanical crisis had a negative and significant effect on economic growth. Covid-19 pandemic had a negative effect and highly signficant effect on economic growth. The remaining control variables [*tro, caf, labgr, mix*] have a positive and highly significant effect on real GDP growth. Developing countries with large financial sectors are exposed to investment inflows and outflows of international financial institutions and markets. These gives rise to financial stability efforts that hampers growth. The general expectation is that financial stability should contribute postively to econmic growth.

Table 3. Random-effects regression

Variables	**Model 1**	**Model 2**
bcap	-0.233***	
	(0.0846)	
breg		-0.203***
		(0.0270)
tro	0.00845***	0.00958***
	(0.00297)	(0.00365)
caf	0.229***	0.221***
	(0.0259)	(0.0385)
labgr	0.125***	0.148***
	(0.0227)	(0.0232)
mix	0.234***	0.266***
	(0.205)	(0.227)
y2001	-0.083**	-0.080*
	(0.776)	(0.021)
y2008	-0.697*	-0.808*
	(0.880)	(0.042)
covid	-0.623***	-0.458***
	(0.674)	(0.795)
Constant	-0.491***	-0.476***
	(0.376)	(0.156)
R-squared	0.5307	0.5935
Observations	162	162
Number of countries	6	6

Source: Authors' own computation. Note: Robust standard errors in parentheses,
**** p<0.01, ** p<0.05, * p<0.1*

This study postulates that the economic growth of developing countries with large financial sectors has not been resilient enough to curb the costs from the financial system. The financial institutions and markets in most these countries are more volatile than developed countries. Therefore, these countries should enact stronger domestic financial structures. They should also increase the resilience of their financial institutions and markets through robust domestic and regulatory capital to effectively mitigate systemic risk. The negative efficacy of financial stability on economic growth may also mean that the financial stability has not achieved inclusive economic growth in these countries.

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chișinău, Moldova

CONCLUSIONS

Financial stability has become a metric that policymakers monitors drastically, especially after the 2008 global financial crises. From the literature, we learn that a positive and robust domestic and international financial system is desired. We examined if financial stability can partially serve as a transmission mechanism to economic growth. Financial stability is a finanical variable that can be added to the financial sector augmented Solow growth model. This study examine the efficacy of financial stability on economic growth by grouping developing countries with large financial sectors from 2006 to 2022. The random-effects model from panel data methodology is an empirical method utilized to obtain the efficacy. From the sample period, financial stability is negatively associated with economic growth. Most importantly, the study find that financial stability is significantly causal and has a negative effect on economic growth. Future research can examine how moderating factors influence the efficacy of financial stability on economic growth in developing countries with large financial sectors.

BIBLIOGRAPHY

1. BARROSO, J. B. R., NECHIO, F. *Financial market development, monetary policy and financial stability in Brazil* [online]. BIS Papers No 113., 2020 [viewed 12 September 2023]. Availble from: <https://www.bis.org/publ/bppdf/bispap113_d.pdf>.
2. KUMAR, S., PRABHEESH, K.P., BASHAR, O. Examining the effectiveness of macroprudential policy in India. *Economic Analysis and Policy*. 2022, vol. 75, 91-113. ISSN 2204-2296.
3. MACHDAR, N. M. Financial inclusion, financial stability and sustainability in the banking sector: the case of Indonesia. *International Journal of Economics and Business Administration* [online]. 2020, vol. 8(1), 193-202 [viewed 24 August 2023]. Available from: <https://www.um.edu.mt/library/oar/handle/123456789/54174>.
4. MISHI, S., KHUMALO, S.A. Bank stability in South Africa: what matters? *Banks and Bank Systems*. 2019, vol. 14(1), 122-136. ISSN 1991-7074.
5. KOONG, S. S., LAW, S. H., IBRAHIM, M. H. Credit expansion and financial stability in Malaysia. Economic Modelling. 2017, vol. 61, 339-350. ISSN 0264-9993.
6. GAMBACORTA, L., MURCIA, A. The impact of macroprudential policies in Latin America: an empirical analysis using credit registry data. *Journal of Financial Intermediation*. 2019, vol. 42, 100-828. ISSN 1096-0473.
7. SARB. *Financial Stability Review* [online]. South Africa: South African Reserve Bank, 2015 [viewed 11 August 2023]. Available from: <https://www.resbank.co.za/en/home/publications/publication-detail-pages/reviews/finstab-review/2015/6938>.
8. SCHINASI, G.J. Defining Financial Stability and Establishing a Framework to Safeguard It. In: Alfaro, R., ed. *Central Banking, Analysis, and Economic Policies*: *Financial Stability, Monetary Policy, and Central Banking*. Central Bank of Chile, 2011, vol. 1(15), pp. 29-62. Available from: <https://www.researchgate.net/publication/254398542_Defining_Financial_Stability_and_Establishing_a_Framework_to_Safeguard_It#fullTextFileContent>.
9. PEUKERT, H. The Financial Crisis: Origins and Remedies in a Critical Institutionalist Perspective. *Journal of Economic Issues*. 2010, vol. 44(3), 830-38. ISSN 0021-3624.

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chişinău, Moldova

10. ALLEN, W. A., WOOD, G. Defining and achieving financial stability. *Journal of Financial Stability*. 2006, vol. 2(2), 152-172. ISSN 1878-0962.
11. TAYLOR, J.B. Defining Systemic Risk operationally. In: Scott, K. E., Shultz, G. P., & Taylor, J. B., ed. *Ending Government Bailouts as We Know Them: Chapter 4*. Hoover Institution: Stanford University, 2010, pp. 33-57. Available from: <https://web.stanford.edu/~johntayl/Defining%20Systemic%20Risk%20Operationally%20Revised.pdf>.
12. SILVA, W., KIMURA, H., SOBREIRO, V. A. An analysis of the literature on systemic financial risk: A survey. *Journal of Financial Stability*. 2017, vol. 28, 91-114. ISSN 1572-3089.
13. BLEJER, M. I. Economic growth and the stability and efficiency of the financial sector. *Journal of Banking & Finance*. 2006, vol. 30(12), 3429-3432. ISSN 1872-6372.
14. GLOCKER, C. (2021). Reserve requirements and financial stability. *Journal of International Financial Markets, Institutions and Money*. 2021, vol. 71, 101-286. ISSN 1873-0612.
15. BEN ALI, M. S., INTISSAR, T., ZEITUN, R. Banking Concentration and Financial Stability. New Evidence from Developed and Developing Countries. *Eastern Economic Journal*. 2018, 44(1), 117-134. ISSN 1939-4632.
16. SCHOENMAKER, D. The financial trilemma. *Economics Letters*. 2011, vol. 111(1), 57-59. ISSN 0165-1765.
17. SHAW, E. S. *Financial deepening in economic development*. Oxford University Press, 1973. ISBN 0195016327.
18. JONES, C. Chapter 16 – Growth and Ideas. In: Aghion, P., Durlauf, S., ed. *Handbook of Economic Growth*. 2005, vol. 1(B), pp. 1063-1111. Avalable from: <https://www.sciencedirect.com/science/article/abs/pii/S1574068405010166>.
19. BARCENILLA-VISÚS, S., LÓPEZ-PUEYO, C., SANAÚ-VILLARROYA, J. Semi-Endogenous versus Fully Endogenous Growth Theory: A sectoral approach. *Journal of Applied Economics*. 2014, vol. 17(1), 1-30. ISSN 1514-0326.
20. COORAY, A. The Financial Sector and Economic Growth. *Economic Record.* 2009, vol. 85, 10-21. ISSN 1475-4932.
21. COORAY, A. Do stock markets lead to economic growth? *Journal of Policy Modeling*. 2010, vol. 32(4), 448-460. ISSN 1873-8060.
22. ANGRIST, J. D., PISCHKE, J. S. *Mostly harmless econometrics: an empiricist's companion*. Princeton: Princeton University Press, 2009. ISBN 978-0-691-12034-8.
23. HAUSMAN, J. A., TAYLOR, W. E. Panel Data and Unobservable Individual Effects. *Econometrica*. 1981, vol. 49(6), 1377-1398. ISSN 1468-0262.
24. JOSHI, R., WOOLDRIDGE, J. M. Correlated Random Effects Models with Endogenous Explanatory Variables and Unbalanced Panels. *Annals of Economics and Statistics*. 2019, vol. 134, 243-268. ISSN 2115-4430.
25. WHEALE, P. R., AMIN, L. H. Bursting the dot.com "Bubble": A Case Study in Investor Behaviour. *Technology Analysis & Strategic Management*. 2003, vol. 15(1), 117-136. ISSN 0953-7325.

DOI: https://doi.org/10.53486/escst2023.13
International Conference, December 07-08, 2023, Chișinău, Moldova

26. AFONSO, A., BLANCO-ARANA, M.C. Financial and economic development in the context of the global 2008-09 financial crisis. *International Economics*. 2022, vol. 169, 30-42. ISSN 2542-6869.
27. CALDERON, C., & KUBOTA, M. *Exploring the Growth Effects of Covid-19 across Developing Countries* [online]. World Bank: Policy Research Working Papers, 2022 [viewed 28 September 2023]. Available from: <https://doi.org/10.1596/1813-9450-9889>.
28. HAIBO, C., MANU, E. K., SOMUAH, M. Examining Finance-Growth Nexus: Empirical Evidence From the Sub-Regional Economies of Africa. *SAGE Open.* 2023, vol. 13(1), 1-18. ISSN 2158-2440.
29. GRIFFITH-JONES, S. Achieving Financial Stability and Growth in Africa. In: Arestis, P., Sawyer, M., ed. *Financial Liberalisation: International Papers in Political Economy*. Palgrave Macmillan: Cham, 2016, 133-175. ISSN 2634-4955.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.14
International Conference, December 07-08, 2023, Chişinău, Moldova

SMALL AND MEDIUM ENTREPRENEURSHIP: ROLE IN ECONOMIC SECURITY

Irene MALGINA

PhD, Associate Professor,
Academy of Public Administration
under the President of the Republic of Belarus, Belarus,
ORCID 0000-0002-7516-8911
E-mail:irina_malgina@list.ru

Abstract: *The article is devoted to the role of small and medium entrepreneurship (SME) in economic security. In the introduction, the author determined that there are different approaches to understanding economic security and the role of SME in it. The purpose of this work is to determine the role of SME in economic security based on the analysis of various documents. In the main part, the author reveals the functions of SME and the goals in relation to them in the national national security strategies of various countries. It was determined that the national security strategies of various countries usually included an element of SME. The author has identified several main national security strategies of various countries. An analysis was made of the levels of economic security and state economic policy for the formation of the SME space. An analysis of the main strategic documents in the field of national security and development of SME in the Republic of Belarus revealed their certain synchronization at the macro level. An analysis of the main directions or really existing challenges and threats to the national security and economic security of the Republic of Belarus from the perspective of SME showed that in most cases the participation of SME is very possible. In conclusion, it is noted that the role of SME in economic, technological, information and other types of security is obvious. Conceptual documents in the field of national security and SME development in the Republic of Belarus pursue the same goals. In this regard, in the context of ensuring economic security, the task of increasing the efficiency of state support for SME is being updated based on harmonizing approaches to the development of its conceptual framework and assessment methodology aimed at leveling internal and external threats to economic security.*

Keywords: *economic security, small and medium entrepreneurship, sustainability, competitiveness*.

UDC: *334.72:339.137.2*

JEL Classification: *010, 038.*

INTRODUCTION

Scientists identify several approaches to the study of economic security. The most frequently used concepts are “competitiveness” and “sustainability”. There are “development” and “sustainability”, which are also the main ones when characterizing the security of entrepreneurship. There are also three groups of approaches to determining national economic security, including “sustainability” (national economy, socio-economic development, economic system, etc.) [1]. It is ensuring the competitiveness and sustainability of the socio-economic system that is the function of SMEs at the state level. In turn, Lithuanian scientists distinguish a macroeconomic approach (Russian school; approach developed by Professor L. Briguglio) and an individual approach (International Labor Organization (ILO), American school). In this case, the experience of the ILO is interesting, which includes analysis of the macro, meso and micro levels and which is also partly related to the state and development of SME [2]. At the meso level, there is a survey of flexibility and labor safety at the enterprise (various types of flexibility - organizational; numerical; functional; working time; wages; labor force, as well as the role of labor legislation, gender preferences, existing mechanisms of labor relations). The micro level

DOI: https://doi.org/10.53486/escst2023.14
International Conference, December 07-08, 2023, Chișinău, Moldova

includes surveys of people's safety (socio-economic status of the respondent and his family; popular ideas about insecurity and safety; sources of socio-economic instability for different socio-demographic groups; coping mechanisms, etc.). At the same time, the American Approach Economic Security Index adopts a general, although often implicit, definition of economic security: the degree to which people are protected from hardships that cause economic losses [3].

PAPER BODY

SME is the most important element of a market economy, without which neither the state nor society can fully develop, without which a competitive environment cannot be formed, a balanced production structure cannot be achieved, social stability can be ensured and the country's innovative potential can be fully used [4].

We can highlight the following individual functions of SME and goals in relation to them in the national security strategies of foreign countries - support for entrepreneurs; formation of a qualified workforce; formation of high added value; regional development; improving the economic system for future generations; internationalization of entrepreneurs; participation in the formation of a national brand; security of financial infrastructures and services; achieving a balance between the needs to improve the quality of life, economic and social well-being and the requirements to preserve the environment as natural resources (Table 1).

Table 1. Functions of small and medium entrepreneurship and goals in relation to them in the national national security strategies of various countries

Country	Document	Year	Role of SME
Poland	National Security Strategy Of The Republic Of Poland	2007	One of the strategic goals was to support Polish entrepreneurs.
Latvia	The National Security Concept	2008	To ensure long-term economic growth, it is very important to be able to use skilled labor, science and innovation in business development when developing projects focused on high-value-added production. Particular attention should be directed to the development of entrepreneurial initiative in the regions of the Republic of Latvia.
Philippines	National Security Policy 2011 –2016	2011	The interest of the national vision of economic solidarity is for Filipinos to become stakeholders in the economy and business enterprises for the purpose of collectively protecting and improving the economic system for themselves and future generations of Filipinos.
Croatia	National Security Strategy	2017	Takes into account the role of business structures in the joint actions of government bodies and local / regional authorities to achieve a balance between the needs for improving the quality of life, economic and social well-being and the requirements for preserving the environment as natural resources.

Source: Ministry of National Defence of Poland https://www.gov.pl/web/national-defence
Ministry of Defence of Latvia https://www.mod.gov.lv
The National Security Council http://www.nsc.gov.ph
National Security Council https://www.uvns.hr/en/legislation/national–security.

DOI: https://doi.org/10.53486/escst2023.14
International Conference, December 07-08, 2023, Chişinău, Moldova

The role of SME in the country's economy is important and is determined by such indicators as the share of SMEs in GDP, GVA, employment, etc. In turn, the SME space contributes to the active development of SME. Based on the theory of public policy in the field of formation of the SME space, the following levels are distinguished: regional level (country), meso level (region), micro level (organization and/or person). At the national and regional levels, the SME space includes elements such as the state, education, financial support, human capital, etc. The task of the state in this area is to develop policies that do not have direct intervention. In this case, the role of the state can be both indirect and direct. The direct one, in particular, lies in the ability to identify SME with high growth potential (which can, for example, actively cooperate with the Ministry of Defense), the indirect one lies, in particular, in the role of the state as an intermediary for SME. There are two government policies regarding the formation of the SME space - traditional and growth-oriented. At the same time, traditional policy will not contribute to strengthening economic security in all its parameters; rather, it will be aimed at neutralizing certain threats, in particular, unemployment. While a growth-oriented policy will help strengthen not only economic, but almost all types of national security, including military. In an effort to build an effective space for SME, the state thereby strengthens economic security at three levels (Table 2).

Table 2. Types of economic security and small and medium entrepreneurship space

Economic security	SME space
National Regional Business entity and/or person	

Source: elaborated by the author

Thus, the levels of economic security correspond to the levels of state economic policy for the formation of the SME space. One of the elements of the SME space is the state, which, in essence, is designed to ensure the effective development of the SME space. Turning to the experience of government policy in the field of formation of the SME space in various countries, the following can be noted. It is advisable to take into account when addressing issues of economic development in accordance with the challenge and/or threat (for example, "the lag in the pace of transition of the economy to advanced technological structures from other states, the degradation of the technological structure of the real sector of the economy" - the Republic of Belarus), which, according to a study by the Kauffman Foundation during 2000 – 2010. Almost all new jobs in the United States were created by fast-growing technology startups. So, in addition to the above and reaffirming the role of SME in military security, the US has a year-long Technology and National Security Fellowship that provides the opportunity for technologists and entrepreneurs to connect with key decision makers at the highest levels of the US government (Department of Defense and Congress USA), to provide advice and new knowledge on issues at a critical juncture in national security.

State regulation of the market model of the economy from the perspective of security interests should not violate self-regulation mechanisms and at the same time create conditions for the effective operation of these mechanisms. One of the mechanisms for self-regulation of SME and the business community of any country is the formation of an SME space. In this context, it should be noted the necessary modernization of "managing the process of reconciling interests and coordinating the efforts of the state and business as

DOI: https://doi.org/10.53486/escst2023.14
International Conference, December 07-08, 2023, Chișinău, Moldova

the main institutions of a market economy" [5]. Analysis of the main strategic documents in the field of national security and development of SME in the Republic of Belarus made it possible to identify their certain synchronization at the macro level (Table 3).

Table 3. Strategic national interests and goals with the participation of small and medium entrepreneurship

National Security Concept of the Republic of Belarus	Strategy for the development of small and medium entrepreneurship "Belarus is a country of successful entrepreneurship" for the period until 2030
sustainable economic development and high competitiveness of the Belarusian economy; achieving a high level and quality of life for citizens	the formation of a dynamically developing SME sector that can significantly improve the structure of the Belarusian economy, increase its competitiveness, ensure effective employment and growth in incomes of the population

Source: elaborated by the author

This table clearly shows the connection between national interests and the goals of SME development. An analysis of the main directions or really existing challenges and threats to the national security and economic security of the Republic of Belarus from the perspective of SME showed that in most cases the participation of SME is very possible.

CONCLUSIONS

All of the above directions fully correspond to the concept of the SME space in terms of solving various problems of state development in socio-economic terms. Thus, the connection between the SME space and economic security is obvious.

In this case, the following statement is true. "Regardless of how we look at national security, there is no question of ignoring the economic vitality of the nation. Without capital there is no business; without business there is no profit; without profit there are no jobs. And without jobs there are no taxes, no military potential… Without jobs, people's quality of life deteriorates to such an extent that society itself may collapse" [6].

The role of SME in economic, technological, information and other types of security is obvious. Conceptual documents in the field of national security and SME development in the Republic of Belarus pursue the same goals. In this regard, in the context of ensuring economic security, the task of increasing the efficiency of state support for SMEs is being updated based on harmonizing approaches to the development of its conceptual framework and assessment methodology aimed at leveling internal and external threats to economic security. In this regard, on the one hand, it is necessary to modernize state support for SME in accordance with modern challenges and threats in the economic sphere, on the other hand, to ensure the maintenance of the state of protection of the SME entity from the negative impact of internal and external threats in accordance with the needs of its free and comprehensive development and based on mandatory requirements established by current legislation.

BIBLIOGRAPHY

1. KOLUPAEV, V. A. Formation of the concept of national economic security in foreign countries. *Belaruskaya Ekonomika: Analiz, Prognoz, Regulirovanie*, 2002, 2-9.

DOI: https://doi.org/10.53486/escst2023.14
International Conference, December 07-08, 2023, Chișinău, Moldova

2. TAMOSIUNIENE, R.; MUNTEANU, C. Current research approaches to economic security. In: *The 1 st International Conference on Business Management, Valencia, Spain*, July 2–3, 2015 / Universitat Politècnica de Valencia, Valencia, p. 135–140.
3. HACKER, Jacob S., et al. Economic insecurity across the American states: New state estimates from the Economic Security Index. *Rockefeller Foundation*, 2012.
4. FEDOROV, V. V. The essence of small and medium-sized businesses and its role in the economy. *Innovation and Investment*, 2018, 5, 345–348.
5. NIKITAEVA, A. Y. *Theory and practice of managing interactions between the state and business: regional aspect*. SFU Publishing House, 2007.
6. RONIS, S. R., et al. (ed.). *Economic Security: Neglected Dimension of National Security* Washington: National Defense University Press Washington, D.C., 2011.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.15
International Conference, December 07-08, 2023, Chişinău, Moldova

CHALLENGES OF DIGITAL PLATFORMS IMPLEMENTATION FOR COOPERATION OF BUSINESS AND TAX AUTHORITIES

Liudmyla CHVERTKO
PhD, Associate Professor,
Pavlo Tychyna Uman State Pedagogical University, Uman, Ukraine,
ORCID 0000-0003-2788-6991
E-mail: chvertko.l@udpu.edu.ua

Illia PUHOLOVKO
PhD student,
Pavlo Tychyna Uman State Pedagogical University, Uman, Ukraine,
ORCID 0009-0006-4720-8759
E-mail: illia.puholovko@gmail.com

Abstract: *Digitalization and transformation to innovative solutions are essential trends in the development of taxation and other areas. In general, the continuous evolution of IT technologies is a crucial factor in digitizing most processes in the modern world. The Main effects and consequences of digitalization are the collection of large amounts of information (big data), which is analyzed by AI and used to make decisions in various areas of economic and social, government, and legislative activities. Today, humanity accumulates as much data as the human brain cannot comprehend and process in a lifetime. The taxation sphere is not an exception, with more and more tools for taxpayers and regulatory authorities now available in digital form. The newest cooperation services between the taxpayer and the government are designed to improve the work of tax authorities and, most importantly, simplify the process of paying taxes, submitting tax returns, and receiving consultations. All of these services have been operating successfully for some time but still need to be improved and expanded. The digital economy is pushing tax authorities to replace traditional models of tax administration with new models that analyze and use big data and electronic tools online to promote effective cooperation between tax authorities worldwide. However, in line with the development of the Ukrainian tax system and the transformation of the taxpayer-state relationship, implementing electronic data transfer components is not always phased, which creates additional risks for businesses.*

Keywords: *SAF-T, accounting system, reporting, tax authorities, tax management, digitalization.*

UDC: *336.22:004.8(477)*

JEL Classification: *H29.*

INTRODUCTION

The digitalization processes and the introduction of cloud-based database storage technologies, online data rooms, bots, AI, etc., require a complete redesign of the financial and tax accounting systems to optimize the management function. It is hard to imagine future business development without the widespread use and improvement of IT technologies based on the extensive use of digital technology and electronic communication with key stakeholders. The tax management systems will also experience significant changes due to the new extensive technological and operational capabilities of business processes, increased share of intellectual labor, increased public control over economic activity, and at the same time, increased types and scale of security-related risks, proper determination of the tax base and treatment of information received.

DOI: https://doi.org/10.53486/escst2023.15
International Conference, December 07-08, 2023, Chișinău, Moldova

PAPER BODY

Many scientists, including O. Adamyk, T. Bochulia, V. Deriy, S. Vasylyshyn, and others, have highlighted the impact of digital technologies on accounting and analytical support as well as the economic security of companies. Professor T. Bochulia considers the information prepared by the accounting system to be the most valuable information resource. Despite its retrospective nature, accounting data is the basis for further analysis of the financial and economic position of the company [1]. Based on research conducted in the context of tax and accounting reporting development under the impact of digital solutions, it is clear that information security is increasingly closely linked to financial security. As a result, to maintain sufficient financial security, it is necessary to ensure protection against information threats.

On the one hand, new IT technologies in accounting and financial reporting ensure high quality of work and, on the other hand, create many threats that lead to unpredictable and even catastrophic consequences for the company. As defined by B. Zasadnyi, information risks include risks resulting from spam, cyber-attacks, financial reporting fraud, malicious misrepresentation of a company's activities via the Internet, illegal access to commercially sensitive information by unauthorized third parties, etc. [2]. Maintaining the privacy of tax and accounting information should prevent unauthorized access to such records of an entity that contain information about its business activities, the amount of employees' remuneration, shareholders, contractors, clients, and business partners.

Currently, European countries are introducing more and more data exchange formats for tax audit and control in an electronic format, i.e., without the usual visits of controllers, inspection of primary documents, and accounting records of taxpayers. This fiscal relations transformation is being implemented by introducing the Standard Audit File for Tax Purposes (SAF-T). Introduced by the OECD in 2005, the Standard Audit File for Tax Purposes (SAF-T) has always been voluntary. Many European countries are now adopting it as a mandatory type of tax data transfer. The Standard Audit File for Tax Purposes (SAF-T) is an XML file (a set of data converted into a special language) created to standardize procedures and expand the possibilities of using data for business control and audit. This file collects all accounting data of companies related to business activities, enabling the processing and analysis of accounting data sets independently of the software used in each company.

A detailed review of the Concept of e-audit Implementation and the Procedure for Submission of Large Taxpayer Documents in Electronic Form indicate that in Ukraine, it is proposed to introduce the submission of the full range of data (all sections) based on the standard SAF-T scheme with additional elements not defined by the standard scheme. In addition, the Draft Law dated 02.11.2021 No. 6255, "On Amendments to the Tax Code of Ukraine on the Implementation of Electronic Audits (e-audit)," was registered in the Parliament, which provides for the submission of SAF-T not only upon request during the audit but also for the conversion of SAF-T into an annual report, the failure to submit which will result in significant penalties.

Even with the standard presentation of SAF-T data, several problems can arise during the transfer and analysis of the information used to generate each report. Whereas structural validation can be easily performed (using the appropriate XML schema), the integrity of the data can be challenging to maintain due to data entry errors, changes in the data over time, or software errors that are difficult to detect during the generation and conversion of large amounts of data. In addition, the analysis of historical data becomes a

DOI: https://doi.org/10.53486/escst2023.15
International Conference, December 07-08, 2023, Chișinău, Moldova

challenge when you use only SAF-T files, as each file contains separate data on customers, goods, taxes, and primary documents for a certain period. When applying analytical procedures, the relationship and evolution of the data can be threatened because we have a limited picture of the organization at a particular point in time [3].

Another problem that needs to be resolved is a contradiction between the industry-specific legislation and the requirements for submitting SAF-T in Ukraine, particularly regarding information disclosure. By Procedure No. 1393, it is obligatory to provide detailed accounting entries of the entity (in the subsection "Accounting Entries") for each specific transaction, including the type of transaction, the amount, the information on the unique taxpayer ID (legal entity or individual if the transaction is conducted with a contractor), as well as accounting entries related to this transaction and other information provided for in this part of the SAF-T. In cases of reporting such information by banks, which are mainly large taxpayers, the issue of banking secrecy remains open. For banks, transactions on customer accounts are accounting transactions that correspond to income/expense accounts or other balance sheet accounts.

The primary purpose of information security is to ensure that a company operates stably and efficiently now and has a high potential for development in the future. Today, much of the information circulating within companies is classified as confidential, as it determines their business and development. To effectively exchange confidential information, in addition to implementing electronic systems, it is necessary to have a high level of organizational and technical information security. Therefore, the technology for processing and transferring accounting information and software should minimize the risks associated with the loss of records, incomplete or incorrect data input into the accounting system, improper control, and a chain of errors that may lead to false analysis results.

It is also essential to understand the existing risks associated with unfair business practices when transferring large amounts of accounting data on business activities. For example, according to international rules, there are three types of unfair business practices:

- all actions that lead to the commercial activities of one company being presented to the consumer as the commercial activities of another;
- discrediting the commercial activities of a competitor by disseminating false information;
- the illegal use of marks that may mislead the consumer in the course of commercial activities.

According to foreign statistics, some companies specialize in industrial spying and profit from it, using professional and often illegal methods of obtaining information [4].

It should be noted that despite the full-scale war, the digitalization of cooperation with the government in Ukraine has made significant progress, for example, access to information through the Diia portal, transformation of the State Statistics Service portal, non-stop work of the Electronic Taxpayer's Office, which allows to obtain a wide range of information about the presence of one's counterparty in the list of taxpayers who meet the risk criteria of the taxpayer (date of inclusion in/exclusion from such a list, risk criterion), submission of tax and financial statements, etc. However, introducing ambitious tax audit reform projects requires close cooperation between the tax authorities and businesses. Without such cooperation, several risks may arise that will have a negative impact on both sides of the relationship.

DOI: https://doi.org/10.53486/escst2023.15
International Conference, December 07-08, 2023, Chişinău, Moldova

CONCLUSIONS

A company's potential success in digitalization-driven changes will depend on changing the accounting system. This system is the main element of modifications to business processes and the primary source of information support for all stakeholder communities related to the economic security of business units.

One of the sources of business security risks in the information sphere is the continuous increase in the complexity of information systems and data exchange channels. These threats can be expressed as intentional and unintentional errors, failures and disruptions of hardware and software, and harmful activity of criminal groups and criminal elements. As a result, the concentration of a large amount of internal confidential information (which may also be reflected in accounting data when transferring data in the form of SAF-T files) could pose an external threat to the company's commercial activities.

Achieving the optimal level of company accounting systems stability and security, which prevents information loss, illegal sharing, and protection in the best interests of the company owners, is possible only if a systematic scientific approach is taken to developing strategies and tactics for digitalized cyber security. Early development of measures to mitigate digitalization risks is the key to economic security and competitive development of enterprises, as well as the success of the national economy.

BIBLIOGRAPHY

1. BOCHULIA, T. Oblikova skladova informatsiinoho potentsialu pidpryiemstva. *Biuleten Mizhnarodnoho Nobelivskoho ekonomichnoho forumu*, 2013, 1(6) 35–42. ISSN 2074-5370 [viewed 18 December 2023]. Available from: < https://econforum.duan.edu.ua/images/PDF/2013/6.pdf>
2. ZASADNYI, B. Ryzyky systemy bukhhalterskoho obliku v umovakh zastosuvannia MSFZ. *Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu*. *Seriia: Mizhnarodni ekonomichni vidnosyny ta svitove hospodarstvo*. 2017, vol. 14 (1), 111-115. ISSN 2413-9971 [viewed 18 December 2023]. Available from: <https://dspace.uzhnu.edu.ua/jspui/handle/lib/16738>.
3. OLIVEIRA, B. [et al.]. Improving Organizational Decision Making Using a SAF-T based Business Intelligence System. *CAPSI 2020 Proceedings* [online], 2020, 34. [viewed 18 December 2023]. Available from: <https://aisel.aisnet.org/capsi2020/342020>.
4. HORNYK, V., KRAVChENKO, S., Mekhanizmy zabezpechennia informatsiinoi bezpeky pidpryiemnytskoi diialnosti yak skladnyka informatsiinoi bezpeky derzhavy. *Scientific Notes of Taurida V.I. Vernadsky University, series "Public Administration*", 2020, 206-212. [viewed 18 December 2023]. Available from: <http://www.pubadm.vernadskyjournals.in.ua/journals/2020/2_2020/36.pdf>
5. VASYLISHYN, S. Improving the levers of digitalization risks management of economic security and formation of cybersecurity of the accounting system. *Herald of Economics* [online], 2021. vol. 1(99), 97-110, [viewed 18 December 2023]. Available from: <http://visnykj.wunu.edu.ua/index.php/htneu/article/view/1206>.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

BUILDING A DIGITAL ROADMAP FOR ENTERPRISES

Mihaela-Sorina CONSTANTINESCU

PhD student,
Bucharest University of Economic Studies,
Economic Cybernetics and Statistics Doctoral School, Romania,
ORCID 0000-0001-7585-8851
E-mail: constantinescu.sorina@gmail.com

Mihai Daniel ROMAN

PhD, Professor,
Bucharest University of Economic Studies, Romania,
ORCID 0000-0002-3859-7629
E-mail: mihai.roman@ase.ro

Abstract:*More and more organizations nowadays are embedding digitalization into their core values. Recent studies have shown that the concept of digitalization is a game changer for all the agents within the value chains of worldwide economy and it is not only creating value but might disrupt it also unless implemented in a structured way. This paper presents an insight into industrial operations and recommends a method of building a digital roadmap, from defining the general scope, identifying the digital strategy relevant to the respective business model while considering specific business opportunities and needs to forming the foundations of the digital component such as relevant technologies and solutions or defining use-cases to enablement of those into the organization all while building up specific digital competencies and capabilities. A more digital leadership becomes a must to enable this new technology operating model and for that roles and responsibilities within organizations are now focused on facilitating collaboration in the industry ecosystem and enabling rapid and agile data architecture whilst ensuring cybersecurity as well. This paper offers insights into industrial operations and proposes a method for developing a digital roadmap. It covers defining the scope, identifying relevant digital strategies, considering specific business opportunities and needs, and establishing the foundations of digital components. The importance of digital leadership, cybersecurity measures, and fostering digital competencies are highlighted. The paper aims to guide organizations through the digital journey with the goal of bringing enterprises closer to the optimal performance mode while adjusting to the fast-paced metaverse era.*

Keywords: *Digitalization, Digital Transformation, Digital Roadmap, Industry 4.0, Digital Competencies, Agile Data Architecture, Digital Leadership, Cybersecurity Measures.*

UDC: *338.26:004.8*

JEL Classification: *O33, O32, L86, M15, L20, M10.*

INTRODUCTION

This paper serves as a foundation to provide a structured approach to building an effective digital roadmap for enterprises and its importance in today's economical landscape. In the contemporary business landscape, organizations are recognizing the need to integrate digitalization into their core values. Recent studies underscore the transformative impact of digitalization on global value chains. This paper delves into the realm of industrial operations, offering insights into the importance of digital transformation. It proposes a method for building and executing a digital roadmap that encompasses defining the general scope, identifying relevant digital strategies, considering specific business opportunities and needs, and establishing the foundations of digital components.

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

Digital transformation stands as a globally significant topic, impacting organizations across various sectors by reshaping customer relationships, internal processes, and overall value creation. A pivotal concern for stakeholders navigating this transformation is the formulation of a clear vision and roadmap that sets the direction for the future.

A recent study provides an extensive literature review on digital transformation, focusing on defining a comprehensive digital transformation roadmap for companies. It discusses various approaches, methodologies, and steps identified in academic and industry papers, categorizing the key phases of digital transformation [1]. The study emphasizes the need for a multi-dimensional evaluation, strategic planning, and the implementation of digital transformation processes. It highlights the diverse perspectives and trends in digital transformation literature, offering insights into the essential components and stages of digital transformation for businesses.

The strategic significance of digital transformation becomes evident, emphasizing its multidimensional nature. The primary goal is to develop effective strategies for digitizing a business and to enhance our understanding by incorporating existing roadmaps, thereby contributing to the development of alternative approaches to digital transformation.

This paper seeks to assist companies in their digital transformation journey by initiating a thoughtful exploration of digital transformation processes while also incorporating recent literature review. The methodology used in the paper involves presenting the framework of digitalization supported by relevant scientific and white papers, as well as capturing the essence of the digitalization concept for organizations. Another objective is to document the necessary steps for a company to execute on its digital journey and categorize them into phases that can be leveraged to plan a strong digital transformation process. The paper will also explore the application of a digital roadmap and concludes with further research suggestions.

NAVIGATING DIGITAL TRANSFORMATION: INSIGHTS FROM LITERATURE

Digitalization has transcended being a mere industry buzzword; it now stands as a pivotal force reshaping the contours of the global economy. This section explores in detail the profound impact of digitalization on customer relationships, internal processes, and value creation within organizations. The failure to adopt structured digitalization is not just a missed opportunity, but it poses a tangible risk of disruption in an era defined by innovation and technological advancements. Beyond the missed opportunities, there exists a real and immediate risk of disruption to operations and market relevance. A systematic integration of digital technologies is not just a strategic imperative but a proactive journey to navigate the challenges and seize the opportunities presented by the digital era.

Digital transformation, a concept concerning the impact of digital technologies on a company's business model, products, and organizational structures, as defined by Hess et al., stands as a major managerial challenge for organizations in recent decades [2]. This transformation requires a synergy of advanced technology and skilled personnel to unlock its full potential. Recent years have seen a surge in academic interest, especially in information systems, resulting in an increased volume of research exploring various technological and organizational facets of digital transformation. This paper seeks to provide a thematic, descriptive analysis of this domain.

A recent study on digital transformation (Nadkarni and Prügl) offers an in-depth analysis of digital transformation in organizations. It discusses the integration of digital technologies into organizational structures and processes, highlighting the importance of

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

both technological advancements and human-centric factors [3]. This highlights as well the need for effective leadership and strategic planning in implementing digital changes. It also addresses the challenges posed by rapid technological evolution, such as workforce skill adaptation and cultural shifts within organizations. The study points out gaps in current research and suggests areas for future exploration, particularly regarding the role of middle management and the skills gap in digital transformation efforts.

In the current era, information technologies are 'one of the threads from which the fabric of organization is now woven', as highlighted by Zammuto et al. [4]. Digital technologies play a crucial role in driving organizational transformation due to their disruptive and widespread impacts, a concept emphasized by Besson and Rowe [5]. Effective digital transformation demands changes at multiple organizational levels: it involves redefining the core business model (Karimi and Walter) [6], altering resource and capability dynamics (Cha et al.; Yeow et al.) [7]-[8], restructuring processes and organizational structures (Resca et al.) [9], evolving leadership styles (Hansen and Sia 2015; Singh and Hess) [10]-[11], and fostering a strong digital culture (Llopis et al.). This review concentrates specifically on digital transformation at the organizational scale, distinct from individual-level impacts.

Another recent article (Oberländer et al.) addresses the growing need for digital competencies in today's workforce due to rapid digitalization [12]. It notes a significant gap between current and required digital skills, emphasizing the necessity of lifelong learning. The research aims to understand digital competencies at work by reviewing existing literature and conducting interviews with professionals. The study highlights overlapping content among different viewpoints, thereby enhancing professional learning and development of digital skills in the workplace.

A recent study focuses on the importance of digital learning in organizational digital transformation (Sousa and Rocha, 2019) [13]. It examines the skills necessary for this transformation and explores different contexts in which digital learning can occur. The paper analyzes the impacts of digital learning on skill development and its influence on organizational transformation. It also includes an online survey to identify key skills for effective digital transformation, highlighting the roles of artificial intelligence, nanotechnology, robotization, and the Internet of Things. The study contributes to understanding the crucial link between skills development and digital transformation in organizations.

INSIGHT INTO INDUSTRIAL OPERATIONS

Understanding the current state of industrial operations is not just beneficial but fundamental to effective digital transformation. This section goes beyond the surface, exploring specific areas within industrial operations where digitalization can facilitate transformative change. By identifying these areas, organizations can lay the groundwork for a successful digital roadmap that aligns with their overarching objectives.

To build a successful digital roadmap, organizations need a nuanced understanding of industrial operations. This involves a deep dive into specific sectors, such as manufacturing, logistics, and supply chain, to identify pain points and areas ripe for digital innovation.

Recent studies have analyzed key aspects of the implementation of digital transformation in manufacturing, particularly focusing on the Industry 4.0 concept (Issa et al.) [14]. It addresses the challenges faced by companies in adopting Industry 4.0 and proposes a framework based on capability maturity and alignment. The paper elaborates on

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

a step-wise approach for successful implementation, highlighting the importance of integrating technology with organizational strategy and objectives. This framework is demonstrated through a case study, providing insights into practical applications and strategic considerations for businesses embarking on digital transformation. It emphasizes a step-wise implementation strategy that integrates technology and business strategy. This approach is designed to address the challenges of digital transformation in manufacturing by providing a clear framework for companies to effectively integrate Industry 4.0 technologies into their operations. The methodology includes assessing organizational readiness, technology adoption, and strategic alignment to ensure successful transformation. This strategy involves a series of stages, each designed to ensure effective adoption of digital technologies while aligning them with the organization's strategic objectives. The approach includes evaluating organizational readiness, adopting relevant technologies, and ensuring these technologies are strategically aligned with the company's goals. Each stage builds upon the previous one, facilitating a gradual and structured transition into the digital manufacturing landscape.

In the era of digitalization, the adoption of Industry 4.0 principles is paramount for organizations seeking to enhance efficiency, agility, and competitiveness. Industry 4.0 represents the fourth industrial revolution, characterized by the integration of smart technologies into manufacturing and business processes. Therefore, a critical component of digitalization is embracing Industry 4.0 principles. This section discusses how technologies like IoT (Internet of Things), AI (Artificial Intelligence), and RPA (Robotics Process Automation) are driving the next industrial revolution and how organizations can strategically integrate these technologies into their operations.

Internet of Things (IoT) involves connecting devices and systems to the internet to collect and exchange data. Among usages of Internet of Things technology, we can refer to embedding sensors in machinery, equipment, and products for real-time monitoring, predictive maintenance, and supply chain optimization. Some key benefits this new technology is bringing are improved operational efficiency, reduced downtime, and enhanced decision-making through data-driven insights.

Artificial Intelligence (AI) encompasses machine learning, natural language processing, and cognitive computing to perform tasks that typically require human intelligence. The application of this technology could consist of implementing AI algorithms for predictive analytics, demand forecasting, and personalized customer experiences. Among the benefits this digital technology is brining are enhanced decision-making, automation of repetitive tasks, and the ability to derive actionable insights from large datasets.

Robotics involves the use of automated machines or robots to perform tasks in various industries. Deploying robots in manufacturing for assembly, packaging, and material handling or collaborative robots (co-bots) working alongside humans are some examples of how robotics could assist the digital journey. This digital technology brings numerous benefits, like increased production efficiency, reduced labor costs, and improved workplace safety.

An interesting aspect that could be part of future research work on the matter is the synergetic effect resulted by integrating these digital technologies. By integrating the technologies, more value can be created during the digital journey.

For example, from a data integration perspective, an organization can establish a robust data infrastructure from seamlessly integrating data from Internet of Things devices,

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

AI systems, and robotic platforms. Furthermore, implementing data analytics tools would then extract meaningful insights and support informed decision-making.

Creating interconnected systems where IoT devices, AI algorithms, and robotic processes communicate and collaborate in real-time could enable a holistic view of operations, facilitating a more agile and responsive organizational structure.

Another opportunity worth exploring is increasing collaboration between humans and machines, particularly in tasks that leverage the strengths of both. Providing training programs to enhance employees' digital skills and adaptability to working alongside advanced technologies.

In order to implement a digital journey governed by Industry 4.0 principles, organizations should start by elaborating a digital strategy. First step recommended is initializing pilot programs to test the feasibility and effectiveness of Industry 4.0 technologies in specific areas of operations. Learning from pilot outcomes to fine-tune strategies before full-scale implementation.

The second element would be embracing an agile approach to technology adoption, allowing for iterative improvements based on continuous feedback. Incorporating lessons learned from Industry 4.0 pioneers and keeping up with emerging technologies.

The third dimension is represented by cybersecurity measures. From an economic security perspective, it is crucial to ensure implementing robust cybersecurity measures to safeguard interconnected systems and sensitive data. As the digital journey is a recent path organizations are stepping on, it is important to address potential vulnerabilities associated with the increased connectivity of devices. This describes a digital paradox: contemporary organizations have the opportunity to leverage new digital connections, tools, and platforms for real-time engagement with customers, suppliers, and partners. However, simultaneously, cybercrime has emerged as a potent counterforce posing a threat to this potential. According to a recent survey executed by an experienced financial technology company supporting over 3,500 organizations globally, the recognition of this issue is on the rise: six out of ten chief executives identify cyber threats and the rapid pace of technological change as primary threats and challenges to their growth. Additionally, around one-third of organizations have fallen victim to economic crime in recent years, underscoring the significant evolution of economic crime. Yet, detection and control programs are struggling to keep pace with this rapid transformation. Furthermore, the financial impact of each fraud case is seeing an upward trend.

The extensive digital transformation can cause disruptions in economies worldwide, presenting organizations with both opportunities and threats. Therefore, just like every other aspect of the newer digital landscape, economic crime is also going digital. The contemporary era of hyper-connectivity provides cybercriminals with entry points to compromise the digital landscape of organizations through diverse means. Potential breaches can manifest in different areas of the digitally evolving economy, ranging from attacks on the Internet of Things, including vehicles and household devices, to mobile and eCommerce services, as well as affecting cloud computing or traditional on-premise Enterprise Resource Planning systems.

Among the challenges for adopting Industry 4.0 principles on the digital journeys, data privacy and security are areas of interest, especially when dealing with vast amounts of sensitive information. This is why it is important that organizations are always complying with regulations and standards to mitigate potential risks and disruptions. From a workforce transformation perspective, another consideration should be given to

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

recognizing the need for reskilling and upskilling the workforce to adapt to new technologies. This would also ensure a smooth transition for employees into roles that complement automated processes. From an investment and return on investment perspective for Industry 4.0 initiatives, a recommendation for organizations is to balance the upfront investment with the long-term benefits in terms of efficiency, productivity, and market competitiveness.

A conclusion for this section is that incorporating Industry 4.0 principles into digital transformation strategies empowers organizations to thrive in the evolving digital landscape. By strategically leveraging newer digital technologies like IoT, AI, and robotics while implementing strong cybersecurity measures, businesses can enhance operational efficiency, drive innovation, and remain competitive in a rapidly changing world. The successful integration of Industry 4.0 requires careful planning, continuous learning, and a commitment to dedication to nurturing a workforce with digital proficiency.

BUILDING A DIGITAL ROADMAP

In the fast-pacing digital landscape, organizations find themselves at crossroads, where strategic decisions in the realm of technology can shape their future trajectory. The relentless pace of change requires a strategic positioning for businesses to not only survive but thrive in this era of digitalization. As we delve into the nuances of Building a Digital Roadmap in this chapter, it is essential to recognize the transformative power that digitalization holds. Digitalization is not merely a technological shift, but it represents a reengineering of how organizations operate, innovate, and create value. To embark on this transformative journey, organizations must not only adapt to change but strategically adopt newer solutions offered by digital technologies.

This chapter unfolds as a strategic guide, indicating the essential components that organizations must master to navigate the complexities of digital transformation successfully - building a digital roadmap. Much more than a technical blueprint, a digital roadmap is a strategic guide that aligns an organization's goals with the vast possibilities offered by digital technologies.

From defining the general scope to nurturing digital competencies, each stage of the roadmap is a piece of the larger puzzle. It represents indeed a journey that involves not just technological integration but a profound understanding of organizational dynamics, market landscapes, and the ever-changing currents of the digital era.

1. Defining the General Scope

Defining the general scope is not just an administrative step, but a strategic alignment of digital initiatives with the broader organizational objectives. This involves a thorough understanding of the business landscape, its unique challenges, and the desired outcomes from digital transformation.

To define the general scope effectively, organizations need to articulate their objectives clearly. This involves a collaborative process, engaging key stakeholders to ensure alignment with overarching business goals. A critical aspect of defining the scope is assessing the organization's current capabilities. This involves evaluating existing technologies, skill sets, and infrastructure to identify strengths and areas that require enhancement.

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

2. Identifying Relevant Digital Strategies

The identification of relevant digital strategies is a pivotal step in crafting a tailored digital roadmap. This involves aligning digital initiatives with the unique business model of the organization, ensuring that each strategy resonates with the core values and objectives.

To identify relevant strategies, organizations must align digital initiatives with their business model. This involves a strategic analysis of how digitalization can complement and enhance existing business practices. Identifying relevant digital strategies also involves a comprehensive risk assessment. Organizations need to anticipate potential challenges and develop mitigation strategies to ensure a smooth implementation process.

3. Considering Business Opportunities and Needs

The strategic assessment of business opportunities and needs is the cornerstone of an effective digital roadmap. This step involves a comprehensive evaluation of areas where digitalization can create value, addressing specific business needs, and fostering a culture of innovation. Organizations must identify opportunities for value creation through digitalization. This involves assessing customer needs, market trends, and emerging technologies to pinpoint areas where digital initiatives can lead to tangible benefits.

In parallel with identifying opportunities, organizations must address specific business needs. This includes streamlining operations, improving efficiency, and responding proactively to market demands through digital solutions.

4. Foundations of Digital Components

In this section, we delve into the technological underpinnings that form the bedrock of a robust digital roadmap. Exploring the selection and implementation of relevant technologies, defining use-cases for organizational enablement, and ensuring seamless integration lay the groundwork for a successful digital journey.

Choosing the right technologies is a critical decision that shapes the success of digital initiatives. This involves a thorough evaluation of available technologies, considering factors such as scalability, compatibility, and alignment with organizational goals.

Once technologies are selected, defining use-cases becomes paramount. This involves identifying specific scenarios and processes where digital components will be deployed to enable organizational functions. Integration is key to the success of digital initiatives. This section explores strategies for seamless integration, considering factors such as interoperability, data flow, and minimizing disruption to existing operations.

5. Developing Digital Competencies

Building digital competencies is not just a tactical necessity but a strategic imperative. Organizations must nurture specific competencies aligned with the digital roadmap to ensure that their teams possess the skills necessary to navigate the complexities of digital transformation.

Organizations need to invest in skill development initiatives to bridge the gap between existing capabilities and the skills required for successful digitalization. This involves training programs, certifications, and fostering a culture of continuous learning. Digital competencies often span multiple disciplines. This section emphasizes the importance of cross-functional collaboration, encouraging teams from different departments to work collaboratively on digital initiatives.

6. Digital Leadership

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

As organizations embark on digital journeys, the role of digital leadership becomes increasingly critical. This section explores the attributes of effective digital leaders and how they facilitate collaboration within the industry ecosystem, fostering partnerships that drive successful digital initiatives. Effective digital leaders possess a unique set of characteristics. This includes a strategic vision, adaptability, strong communication skills, and the ability to inspire and motivate teams through the challenges of digital transformation.

Digital leadership extends beyond organizational boundaries. Leaders must navigate and collaborate within the broader industry ecosystem, fostering partnerships with external entities such as suppliers, customers, and technology providers.

7. Agile Data Architecture

The agility of data architecture is a crucial element in accomplishing effective digital transformation. Rapid and agile data architecture, when coupled with robust cybersecurity measures, ensures a secure and flexible foundation for digital initiatives. This adaptability becomes particularly crucial as organizations respond to evolving business requirements and technological advancements. Data is the foundation of digitalization and the versatility of agile data architecture in responding to changing business needs, leveraging real-time insights, and facilitating seamless data flow across organizational functions is key to an effective digital transformation.

8. Key Elements for a Digital Journey

Navigating the digital landscape requires a strategic mindset and a keen understanding of key elements that can influence the success of the digital journey. Economic factors are playing an important role, so understanding the financial implications, return on investment, and long-term sustainability are critical components of this exploration. Additionally, in an era of increasing cyber threats, robust cybersecurity measures are non-negotiable. This part emphasizes the need for organizations to prioritize cybersecurity, adopting best practices, and continually evolving their defenses against evolving threats.

Embarking on a digital journey requires careful consideration and strategic planning. Success in the digital landscape hinges on several key elements that organizations should prioritize:

- **Clear Vision and Strategy**: definition of a clear vision for digital transformation aligned with overall business objectives and development of a comprehensive strategy that outlines the roadmap and expected outcomes;
- **Leadership Commitment**: gaining commitment from top leadership to champion digital initiatives and ensuring leaders understand and endorse the transformative nature of digitalization;
- **Cross-Functional Collaboration**: foster collaboration across different departments and functional areas, break down silos to encourage the sharing of insights and expertise;
- **Agile and Adaptive Culture**: cultivate an agile and adaptive organizational culture, embrace change and encourage a mindset that views challenges as opportunities;
- **Digital Competencies and Skills**: assess and develop digital competencies within the organization, invest in training programs to upskill employees in emerging technologies;

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

- **Customer-Centric Approach**: prioritize a customer-centric approach in digital initiatives, understand customer needs and use digital solutions to enhance the overall customer experience;
- **Data-Driven Decision-Making**: establish robust data governance practice and emphasize data-driven decision-making to enhance efficiency and effectiveness;
- **Technology Infrastructure**: Invest in a scalable and adaptable technology infrastructure, leverage modern technologies that align with the organization's goals;
- **Cybersecurity Measures**: Implement robust cybersecurity measures to safeguard digital assets, Prioritize data security and compliance with industry regulations.
- **Continuous Innovation**: Foster a culture of continuous innovation, encourage experimentation and learning from both successes and failures;
- **Change Management**: Implement effective change management strategies, communicate changes transparently and involve employees in the transformation process.
- **Metrics and Key Performance Indicators**: define key performance indicators (KPIs) to measure the success of digital initiatives and regularly monitor and assess progress against established metrics;
- **External Partnerships**: collaborate with external partners and seek support from organizations with expertise to the digital transformation process.
- **Regulatory Compliance**: stay ahead of regulatory requirements related to digital practices and ensure compliance with data protection and privacy regulations.
- **Sustainability Considerations**: integrate sustainability into digital strategies and assess the environmental impact of digital initiatives and adopt eco-friendly practices like green IT infrastructure or renewable energy sources.

In conclusion, by systematically progressing through these key stages, businesses can not only navigate the complexities of the digital landscape but also cultivate a strategic advantage in the evolving market. The formulation of a successful digital roadmap requires a multidimensional approach that aligns technological advancements with organizational goals. The significance of defining the general scope lies in its transformative potential, turning administrative steps into strategic imperatives. Identifying relevant digital strategies ensures that the roadmap is tailored to the unique business model, creating a synergy between technological initiatives and organizational values. Considering business opportunities and needs acts as the compass, guiding organizations toward areas of value creation and innovation. The foundations of digital components establish the technological bedrock, emphasizing the importance of careful selection, use-case definition, and seamless integration. Developing digital competencies emerges as a crucial element, emphasizing that success hinges on nurturing a workforce equipped with the skills essential for a digitally driven future. Digital leadership emerges as the guiding force, steering organizations through the challenges of transformation and fostering collaboration within the broader industry ecosystem. Agile data architecture ensures that organizations can adapt swiftly to changing business requirements while maintaining the security and flexibility of their digital foundations.

From visionary leadership and cross-functional collaboration to embracing change and prioritizing data security, these elements collectively contribute to the success of the

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

digital roadmap. The emphasis on continuous innovation, effective change management, and sustainability considerations reinforces the dynamic nature of digital transformation.

CASE STUDY

Next the paper gives an example of such a Digital Roadmap that a global agribusiness company has embarked recently and some key milestones and elements identified. The organization is a global agribusiness and food company that operates across the entire food supply chain that operates in multiple countries worldwide, with a significant presence in key agricultural regions. This global footprint allows the company to source, process, and distribute agricultural products on a large scale. The organization is known for its vertically integrated supply chain, connecting farmers to consumers. The company is involved in every stage of the agricultural supply chain, from sourcing raw materials to processing and delivering final products. Its diversified operations encompass agribusiness, food and ingredients, and sugar and bioenergy, positioning the company as a major contributor to the world's food and agricultural systems.

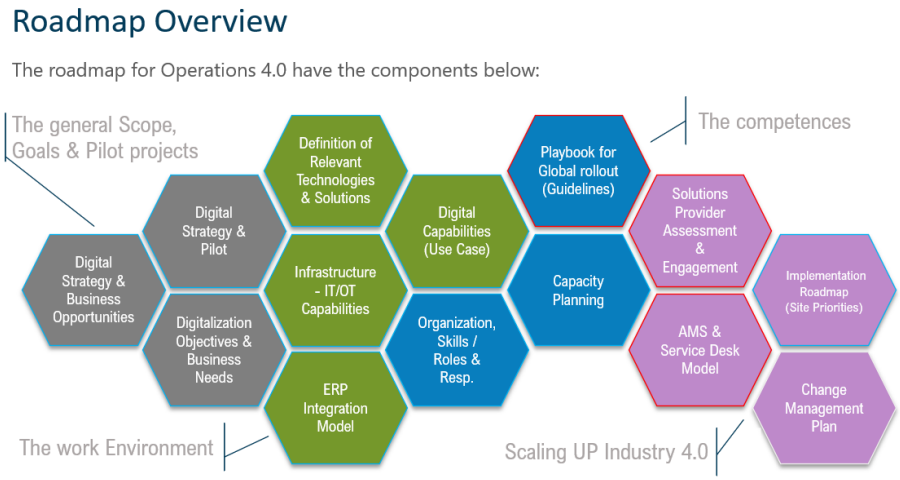


Figure 1. Example of Digital Roadmap from an Agribusiness Company
Source: Confidential interview with industry expert, 2023

As the picture above shows, this enterprise has structured their digital roadmap into four main pillars:

- **Strategy** (where they assessed and set the general scope, set the business goals and objectives and agreed on their pilot projects)
- **Foundation** (facilitated a work environment than enabled an open mentality towards learning, change and experimentation, assessed relevant digital technologies with suitable solutions to their needs, analysed the existing infrastructure and capabilities, as well as their enterprise resource planning integration model and defined use-cases)
- **Enablement** (identified and addressed digital competencies that needed to be developed)
- **Roll-out and Continuous Improvement** (scaling up activities for Industry 4.0 and plan to replicate what is working properly from one facility to another, as well as increase, change, improve additional requirements, recruit and manage talent, prioritizing multidisciplinary teams and the capacity to turn data analysis

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

into a strong asset, define the team of providers, validate results and systematize the learning mechanisms.

Each Pillar is expanded with a specific list of components to deploy Operations 4.0. The current deficiencies of the organization have identified and expected outcomes are identified as well. From a strategy and foundation perspective governed by Industry 4.0 principles, this organization has derived 4 main digital programs:

- **Link floor to business** – with focus on current Enterprise Resource Planning (ERP) systems, Business Intelligence tools, System integration with the objective of increasing the availability of shop floor data for online integration for all company systems and processes
- **Data** – focus on Big Data, Cloud Computing, Artificial Intelligence and Robotics Process Automation (RPA) technologies
- **Adaptability** – its aim is to allow simulations and 3D printing
- **Empowered team** – trainings to improve digital competencies, increase the use of collaborative robots and smart devices in the daily operations.

Digital transformation is impacting every sector and business, and the organization included in this case study is no exception. With the changes in their operating model, they have initiated several initiatives aimed at rewiring and simplifying their organization. While ongoing efforts continue to focus on strengthening foundational processes and systems, they have identified opportunities to enhance business value through digital solutions, revolutionizing both their operations and customer service. Several promising digital initiatives are already in progress and they have embarked on a digital journey since 2021. Recently the organization has formed a cross-company working group to comprehensively explore digital opportunities. This endeavor has identified key priorities in digital, each with the potential to reshape the business landscape: commercial analytics, customer and producer interactions, industrial operations, and data architecture. Armed with insightful ideas, this enterprise is ready to transition to the next phase, where they have started formulating specific project plans and diligently execute them.

The Digital Programs derived from the Digital Roadmap for this particular enterprise are built around the objective of optimizing the value chains. From **origination** initial stage, where the decision making process around commodity sourcing is key to the **in-land transportation** where the organization needs to both make short-term trade-offs to transport their volumes with minimum freight cost given the operating conditions as well as maximizing the margins by selecting optimal routes and means of transport for their process flows to the silos. Next the value chain moves into the **silos** where there is a high need for optimization of the warehouse storage by improving controlling and selection process and measurements followed by the **production** stage, where profitability can be maximized by addressing yield, efficiency and digital and analytics optimizations are in high demand. The immediate step in the flow are the **ports**, where the organization needs to ensure visibility and optimizise the flow and quality of goods between production and client demand as well as maximizing long-term port utilization. The flow continues with the **vessels** where the enterprises needs to maximize global asset utilization by allocating vessels to routs so that origin and destination requirements are met from a regulatory and compliance perspective and ends with the **customers**, where there are processes around inbound, storage and processing to definte the quality and volume with the same objective of maximizing the margins, ensuring their profitability.

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

While defining their digital strategy, this organization has identified the following areas where digital transformation can bring additional value: safety (increase through embedded intelligence and leverages data to deliver predictive capabilities to reduce/eliminate incidents), quality and food safety (provide compliant end products enabled through Artificial Intelligence and Machine Learning techniques and automations that can optimize quality and increase profitability), environmental susteinability (optimize water, waste and energy use by leveraging data), productivity (fully automated, self-optimizing with seamless integration across the value chain), efficiency (provide real time asset lifecycle management to increase utilization and efficiency), foundation (ensure standards for operational technology and automation, sensorsing and cybersecurity capabilities, as well as edge-to-cloud connectivity). The digital roadmap includes elements that will leverage the digital and analytics to achieve optimal responses while ensuring business continuity, as well as in parallel empower and upskill and train their employees and maximizing value for the entire value chain described above.

Phase 1 of their digital journey is ongoing and it includes 11 production lines that have been defined as use cases were automations are being piloted, infrastructure in being upgraded (new firewalls, automation servers), dashboards and analystics tools are being implemented, as well as quality sensors, basic instrumentation, asset monitoring sensors in critical equipments. In parallel, a new tower in the organization has been built around digital expertise with roles like data scientist, accelerated facility leaders, automation experts, data architects, system integrators. Early 2024 the first phase of the digital journey will come to an end and comprehensive lessons learnt will be derived, as well as financial results.

The journey of the global agribusiness company into digital transformation has demonstrated some valuable lessons that transcend technological aspects and touch upon the very fabric of organizational dynamics. One fundamental takeaway is the paramount importance of aligning expectations across the organization, ensuring a shared understanding of the digital roadmap's pace and impact. The adoption of an agile approach emerged as a necessity, allowing the organization to flexibly navigate the dynamic digital landscape. Cross-functional collaboration proved instrumental, enriching the transformation process with diverse perspectives and aligning digital initiatives with overarching organizational goals. The realization that investing in employee training and upskilling is foundational to success underscores the human-centric aspect of digital transformation. Additionally, effective change management strategies, including transparent communication and employee involvement, were revealed as pivotal in overcoming resistance and ensuring a smooth transition. The continuous vigilance in cybersecurity measures underscored the need to stay ahead of emerging risks, safeguarding digital assets. Careful vendor and technology selection, considering both immediate needs and future scalability, showcased the importance of strategic decision-making. Lastly, maintaining a customer-centric approach throughout the digital journey emerged as a guiding principle, ensuring that digital solutions align with and enhance the customer experience. These lessons collectively illuminate the holistic nature of successful digital transformation, emphasizing adaptability, collaboration, and a strategic mindset as indispensable elements of the digital transformative process.

The organization is confident that the Digital Roadmap and derived Digital Programs governed by Industry 4.0 principles are a key enabler for increasing both productivity and manufacturing excellence, as well as enhancing optimizations in the areas of quality, production, maintenance and transportation.

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

CONCLUSIONS

In conclusion, this paper underscores the transformative role of digitalization and the strategic imperatives that organizations must embrace to thrive in the ever-evolving digital landscape. The exploration of Industry 4.0 principles and the emphasis on strategic planning, cross-functional collaboration, and robust cybersecurity measures provide a comprehensive guide for organizations embarking on their digital journey.

As we conclude, it is imperative to not only absorb the insights presented but to catalyze action within organizations. Actively implementing the recommendations outlined in this paper is essential for achieving tangible success in the realm of digital transformation.

While this paper strives to offer valuable insights, it is essential to acknowledge that the field of digital transformation is dynamic and ever-changing. Future research and exploration are warranted to address emerging challenges and opportunities in this fast-paced environment.

As organizations navigate the digital terrain, the unique contributions of this paper in providing actionable recommendations and strategic insights position it as a valuable resource. By actively embracing the principles and practices discussed, organizations can not only meet the immediate challenges of digitalization but also foster sustained resilience and competitiveness.

This concludes our journey through the nuances of digital transformation, with the hope that organizations will leverage the presented roadmap to navigate the digital realms successfully.

BIBLIOGRAPHY

1. ZAOUI, F., SOUISSI, N. *Roadmap for digital transformation: A literature review.* The 7th International Conference on Emerging Inter-networks, Communication and Mobility (EICM). Leuven-Belgium, August 2020. Procedia Computer Science 175 (2020) 621-628
2. HESS T., MATT C., BENLIAN A., WIESBÖCK F., *Options for formulating a digital transformation strategy*, 2016, MIS Q Exec 15(2):123–139
3. NADKARNI, S., PRÜGL, R., *Digital transformation: a review, synthesis and opportunities for future research*. Management Review Quarterly, 18 April 2020, (2021) 71:233–341
4. ZAMMUTO RF, GRIFFITH TL, Majchrzak A, Dougherty DJ, Faraj S (2007) *Information technology and the changing fabric of organization*. Org Sci 18(5):749–762
5. BESSON P, ROWE F, *Strategizing information systems-enabled organizational transformation: a transdisciplinary review and new directions*, 2012, J Strateg Inf Syst 21:103–124
6. KARIMI J, WALTER Z, *Corporate entrepreneurship, disruptive business model innovation adoption and its performance: the case of the newspaper industry*, 2016, Long Range Plan 49(3):342–360
7. CHA KJ, HWANG T, GREGOR S, *An integrative model of IT-enabled organizational transformation: a multiple case study*, 2015, Manag Decis 53:1755–177
8. YEOW A, SOH C, HANSEN R, Aligning with new digital strategy: a dynamic capabilities approach. 2018, J Strateg Inf Syst 27(1):43–58

DOI: https://doi.org/10.53486/escst2023.16
International Conference, December 07-08, 2023, Chișinău, Moldova

9. RESCA A, ZA S, SPAGNOLETTI P, *Digital platforms as sources for organizational and strategic transformation: a case study of the Midblue project.*, 2013, J Theor Appl Electron Commer Res 8(2):71–84
10. HANSEN R, SIA SK, *Hummel's digital transformation toward omnichannel retailing: key lessons learned*, 2015, MIS Q Exec 14(2):51–66
11. SINGH A, HESS T, *How chief digital officers promote the digital transformation of their companies*, 2017, MIS Q Exec 16(1):1–17
12. OBERLÄNDER, M., BEINICKE, A., BIPP, T. *Digital competencies: A review of the literature and applications in the workplace*, Computers & Education, Volume 146, 2020, 103752, ISSN 0360-1315
13. SOUSA MJ., ROCHA, A. *Digital learning: Developing skills for digital transformation of organizations.* Future Generation Computer Systems. Volume 91, 2019, Pages 327-334, ISSN 0167-739X
14. ISSA, A., HATIBOGLU B., BILDSTEIN, A., BAUERHANSL, T. *Industrie 4.0 roadmap: Framework for digital transformation based on the concepts of capability maturity and alignment.* Procedia CIRP. Volume 72, 2018, Pages 973-978, ISSN 2212-8271.
15. Whitepaper on *The Future of Finance [online]*. Available from: <https://www.serrala.com/whitepaper/whitepaper-the-future-of-finance>

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chişinău, Moldova

CYBERSECURITY RISK

Serghei OHRIMENCO

PhD Habilitat, Professor,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0002-6734-4321
E-mail: osa@ase.md

Valeriu CERNEI
PhD Student,
Academy of Economic Studies of Moldova,
Partner, IT Audit & Advisory BSD, Management SRL, Moldova,
ORCID 0000-0003-3300-334X
E-mail: valeriu.cernei@bsd.md

Abstract: *This paper presents the multifaceted field of cyber risks, their structure and composition, exploring the challenges posed by the rapid evolution of digital technologies. It highlights the prevalence of cyber risks as a set of activities performed in various sectors of human life, revealing the vulnerabilities faced by individual and collective users, commercial organisations, governments and individuals in today's hyper-connected landscape. The paper emphasises the importance of robust risk management strategies, highlighting the dynamic and persistent nature of cyber threats. A host of relevant international standards, frameworks and cyber risk management techniques to mitigate potential losses are reviewed. Approaches to defining the category of cyber risk are analysed. Daily attack techniques are reviewed. Risk analysis based on a set of reports from leading computer firms has been carried out. The structure of cyber security threats affecting the level of risk is determined. Despite the existing scientific and practical achievements in the field of cyber security, the ever-changing tactics of cyber criminals require constant adaptation of organisational and technical actions and the adoption of a set of proactive measures. Cyber risk management strategies are discussed, which include the selection of possible approaches, taking into account factors such as the level of cyber maturity, available resources, required skills and experience in cyber risk management. The article identifies the most prominent risk management tools, suggests some risk management strategies and advocates a comprehensive approach to cyber security that recognises the inevitability of cyber attacks and the need to build resilience in the face of emerging threats.*

Keywords: *threat, risk, cyber, risk management, risk strategy.*

UDC: *004.056.53:330.131.7*

JEL Classification: *D74 D81 F52.*

INTRODUCTION

Currently, the digital world embeds everyone as they use platforms, applications, data, services, and communication tools. It is almost impossible to find an area of activity where modern achievements in information and communication technologies and applications are not used. In this regard, ensuring the security of users' activities is of crucial importance to protect people, organizations, the environment, and infrastructure. We manage risks every day and everywhere and technology brings many specific risks that may have a critical impact on our lives. By the other side, related to technology, a complex of specific solutions based on developments and achievements in artificial intelligence, "zero trust" model, etc., is being used to counteract these risks.

The ongoing and dynamic confrontation between groups of malicious software (malware) developers and information security tools reflects the ratio of achievements in theory and practice. As threats change and increase qualitatively and quantitatively, risks

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chişinău, Moldova

also change. Digital threats require increased vigilance and determination to adequately respond to the constantly expanding risk cycle. The landscape of cybersecurity risk management is rapidly changing, and experts expect the emergence of new developments from official regulators and standards aimed at developing cyber risk management strategies as well as organizational-technical plans to mitigate the consequences of incidents.

It should be kept in mind that cybersecurity breaches are inevitable, and there are objective reasons for this. Among security and risk management experts, there is an opinion that preventing all hacks and information leaks is practically impossible, despite serious investments in the protection system. One cannot minimize risks to a "zero absolute". It is essential to focus efforts on the resilience of the information security system, treating breaches as incidents and building a learning and resistance system based on their knowledge base.

Information security specialists know and understand that nothing ever works without disruptions for an extended period. Any internal or external threat or risk can lead to a state where a well-functioning management object loses its competitive advantages, faces disruptions, etc. There is a constant hope that information security specialists will establish processes that allow for a systematic analysis of risks, threats, hazards, and issues and provide a list of economically efficient measures to reduce the risk to an acceptable level.

RISKS AND RISKS MANAGEMENT

Literature review

There are quite a few literary sources that address the issues of managing cyber risks. Among the main ones, we should mention the following: " Cyber-Risk Management" [1], "Optimal Spending on Cybersecurity Measures: Risk Management" [2], "Managing Information Risks: Threats, Vulnerabilities, and Response Measures" [3], "Managing Risks of Organizational Incidents" [4], "Cyber Risk, Intellectual Property Theft, and Cyber Warfare: Asia, Europe, and the USA" [5], and others.

First of all, let's point out the book by Karl Young, " Cybercomplexity: A Macroscopic View of Cybersecurity Risk" [6]. This book examines the issue of IT environment complexity, or "cyber entropy," which is usually considered a primary source of cybersecurity risk. The complexity is defined and simplified for analysis, assuming a probabilistic approach to security risk management. Then, a simple model of cyber entropy based on Shannon's entropy, a fundamental concept in information theory, is proposed. Key factors of cyber entropy emerge from this model, where these drivers reveal the dependence of cybersecurity risk on scale and explain why macroscopic security measures are necessary to eliminate cybersecurity risk on an enterprise scale. The book also discusses significant operational consequences of cyber entropy, thus providing both theoretical foundation and practical guidance for addressing this longstanding issue in cybersecurity risk management.

The goal of managing cyber security risks is to identify and eliminate factors that compromise information or disrupt business related to information by applying security measures in accordance with the organization's risk tolerance [6, p.153].

A fundamental aspect of security risk management is that all threat scenarios are equivalent when viewed from a sufficiently high level. This equivalence partially explains why the risk assessment process is universal. However, equivalence is not the same as identity. It is evident that all threat scenarios are not identical, explaining why the experience required for security risk management depends on the details of the scenario.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chişinău, Moldova

Another source of interesting information on cyber risks is the book by the collective authors David Insua, Caroline Baylon, Jose Vila, "Security Risk Models for Cyber Insurance" [7]. The authors propose a "model solution" [7, p.56-60], the essence of which is as follows: to determine a rational distribution of resources for the protection object (the so-called "cybersecurity portfolio," which is a combination of security products, security management and control tools, and recovery and insurance products (cyber insurance)), several steps are required:

- The problem of risk management should be considered from the perspective of the "defender" and the model of their preferences (i.e., their utility function) regarding the optimal distribution of resources, considering alternative solutions among different types of security products (portfolio of security control means and portfolio of recovery control means) and insurance options, as well as conditional probabilities of various threats or impacts.
- To determine the conditional probabilities of threats from the "attacker," it is necessary to investigate the risk management problem from the perspective of the "attacker" or adversary – their strategic thinking. It is necessary to create influence diagrams of the attacker and build a model of preferences (utilities) regarding the conduct of targeted attacks. It should be noted that the actions of the attacker are constrained by various factors, including the probability of detection, the consequences of the attack, the existence of alternative types of targeted attacks, etc. Then, the probability of an attack by the "attacker" on the "defender" should be modelled.
- Optimization is carried out to maximize the expected utility of the defender's actions, taking into account the strategic thinking of the attacker. We also consider the probability that the "defender" may be attacked by one or more "adversaries." Each possible case is matched with a potential cybersecurity portfolio that maximizes expected utility and demonstrates the optimal choice of a cybersecurity portfolio to protect against adversaries.

Simultaneously, it is necessary to understand the defender's challenge, which involves viewing the risk management problem from the defender's perspective and modelling their preferences, i.e., their utility function. This includes determining the optimal distribution of resources considering alternative security product solutions, such as portfolios of security control measures and portfolios of recovery control measures, along with insurance options.

There are numerous relevant international standards, frameworks and methods for managing cyber risks and helping answering the defender’s questions. Some most popular include [8] - [15]:

ISO/IEC 31000: Contains principles and general recommendations for risk management. The standard is not specific to any industry or sector; it can be applied to a wide range of activities, including strategies and decisions, operations, processes, functions, projects, products, services, and assets. It should also be applied to any type of risk.

ISO/IEC 27005: Provides recommendations for information security risk management. These recommendations are based on ISO/IEC 31000. This standard supports the general concept of ISO/IEC 27001 regarding the requirements for managing information security systems. ISO/IEC 27032 offers cybersecurity recommendations with a focus on the virtual world and virtual intangible assets. According to ISO/IEC 27002:2022 , "information related to information security threats must be collected and analyzed to obtain information about threats."

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

CRAMM (CCTA Risk Analysis and Management Method): Developed by the British government agency CCTA (Central Communications and Telecommunications Agency), now renamed the Office of Government Commerce (OGC).

EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité): Developed by DCSSI (Central Directorate for Information System Security, under the Prime Minister) in France. EBIOS is designed to adapt to the specific characteristics and needs of French organizations and has some cultural and legal specificities.

Mehari Methodology: Developed in 1995 by CLUSIF (Club for Information Security and Freedom of Communications). Mehari focuses on assessing information security and IT resource risks in organizations, providing a structure for analyzing and managing these risks. One significant difference is that Mehari was developed by an independent organization, and specific approaches and tools may vary.

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation): Developed by Carnegie Mellon University in the United States, providing a sophisticated risk modeling methodology with a focus on identifying and assessing operational risks and security practices.

FAIR (Factor Analysis of Information Risk): A framework for analyzing and managing risks in information security and operational risks. It is a quantitative and model-based approach designed to help organizations understand, analyze, and quantitatively assess risks associated with information in financial terms.

NIST IR 8441 (Cybersecurity Framework Profile 20 for Hybrid Satellite Networks): A profile of the cybersecurity framework for hybrid satellite networks. This profile serves as a practical guide for organizations and stakeholders involved in designing, acquiring, and operating satellite buses. Using this profile provides protection of services, self-assessment in accordance with cybersecurity principles, detection of cybersecurity-related disruptions, timely and effective response to service anomalies, and recovery to normal operation after a cybersecurity incident.

It is worth mentioning that organizations and countries, aiming to minimize risks, issue and recommend the use of guidance documents, best practices, and specialized literature to systematize and more effectively manage them. In this regard, ISO 19600 introduces compliance risk assessment, consolidating individual compliance management and risk management standards, with processes closely aligned with ISO 31000. This standard aids in evaluating how legislative acts, guiding documents, and best practices have been implemented and maintained in terms of managed risks. Among them, notable standards and directives include Basel III, NIS (II) Directive, European Union Cybersecurity Act, Federal Information Security Management Act (FISMA), Payment Card Industry – Data Security Standard (PCIDSS), Sarbanes Oxley Act (SOX), and others [16].

It is also worth mentioning the models considered by the authors, which contribute to the development and improvement of the CCSMM model - The Two-Dimensional CCSMM and The Three-Dimensional Model for a Community. It is the latter version of this model that allows for research at practically all levels, from the individual level, organization, to the state and nation. The model takes into account five levels of coverage, from initial to advanced. This model demonstrates the thesis that society consists of individual personalities and organizations, and their maturity influences the overall cybersecurity maturity of society. The three-dimensional model, in particular, has expanded the possibilities for researching cybersecurity issues, providing flexibility and scalability in the analysis of processes.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

Analysts argue that this model serves as a roadmap for improving cybersecurity for individuals, organizations, communities, states, and nations.

Threats and Risks

Let's present several definitions of risk. "Risk is the probability of an incident occurring and its consequences for the object" as defined by [1, p.9]. The "classic" risk management approach is based on the threat. Several definitions are used, among which the following is considered relevant: "A threat is the point of interaction and convergence of people, the Internet, and computers. The threat arising from interaction can result from an error or a malicious influence. An error can be eliminated by increasing the awareness of the importance of handling, for example, confidential information. In this regard, a malicious strike is different." [2, p.19]. The author associates information security threats with the activities of criminal groups and transnational organized crime (TOC). Criminal networks and organized groups operate in many countries, planning their activities and achieving their business goals. Their activities may include a multitude of heinous crimes - human trafficking, sexual exploitation of adults and children, drug trafficking, violent crimes, corruption, arms trafficking, and even the sale of human body parts and representatives of flora and fauna under threat of extinction. Unfortunately, it should be noted that TOC was the first to appreciate the benefits and implement modern information technologies and communications, as well as reliable security systems.

The goal of cybersecurity risk management is to identify and eliminate factors that compromise information or disrupt business by applying security measures in accordance with the organization's risk tolerance [3]. "We can define risk analysis as a set of knowledge (methodology) that assesses and determines the probability of adverse effects on an agent (chemical, physical, or other), industrial process, technology, or natural process," as stated [4].

In cybersecurity, risk is the probability of an adverse event occurring. Thus, risk includes two key parameters: the probability that the event will actually occur and the impact it will have, which can be assessed based on the probable seriousness of the event. In mathematical terms, risk can be expressed as a deviation or variation from the expected result. That is why in financial markets, high-risk investments may be more preferable than low-risk investments, as there is at least a chance of very high returns. However, in the field of computer security, it is usually necessary to create an environment with a low level of risk, where threats and the damage they can cause are actively minimized [5, p.16].

According to the "Global Risks" report for 2023 prepared by the World Economic Forum [17], global risks, ranked by severity in the short term (up to 2 years) and long term (10-year period), include several directions, including the technological sector. In particular, for short-term and long-term forecasts, the value "Widespread cybercrime and lack of cybersecurity" is ranked 8th. The report states that technologies will exacerbate digital inequality, while risks associated with cybersecurity will remain a constant problem. The technological sector will be the main target for industrial policy and expanded government intervention. Government aid, military budgets, and private investments will ensure high rates of development and research in new technologies over the next decade, with a focus on areas such as artificial intelligence, quantum computing, and biotechnology.

For some countries, this will be a partial solution to a range of emerging crises (healthcare, food security, and the consequences of climate change). For some countries, digital inequality and divergence will grow. In all economies, technologies bring risks as disinformation increases, and uncontrolled turnover occurs among both workers and "white-collar" workers. Along with the growth of cybercrime, an increase in attacks on

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

critical infrastructure objects is forecasted, including agriculture, water supply systems, financial systems, public safety, transportation, energy, and communication infrastructure (space and underwater). Technological risks will be associated not only with fraudsters. Big data analysis will allow the abuse of personal information; weaken individual digital sovereignty, and the right to privacy.

The map of interconnections in the landscape of global risks in the report for the technological group includes adverse consequences of advanced technologies, concentration of digital power, digital inequality, disruption of critical information infrastructure, widespread cybercrime. In other words, a low level of cybersecurity.

In most cases, when it comes to risk management, the main threat is hackers' activity and cyberattacks. Due to the extremely rapid development of technology (technical and software), a significant part of hackers' activity has radically changed. From individual acts of vandalism and theft, an underground industry has grown, well-organized and excellently equipped with the latest innovations [18]. There has been a rapid growth and leap from individual hacking cases to the creation of specialized structures whose activities range from extracting financial benefits to achieving political goals [19].

The seriousness of this activity is confirmed by information on events from September 16 to 30, 2023, recorded by the website https://www.hackmageddon.com [20]. Computer analyst Paolo Passeri presents the results of the study for this period: information on 165 events was collected and processed, or 11 events per day. The total number of cases consists of 119 cases (72%) of cybercrime, 23 cases of cyber espionage (13.9%), 8 cases of hacktivism (4.8%), and no data in 15 cases (9.1%). The techniques of daily attacks are characterized by the following data: malware 58 cases (35.2%); unknown 32 (19.4%); vulnerability exploitation 26 (15.8); targeted attacks 24 (14.5%); account takeover 11 (6.7%); DDoS attacks 8 (4.8%); scams or fraudulent schemes 4 cases, cross-site scripting 1, attacks through publicly available container images 1.

Experts have detected several large-scale organizations operating in the financial technology sector which had been compromised. For example, the company Mixin Network lost an amount equivalent to 200 million dollars. This case became the largest hack in 2023.

Risk aspects are also noted in the Hiscox report on cyber readiness for 2023 [21]. The report identifies several significant changes in cyberspace that should be noted by anyone involved in combating cybercriminals. Cyber technologies remain the number one issue for business, but timid sprouts of optimism are beginning to appear. The top ten business risks are listed in the following table 1.

Table 1. Top 10 major risks (%)

№	Name	2023	2022
1	Exposure to a cyber attack	40	45
2	Losses due to economical issues e.g. inflation	38	40
3	Emergence of new competitor	36	36
4	Skills shortage	35	40
5	Reputational damage e.g. negative press	35	37
6	Regulatory or legislative changes	34	37
7	Pandemic or infectious diseases	33	42
8	Geopolitical conflicts disrupting operations	33	-
9	Fraud and white-collar crime	32	38
10	Extreme weather and natural disasters	29	33

Source: Hiscox Cyber Readiness Report 2023.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

The structure of cybersecurity threats that impact the risk is as follows [22, p.28-29]:

- ✓ *Phishing Attacks*: These attacks involve the use of fake emails or messages to trick people into providing confidential information or clicking on malicious links, often leading to the theft of confidential information or malware infection.
- ✓ *Ransomware Attacks:* Ransomware is a type of malware that encrypts an organization's data and demands payment in exchange for a decryption key. These attacks can result in significant disruptions to business operations and substantial financial losses.
- ✓ *Malware Attacks:* Malware is any type of software designed to harm a computer system or network. This category may include viruses, worms, and trojans, among others.
- ✓ *Insider Threats:* These threats originate from within the organization, such as employees or contractors who intentionally or unintentionally misuse their access to confidential information or systems.
- ✓ *Advanced Persistent Threats (APTs):* APTs are targeted attacks carried out over an extended period by experienced attackers seeking unauthorized access to confidential data or systems.
- ✓ *Internet of Things (IoT) Attacks:* As the number of Internet-connected devices increases, IoT devices become more vulnerable to cybercriminals who can exploit vulnerabilities to gain access to networks or cause disruptions.
- ✓ *Cloud Security Risks*: Cloud services have become an integral part of modern business operations, but they also introduce new security risks, including data leaks, service interception, and unauthorized access.
- ✓ *Social Engineering Attacks:* These attacks involve manipulating individuals into disclosing confidential information or taking actions that harm security, often using psychological tactics.
- ✓ *Distributed Denial of Service (DDoS) Attacks:* DDoS attacks involve overwhelming a system or network with traffic to make it unavailable to users. These attacks can be used to disrupt business operations or extort organizations.
- ✓ *Cyber Espionage*: Cyber espionage involves the theft of confidential information to obtain advantage by organizations and / or States.

Strategies for managing cyber risks

Strategies for managing cyber risks involve choosing possible approaches, considering factors such as the level of cyber maturity, available resources, necessary skills, and experience in managing cyber risks [23]. Various literature sources present different models for responding to identified risks. The authors have analyzed and summarized well-known models, as presented în the table further.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

Table 2. Risk management strategies

№	Risk Strategy	Description
1.	Terminate	Applied when the risk level is high, and it's not possible to apply measures to minimize it, or the cost of implementing measures is too high
2	Control	The most effective measure, involving the implementation or reinforcement of control measures. It is also the most common approach in IT and cybersecurity
3	Transfer	Applied when the risk impact is assessed as high, but the probability of occurrence is low. Transferring risk to a third party can be either complete or partial
4	Contingency	A response measure for risks with high impact and low probability, involving the implementation of backup mechanisms or technologies
5	Take More	Used when both the impact and probability of the risk are low, exploring solutions to optimize resources or new investment directions
6	Tolerate/Accept	Risks with low impact and probability can be considered insignificant and accepted without any specific measures
7	Communicate	A stage in the risk management process related to risks with high impact and medium or low probability. When implementing security control measures cannot reduce risks to an acceptable level, it is recommended to communicate the existence of the risk to all stakeholders, indicating that the risk exists and may affect goal achievement. This aspect is often overlooked
8	Research	Applied in organizations with a mature risk management process, involving a more in-depth study, including impact assessment, probability analysis, comparative analysis, etc. This is typically used by large companies developing products (e.g., antivirus software)
9	Consult	For some risks with a high impact and high probability, more effective measures may be suggested by specialized companies rather than by internal risk management personnel
10	Compliance	Often overlooked, this measure focuses on areas where control is critical to minimize compliance risks and includes checking the effectiveness of control

Source: authors

These strategies provide a framework for organizations to respond effectively to cyber risks based on their specific circumstances and risk profiles.

CONCLUSIONS

In conclusion, the evolving landscape of cyber risks poses significant challenges to organizations, governments, and individuals. The interconnected nature of digital technologies in cyberspace creates both, opportunities and threats. The opportunities provided by widely interconnected digital technologies in cyberspace come with costs, including the creation of possibilities for crime and espionage.

Today, every sector of the economy, every government, and virtually every citizen are constantly exposed to cyber attacks. Most of them suffer from persistent malware infections. Cybercriminals infiltrate quickly and remain unnoticed for months.

Defenders have learned a lot about modern cyber threats, including the types of organizations that cause the most damage, their resources, how they operate, and their motives. We have studied best practices and ways to enhance protection, significantly complicating success for adversaries. The risk can be reduced. However, we also understand that adversaries will be persistent and catch us off guard, regardless of how strong our defence is.

Despite advancements in understanding and implementing cybersecurity measures, the persistent and sophisticated tactics employed by cybercriminals demand constant vigilance. It is important to adopting comprehensive risk management strategies,

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

acknowledging the inevitability of cyber attacks, and the need for continuous adaptation to emerging threats. As technology continues to advance, a proactive and adaptive approach to cybersecurity remains crucial in mitigating the impact of cyber risks and ensuring the resilience of digital ecosystems.

BIBLIOGRAPHY

1. REFSDAL, Atle, et al. *Cyber-risk management*. Springer International Publishing, 2015. p. 33-47.
2. KISSOON, Tara. *Optimal Spending on Cybersecurity Measures: Risk Management*. Routledge, 2021.
3. TAPLIN, Ruth. *Cyber Risk, Intellectual Property Theft and Cyberwarfare: Asia, Europe and the USA*. Routledge, 2020.
4. REASON, James. *Managing the risks of organizational accidents*. Routledge, 2016.
5. SAFFADY, William. *Managing information risks: threats, vulnerabilities, and responses*. Rowman & Littlefield Publishers, 2020.
6. YOUNG, Carl S. Complexity and Cybercomplexity. In: *Cybercomplexity: A Macroscopic View of Cybersecurity Risk*. Cham: Springer International Publishing, 2022. p. 79-87.
7. INSUA, David Ríos; BAYLON, Caroline; VILA, Jose (ed.). *Security Risk Models for Cyber Insurance*. CRC Press, 2020.
8. MCCARTHY, James, et al. Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN). *National Institute of Standards and Technology, NIST Interagency or Internal Report (IR) NIST IR*, 2023, 8441.2023: 28.
9. SCHREIDER, Tari. *Cybersecurity Law, Standards and Regulations*. Rothstein Publishing, 2020.
10. Information Security Forum. *Standard of Good Practice for Information Security* [online] 2020. [viewed 9 November 2023]. Available from: <https://www.securityforum.org/solutions-and-insights/standard-of-good-practice-for-information-security-2020/>
11. MALEH, Yassine, et al. *IT governance and information security: Guides, standards, and frameworks*. CRC Press, 2021.
12. Peltier T. R. Information security risk analysis. – CRC press, 2005.
13. WHITE, Gregory B. The community cyber security maturity model. In: *2011 IEEE international conference on technologies for homeland security (HST)*. IEEE, 2011. p. 173-178.
14. Hafiz Sheikh Adnan Ahmed. *A Guide to the Updated ISO/IEC 27002:2022 Standard.* Part 1. [online]. 2023. [viewed 6 December 2023]. Available from: <https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2023/volume-7/a-guide-to-the-updated-iso-iec-27002-2022-standard-part-1>
15. YOUNG, Carl S. Complexity and Cybercomplexity. In: *Cybercomplexity: A Macroscopic View of Cybersecurity Risk*. Cham: Springer International Publishing, 2022. p. 79-87.
16. SCHREIDER, Tari. *Cybersecurity Law, Standards and Regulations*. Rothstein Publishing, 2020.

DOI: https://doi.org/10.53486/escst2023.17
International Conference, December 07-08, 2023, Chișinău, Moldova

17. World Economic Forum. *Global Risks Report 2023*. [online]. 2023. [viewed 29 November 2023]. Available from: < https://www.weforum.org/reports/global-risks-report-2023>
18. OHRIMENCO, Serghei; BORTA, Grigori; CERNEI, Valeriu. Estimation of the key segments of the cyber crime economics. In: *2021 IEEE 8th International Conference on Problems of Infocommunications, Science and Technology (PIC S&T)*. IEEE, 2021. p. 103-107.
19. OHRIMENCO, Serghei; ORLOVA, Dinara; CERNEI, Valeriu. Cyber Threats Modeling: An Empirical Study. *Business Management/Biznes Upravlenie*, 2023, 3.
20. PASSERI, P. Hackmageddon. *Cyber Attacks Timeline. 16-30 September 2023*. [online] 2023 [viewed 28 November 2023]. Available from: <https://www.hackmageddon.com/2023/11/28/16-30-september-2023-cyber-attacks-timeline/>
21. Hiscox. *Cyber Readiness Report 2023*. [online]. [viewed 11 December 2023]. Available from: https://www.hiscoxgroup.com/sites/group/files/documents/2023-10/Hiscox-Cyber-Readiness-Report-2023.pdf
22. WATTERS, Paul A. *Cybercrime and Cybersecurity*. CRC Press, 2023.
23. ULSCH, MacDonnell. *Cyber threat!: how to manage the growing risk of cyber attacks*. John Wiley & Sons, 2014.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.18
International Conference, December 07-08, 2023, Chişinău, Moldova

THE CURRENT SITUATION WITH THE INFORMATION SECURITY IN UKRAINE

Liudmyla RYBALCHENKO,

PhD, Associate professor,
Dnipropetrovsk State University of Internal Affairs, Dnipropetrovsk region, Ukraine,
ORCID 0000-0003-0413-8296
E-mail: luda_r@ukr.net

Abstract: *The condition in which Ukraine is since 2022 after russia's full scale military invasion, forces us to consider the issue of security in all spheres of life as one of the main components of the state's national security. Conducting informational influence on human consciousness has changed significantly, which is carried out with the use of mass media. The creation of mass information attacks, bots, fakes and other means of influence are effective tools for disorienting the entire society and manipulating people to increase panic. Specially created information resources try to influence in such a way that a person perceives information in the way it is presented and believes it.*

Keywords*: information security, national security, protection of personal data, information technology.*

UDC: *004.056(477)*

JEL Classification: *H56; D81.*

INTRODUCTION

Rapid changes that are taking place in the modern information space require effective protection of national information security, which should guarantee the safe functioning of all spheres of life for Ukrainians. Ensuring information security at all levels of socio-economic development, improving legislative and regulatory provisions on information protection, identifying possible threats and preventing them, and cooperation with other countries and international organizations is an important strategy for the international and national security of the country, especially during the martial law period in Ukraine.

To the main regulatory documents and laws regarding information security of Ukraine belongs: the Constitution of Ukraine, the Criminal Code of Ukraine, the Law of Ukraine "On the Basic Principles of Cybersecurity in Ukraine", the Law of Ukraine "On Information", the Law of Ukraine "On Protection of Information in Information and Telecommunication Systems", the Law of Ukraine "On Personal Data Protection" and documents in the field of personal data protection, the Law of Ukraine "On Access to Public Information", the Law of Ukraine "On National Security of Ukraine" and other laws, also, the Information Security Doctrine of Ukraine, the Council of Europe Convention on Cybercrime and other.

PAPER BODY

The issue of information security is related to information technologies that are used to ensure information security. Protection of information security consists not only of the protection from an unauthorized access to information, but also of the use of appropriate methods for its security and protection [1].

Today, preserving information sovereignty and forming an effective security system in the information sphere is a top priority for our country. Ensuring the integrity of

DOI: https://doi.org/10.53486/escst2023.18
International Conference, December 07-08, 2023, Chişinău, Moldova

society, protecting the national information space and countering all negative information influences is an important issue for Ukraine.

Ensuring reliable information security in the country will protect the interests of the citizens in obtaining true and quality information. Information security is one of the important components of the country's national security. It is information security that reflects the state of protection of the interests of citizens and the country from negative informational influences and dangers that may be associated with unauthorized access and interference with personal or state information, as well as its dissemination [2]-[3].

The issue of guaranteeing information security in Ukraine became the most urgent during the war due to the influence and spread of russian propaganda through mass media on the consciousness of Ukrainian citizens and the public around the world.

Now there are significant threats in the national information space of Ukraine, which pose a danger to our state, its sovereignty, integrity, political and economic development.

The creation of threats to the national security of Ukraine in the information sphere is a danger to the life of every citizen, it has a negative informational impact on the consciousness of citizens, the information, technical and critical infrastructure of the country.

The rapid development of information technologies has become a significant impetus for the creation of new manifestations of security caused by the situation of a new technological level.

The division of spheres of influence in cyberspace is constantly increasing. The country's ability to protect its national interests is a priority component of every country's cyber security. The creation of cyber troops in the state will contribute to the powerful protection of the information infrastructure against possible cyber attacks, reliable protection against interference in the national information space, as well as the management of the enemy's information systems and their destruction.

The main cyber threats include violations of data integrity, unauthorized access, information confidentiality, interference with corporate or state secrets, etc. Such threats affect the functioning of any information system, the sphere of activity of a company or institution, as well as ensuring national security.

Therefore, in order to manage any dangers, it is necessary to create powerful protection against possible and potential threats with the involvement of highly qualified personnel and the use of modern software tools.

National-level issues include the identification of cyber threats, cybersecurity measures and capabilities, the development of the main indicators of cyber security, their research according to certain characteristics, and the creation of appropriate groups of cyber security indicators for the analysis and development of measures to avoid them. All government agencies and private entities interact with each other to prevent and overcome negative consequences.

Since there is a war going on now in Ukraine, there is a growing need to ensure security against threats in cyberspace of the country. The priority prospects are the adoption of such strategic decisions, which would be aimed at managing the risks of the companies and strengthening their stability in terms of security. Most business leaders see cyber resilience as a business priority in their organization. Moving from cyber security to cyber resilience is an important step towards a more secure and sustainable future.

The Ministry of Digital Transformation of Ukraine and the State Service of Special Communications and Information Protection of Ukraine are conducting work on strengthening protection against cybercrime through updating and reforming the legislative

DOI: https://doi.org/10.53486/escst2023.18
International Conference, December 07-08, 2023, Chișinău, Moldova

framework, improving the mechanism of cyber protection of state authorities, their information and telecommunication systems, conducting an analysis of the condition of cyber protection of state information resources and critical information infrastructure [4].

It is worth mentioning that the modern development of digital technologies is much faster and contributes to the spread of cybercrime. Therefore, the existing regulatory legislation, which is aimed at regulating this type of crime, needs constant improvement.

CONCLUSIONS

Thus, in the conditions of military aggression of russia in Ukraine, the current national information space of our country is not sufficiently protected from negative informational influences and threats. Therefore, the protection of information sovereignty, the creation of a powerful and effective information security system of Ukraine, countering cyber attacks and threats are strategic tasks of the state.

Therefore, at the state level, the current legislation should be improved in the direction of strengthening the legal support for the protection of national information security, in the field of cyber security and cyber protection, through fruitful cooperation with the divisions of the leading countries of the world.

BIBLIOGRAPHY

1. RYBALCHENKO L., KOSYCHENKO O., KLINYTSKYI I. Ensuring economic security of enterprises taking into account the peculiarities of information security. *Scientific journal «Philosophy, Economics and Law Review»*. *Volume* 2 (1), 2022. – p. 71-81. ISSN 2786-491X
2. RYBALCHENKO L., KOSYCHENKO O. Peculiarities of using visual means of information and analytical activity in legal and law enforcement sphere. *Scientific journal «Philosophy, Economics and Law Review»*. Volume 2 (2), 2022. – p. 162-169. ISSN 2786-491X
3. RYBALCHENKO L., RYZHKOV E., OHRIMENCO S. Economic crime and its impact on the security of the state. *Scientific journal "Philosophy, Economics and Law Review"*, 1(2), (2021). – p. 67-80. ISSN 2786-491X
4. STATE SERVICE OF SPECIAL COMMUNICATIONS AND INFORMATION PROTECTION OF UKRAINE [online]. [viewed 15 october 2023]. Available from: < https://cip.gov.ua/ua >

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

CYBER SECURITY CHALENGES OF PROTECTING SMART CITIES SUSTAINABILITY

Krasimir SHISHMANOV

PhD, Professor,
D. A. Tsenov Academy of Economics, Bulgaria,
ORCID 0000-0001-9874-2149
E-mail: k.shishmanov@uni-svishtov.bg

Iskren TAIROV

PhD, Head Assist. professor,
D. A. Tsenov Academy of Economics, Bulgaria,
ORCID 0000-0002-2971-5451
E-mail: i.tairov@uni-svishtov.bg

Abstract: *Smart cities provide many positive implications that aim at transforming the everyday lives of individuals. This includes enhancing profitability, lowering expenses, and lowering ecological impact, but the smart city concept remains in its infancy. Considering the system mostly relies on electronics, it lets the entryway to hacking attempts and criminals, which might lead to serious harm and potential dangers. A continuing concern is the psychological and formal aspects of smart city protection that have been the result of competing interests, extensive interconnectedness, and cultural and administrative complexities. Due the results of our review, present laws and directions are insufficient to identify the positions and responsibilities of different companies and citizens do not have the same understanding of critical safety requirements. The research carried out assessed smart cities' cyber security initiatives, with a focus on technology demands and legislative architecture. According to the analysis conclusions, the present research argued for an apparatus that comprises technical norms, managerial input, a regulatory mechanism, and conforming verification to ensure security is monitored throughout all phases in smart cities.*

Keywords: *smart cities, security, measures, deep learning.*

UDC: *004.056*

JEL Classification: *L86.*

INTRODUCTION

The concept of a "smart city" denotes the integration of current structures with established communication and information technologies with the objective of developing a seamless system of functional recreational opportunities [1]. A smart city connects physical possessions, technical infrastructure, social infrastructure, and business facilities to strengthen the city's collaborative thinking [2]. Smart cities are enormous, complicated, and technologically dependent, and they face a wide range of technical, financial, electoral, and social challenges. Some of the issues and obstacles that smart cities face are socioeconomic and technological concerns, individual ever-shifting requirements, teamwork across interested parties, easy to implement connecting, and security and stability. Smart cities provide six key components: smart governance, intelligent individuals, smart business, intelligent transportation, environment, and lifestyle [3]. Smart cities meet the needs of organizations, people, and governments by delivering appropriate and effective solutions. Urban support could be expanded in the ecological, tourism, well-being, departure, energy sectors, and home security sectors [4]. Considering the benefits of smart cities for residents, companies, the environment, etc, smart cities are subject to many

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

security concerns, making enabling sustainable growth difficult to accomplish. A dangerous action by an individual or group in a smart city may endanger the entire community [5]. That type of complex metropolis additionally poses a substantial challenge for automated court investigations.

Ensuring privacy in a smart city includes safeguarding data and the architecture against attacks and illicit activity. Suppliers seldom examine the cyber-security of smart city devices and their software. As a result, employing certain vulnerable things can lead to the connection being filled with forged information, the network being taken off, or the equipment malfunctioning as a result of infiltration [6]. Aside from information security, another issue to be worried about is the protection of individual privacy and contacts with authorities [7]. The risk of personal information breaches and a lack of security measures in smart cities might render public acceptance of these advancements difficult. Recognizing cyber security challenges and threats to citizens' privacy is the first step toward overcoming security issues in smart cities and preserving citizens' confidentiality. Individuals cannot expect a smart city to be created, carried out, and grown effectively until the aforementioned problems are addressed and appropriate solutions are offered [8].

LITERATURE REVIEW

Cyber security concerns and dangers to user anonymity in smart cities have been examined by many experts through several perspectives, among which prominent ones are included beneath.

A study highlighted the protection of infrastructure as a successful influence on data and data security in smart cities in a complete evaluation of studies linked to significant safety issues and current remedies in smart cities [9]. There exist numerous hazards and weaknesses associated with urban intelligence's physical-cyber foundation advantages. In the main physical-cyber systems, city infrastructure, involving power and water supply, roadways, structures, and so on, confronts multiple security concerns. Imaging devices, communication networks, management of building platforms, and systems for managing transportation are examples of these parts and technologies.

Another study classified privacy issues as interaction and corporate protection [10]. Eavesdropping, denial of service, fraudulent control and assaults, route incidents, identification, and subsequent usage were all hurdles to achieving privacy. Furthermore, phishing corporate security risks comprised frauds and attempts on data reliability. Other authors offered an exhaustive analysis of a smart city protection potential, highlighting safety issues and providing extensive insight into digitized smart city assessments [11]. According to city organizations, they highlighted security concerns such as smart grids, automated building integrity, aircraft security, smart automobiles, Internet of Things (IoT) sensors, and cloud infrastructure.

Authors like Arabo explored the features and difficulties of smart gadget cyber-security in linked intelligent structures [12]. He researched some of the historical details connected to the growth and need for integrating technology to offer people with various capacities and skills. Furthermore, he demonstrated that, notwithstanding their potential, these innovations are not without risks and obstacles. Lastly, he addressed cyber-security concerns with smart gadgets in linked intelligent structures. Based on the paper, the key issues confronting autonomous structures are breaches of privacy, altering corruption of information, and infection. Thing evaluated the prospects for current global smart cities, as well as the security problems and challenges in any of their major domains [13]. He

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

discussed the use of cyber security to build a smart, secure, and enjoyable city. He outlined security difficulties as well as worries that important sectors of the smart city face, such as banking, medical care, governance, power, and overall safety. Khatoun and Zeadally defined smart city design fundamentals and examined innovative smart city plans [14]. They explored multiple remedies, proposals, and norms connected to these concerns, especially after describing many security concerns and security holes in smart cities. Furthermore, they investigated the fundamental difficulties confronting smart cities through the viewpoints of smart city information security design and the privacy and security issues of various smart city components.

To guarantee cyber security and confidentiality in smart cities, some researchers suggested all three planning and execution assessments for encoding, authorization for use, verification, and firmware upgrades when carrying out fresh initiatives, traditional and safe denial in all urban infrastructure, and developing working strategies and processes for reacting to cyber attacks [15]. Cerrudo and others offered a few of the greatest viable smart city cyber-security strategies [16]. In that study, institutions were given recommendations for selecting and testing smart city-related solutions. The study focused on developing appropriate assessment and validation methodologies for picking such technologies and their associated providers. Other authors conducted a broad examination of existing cyber-security according to six machine-learning categories [17]. Researchers suggested prospective research topics in cyber-security. Another study from 2020 suggested a multi-view composite technique for combining the results of individual scorers [18]. The research altered an inexpensive and lazy strategy with multiple sites for searching for threats. According to Habibzadeh, smart city applications can create weaknesses in security [19]. Furthermore, removing weaknesses in security required the participation of both governmental and technology objects. Smart cities could be regarded as an instance of security. Said and Tolba developed a deep learning algorithm to forecast the efficacy of IoT communication networks using an adaptive neural net methodology for accomplishing forecasting procedures [20]. They discovered that the approach was having a considerable beneficial effect on sustaining smart cities and avoiding IoT network faults. Khan and others proposed a deep learning-based solution for transportation data projection and integration [21]. The findings revealed an improvement in precision, duration, and mistakes. Ghiasi and others investigated the Hilbert-Huang shift method for identifying fake data insertion attempts on the small scale [22]. The work they conducted relied on blockchain database technology and the study of electricity and electricity signals in sensors. Researchers discovered that the suggested approach might improve data interchange confidentiality in the network while also providing a more precise and reliable identification mechanism.

Other researchers used a combination of a singular value decomposition and two-dimensional Fourier transforms to identify the indices of the switching surface in sliding mode controllers [23]. They additionally tested the suggested approach in several bogus information attack vectors. Studies have demonstrated that the suggested approach can shorten the identification duration of an assault. In addition, the technology they used detected attempts with 96% accuracy. The authors studied electrical system resiliency principles by introducing assessment features [24]. They also developed an optimal configuration for robust power plants in the Noorabad system. They employed the grey wolf algorithms to discover the best grid settings. The results showed that both the suggested approach and the offered modification could increase efficiency and lower grid expenses.

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chişinău, Moldova

SMART CITIES AS A CYBER CRIMES TARGET

Cities have grown more intelligent and technologically advanced in the past few decades. Recent advances in technology, in addition to quick and easy interaction, allow cities to utilize more efficiently use their own resources, save finances, and provide excellent amenities to their inhabitants [25]. Cities' struggle for investment, new inhabitants, and visitors has increased emphasis on offering an excellent standard of existence and an exciting financial picture. Authorities have determined that, while budgetary constraints, inadequate funds, and outmoded processes often pose barriers to their objectives, emerging technology can transform these obstacles into possibilities. According to Chen and others, a smart city is one that employs an infrastructure to computerize and modify governmental processes in order to improve the lives of its residents [17]. Smart Cities improve technical infrastructure by increasing the efficiency and method of urban support, lowering financial burden and resource utilization, and interacting passionately and productively with residents. With the development of smart city technology, areas such as government functions and congestion, travel, water, power, wellness, and garbage disposal have grown by implementing Intelligent parking detectors, organized health monitoring, immediate noise in cities visualization, traffic management, sector optimizing, and automated illumination are examples of such devices based on the Internet of Things concept (IoT) [26]. Cloud computing, on the other hand, is an evolving framework for collecting and deciphering central smart city information [27].

Considering the essence of smart cities, it should be noted that urban smart design could incorporate mainly smart government, smart healthcare, smart energy and smart transport.

Smart government creates benefits for long-term social output by utilizing information and communication technologies for organizing, administration, and activities at one or multi-layer levels. In a nutshell, the deployment of company procedures that utilize technological innovation in intelligent administration promotes data continuity with management and the supply of exceptional services. The following phase in e-government is smart governance able to reduce crime by boosting the state of mind, enabling a rapid and effective reaction to incidents, researching situations, and enhancing public services [28].

Smart healthcare is a healthcare system which links individuals, medical centers, and organisations by utilizing technology like wearables, the Internet of Things, and mobile devices to constantly obtain data which proactively controls the environment's demands and reacts more intelligently [29]. Medical professionals, patients, healthcare facilities, and scientific institutions are the fundamental parts of smart healthcare. Infection avoidance, tracking patients, diagnosis and therapy, administration of hospitals, wellness choices, and research in medicine are all aspects of smart healthcare. Simply linking smart gadgets to medical facilities and statistical platforms allows for surveillance from afar.

Smart energy management was formed as a result of the inability of conventional power distribution networks to meet the rising needs of populations. A smart and contemporary electrical infrastructure is required to meet the demands for stability, scaling, control, sustainable energy output, and affordability [30]. A smart energy infrastructure having technological innovations may facilitate two-way exchanges of information and currents of electricity via network units. The smart grid allows for continuous evaluation, assuring the energy transfers across the energy network and customers are optimized and additionally allows for the generation of green energy by incorporating sources of clean energy into the electrical system (on the part of both the Power Company and the consumers.

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

Smart transport makes the best use of current infrastructure and advances in technology to boost network effectiveness while also increasing automobile and passenger security and decreasing time spent travelling. To attain that objective, transportation infrastructure requires effective structures that benefit the transportation industry, as well as adequate oversight of those networks [31]. The most significant benefits of implementing smart transportation systems are reduced congestion in traffic, greater security, savings in time, decreased emissions, and improved service. This technology's important components include infraction tracking and storage frameworks, a weather condition database, a driver alert mechanism, and an automobile data scheme, as well as the convenience of rapid and accurate investigations and increased welfare benefits.

CYBER SECURITY ASPECTS IN SMART CITIES

Cities have to embrace modern technological innovations in order to get sophisticated. Each emerging technology or metropolitan infrastructure provides cyber criminals with a fresh opening. For instance, in smart roadway management infrastructure, many connections across traffic controllers and lights occur sans encoding or verification, enabling an intruder to manipulate or falsify input [32]. Denial of service via channel gridlock, mathematical floods of devices that has limited power consumption (such as smart meters), a global denial of service to a city network, or postponing a time-critical communication that can lead to prevalent interruption is one of the most serious smart grid incidents. Fraud of information from different detectors is an additional concern in the metropolitan environment; for instance, forging devices to identify floods, quakes, assaults, and other natural disasters can result in erroneous warnings and public fear. An intruder spying on personal information transmitted through an intelligent structure to a meter with sensors poses a serious threat to user confidentiality. Furthermore, a hacker fabricating an individual's persona in order to remotely manipulate construction machinery can result in a variety of losses to the user.

The smart grid's reliance on the data system undoubtedly opens itself with potential connectivity and grid technology weaknesses. Grid management systems in older electrical networks were maintained segregated to insecure settings like the Internet. Cyber assaults on the electricity network are nevertheless readily taken through the context of smart grids from various elements of the network. An intruder, for example, is not required to gain entry into protected installations or equipment (such as generators, substations, command centers, and so on) to disrupt the electric power distribution chain. A threat may conduct an assault at every point on a smart grid [33]. Illegal network penetration could result in a wide range of negative effects on the intelligent grid. These repercussions involve customer data leaks, breakdown cycles that result in major interruptions, and generating and infrastructure downtime. The smart transmission grid is a collection of cutting-edge innovations that aim to upgrade the electrical supply network by incorporating information and communication technology. The data storage architecture for smart distribution networks is made up of computer programs and datasets. To perform effectively and manage, smart grid data center applications have to interact with one another. Thousands of important pieces of technology are employed in smart grids, and all of these devices are linked to smart city networks.

Data theft is one of the most serious security issues related to smart buildings. User confidentiality is a major issue in the age of smart grids and to improve safety, operation and customer benefits, high-energy user electrical usage data is transferred from

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

consumers' smart meter systems to various smart grid organizations which compromises user confidentiality [34]. Private data concerning the person such as their energy usage habits, the kind of electricity used, when the facility is vacant or full, and so on, can be revealed. Furthermore, traces left by battery purchases are able to be exploited by various organizations such as charging infrastructure as providers to gather information about electricity automobile use and setting, infringing on consumer confidentiality. Also, the assailant may get confidential data regarding the user and infringe confidentiality by spying. An additional threat of smart structures is communication modification or repetition - a criminal could put a sophisticated building's security at risk by altering or replaying messages about measurements could be altered. Because data from measurements is utilized for an array of functions accurate information tampering can result in loss of revenue for smart grid companies and weaken the reliability of the grid. An outsider could introduce updated usage signals or replay previous expenditure information of a gadget in a smart meter and bill the consumer for power not utilized. If necessary, the client sells power to the network by placing solar panels in the structure and also exports power against the intelligent grid in a crisis by employing an electric car to defend the grid against potential overloading failures. Each message delivered through the smart grid to an intelligent structure can be modified through an assail resulting in massive amounts of smart grid outages. Actual unscrupulous user may alter the email sent from the smart meters to the electrical provider including property usage statistics and reject payment for the consumption of electricity. Adjusting communications with flexible pricing communication from the energy sector to the client results in the client getting incorrect prices and making inappropriate decisions about when to use high-consumption appliances, thereby imposing an expense on the individual and putting more strain on the distributed energy system. Furthermore, a hacker may impersonate a smart meter and report erroneous quantities of energy used to the smart grid, as well as request/enter false power signs to be sent to sources of energy and electric automobiles, or obtain messages from the smart grid. The assailant can even pose as a client and remotely operate the electrical systems in the structure causing the consumer to make the remote control error and cannot operate the considered device when an intruder impersonates it [35].

MEASURES TO SECURE CRITICAL SMART CITY RESOUCES

The majority of programs for smart cities nowadays are supplied by electrical power. Lacking power, the majority of the smart city infrastructure and businesses will be unable to function, leaving the city in darkness. As a result, protecting power sources and delivering energy is crucial for smart cities. Electricity generation can be stopped by intentionally harming the location or by interfering with the production of the electricity process. That necessitates strong safety measures to ensure that power output is not disrupted and that backup power is available in the event of an outage. Energy shipment, on the other hand, refers to power communicated by cables, converters, relays that are toggles, and power stations. As a result, cyberattacks upon any of these parts can disrupt the supply of electricity, disabling all smart city operations. Hackers have been reported to be eyeing electricity-producing plants as probable targets for attacks in order to cause huge city outages and maybe spark mass uprisings [36]. It is critical to build an extensive scheme and structure for guaranteeing power production and electricity distribution to the metropolis. Moreover, because a power supply system is highly interconnected, a chain reaction of interruptions is possible, increasing the damage of one isolated attack. That can

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chişinău, Moldova

cause widespread outages across different places. To counter these kinds of assaults, smart towns must have included durability and separation capacity.

Communication is required for smart city facilities to link cameras, detectors, servers, and other devices. As a result, connection (together with energy) is an additional lifeline for smart cities. Connectivity can take place via wireless as well as wired networks. This might also be considered as IoT security. The device, data, and connectivity privacy are all aspects of IoT security. Safety for data is provided by encoding, while network privacy is achieved through the use of lightweight protection from beginning to end transportation protocols. Current communication networks that provide fixed high-speed internet or mobile cellular networks are fairly secure, with only a few instances of connection theft. Nevertheless, for a smart city, protection criteria ought to be increased since individuals want cities with sensors to be safer than regular cities.

Many smart city software may sense, obtain, procedure, and analyze information to produce meaningful knowledge, which will then be used to develop meaningful solutions. Smart transport applications will gather vehicle, traffic, and passenger data, whereas smart-health applications may capture individuals and doctor data. No matter what smart city applications are used, data will continue to be collected as part of the smart city system and must be protected, as well as in terms of its contents and its storage. This type of data can be safeguarded in numerous ways like access control entails preventing unauthorized access to data, cryptography techniques, identification, digital certificates, confidentiality etc.

According to the EU Agency for Network and Information Security, a list of best practices for the cybersecurity protection of smart cities has been identified [37]. They are:

- use of VPNs;
- encryption of data;
- use of network intrusion detection system;
- use of physical protection;
- install access control;
- install alarms and surveillance;
- implement security policy;
- creation of activity logs;
- maintenance of backups;
- regular auditing;
- shutdown procedures.

APPLYING DEEP LEARNING FOR CYBER SECURITY CHALLENGES

Deep learning is a subset of machine learning which focuses upon the research and construction of algorithms that learn systems [38]. Within simple terms, deep learning with data processing and similar to a human seeks out certain characteristics by itself, by means of a variety of sequential sections in its framework, with the aim to build a template for selection to resolve an issue. Because there are numerous levels to consider, deep learning can uncover specific elements that exist in each of them and use them to arrive at more informed choices when addressing the challenge. Deep learning is based on the continuous discovery and exploration of complicated databases. Learning is accomplished by constructing computer simulations known as neural networks, or neural networks, which are motivated by the inner workings of the human brain [39]. The system in question is divided into various operating layers. Deep learning attempts to take advantage of the undiscovered design in how inputs are distributed to try to identify suitable depictions

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

through an ordered arrangement of notions that correspond to the processing levels. Having learning from unmarked data input, deep learning may now generate additional data. As a result, it has been dubbed "innovative mind". Dispute-producing systems, for instance, one of the most common deeply creating models now, can generate images of outstanding quality, enhance the appearance of images, transform pictures to written form, and be utilized in security online to mimic attacks, help healthcare evaluate cancer via more genuine tests, and have employed in an assortment of additional limitless possibilities". It is worth noting that deep learning has joined the industry after the introduction of artificial intelligence. This learning process has aided machines with intelligence in responding more readily to human requirements and wants. Typical neural network types include multilayer and cyclic networks of neurons.

The first type is a deep learning technique that accepts a source image and allocates priority to every single object/aspect in the graphic to ensure they can be identified by one another. When opposed to other classifying methods, this technique involves lesser preparation. Whereas the primary approach to filtration is designed by hand, given sufficient instruction, a network of convolutional neural networks can acquire such filter/specifications [40]. The last kind is a sort of artificial brain network that is used for speech recognition, natural language processing, and sequencing data mining. Recurrent neural networks, compared to convolutional neurons, feature an adaptive loop whereby their output, in addition to each subsequent data, goes back to the network. Because of its inbuilt recall, a neural network with recurrent may remember its prior input and use it to process an ordered set of inputs. In terms of structure, these networks of neurons are made up of a cyclical loop that avoids prior data from being deleted and keeps it in the network.

Authorities are increasingly worried about security online in the last few years. It is a typical instance of how firms operating in the European Union (EU) have been compelled to follow tight EU standards, a method that has drastically decreased incidents of data theft. Methods using deep learning have a number of intriguing applications in smart cities. Without a doubt, a learning plan provides precise discoveries once outcomes of the entirety or comparable elements of the instruction and evaluation material are included. The second study area is knowledge disposal, which involves changing or transmitting the distribution of instruction and evaluation from a single system to another. Furthermore, researchers might look into incorporating linguistic networks into smart city applications to improve efficiency.

CONCLUSIONS

In this research, confidentiality and cyber-security in smart cities were investigated. The field of smart city network safety is nevertheless in its early days, with many rules, structures, goals, and technological advancements related to this critical subject. A review of the smart city security literature discovered that several studies provide useful assistance for politicians with city administrators seeking to more efficiently create and carry out smart city objectives and operations plans. Other research projects have outlined the conceptual framework of the deployment and evaluation of IoT in smart cities in order to give a framework for evaluating and testing proposals on a wide scale underneath real-world settings, but only a few have researched cyber security and confidentiality. People in the smart city noted an important research deficit in this field. Protection encompasses illegal data entry as well as actions, which interrupt accessibility to facilities. Considering the expansion of human populations and technological advancements in cities, sophisticated

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

methods of administration that leverage cutting-edge platforms and technologies in order to make urban infrastructure smarter are essential. Smart cities are an emerging form of technological and technological combination. The rate of assaults and vulnerability will rise as systems are linked and integrated. On the contrary hand, as additional information emerges involving the movements and behaviors of digital people, anonymity will become more insecure. As a result, it is critical to create strategies which concentrate on long-term cyberspace safety and danger reduction techniques. The analysis conducted in the current investigation revealed that overcoming these difficulties requires a great deal of administrations, software and hardware makers, and organizations delivering information technology safety services. Furthermore, creating adaptable systems with outstanding knowledge security capacities is critical to preventing major safety catastrophes, which can result in devastating monetary info, loans, including confidence losses. Because technological concerns or dangers to users' confidentiality are not just as significant in the context of smart cities, and relevant organizations and governments have a limited ability to react to their ears, further research should include an assessment and grading method.

BIBLIOGRAPHY

1. ALDAIRI, A., TAWALBEH, L. Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*. 2017, (109), 1086-109. ISSN: 1877-0509
2. ALIBASIC, A., JUNAIBI, R., AUNG, Z., WOON, W, L., OMAR, M., A. Cybersecurity for Smart Cities: A Brief Review. In: *Data Analytics for Renewable Energy Integration*. Riva del Garda, Italy, September 23, 2016, 22-30.
3. ARABO, A. Cyber Security Challenges within the Connected Home Ecosystem Futures. *Procedia Computer Science*. 2015, (61), 227-232. ISSN: 1877-0509
4. BAIG, Z., A., SZEWCZYK, P., VALLI, C., RABADIA, P., HANNAY, P., CHERNYSJEV, M., JOHNSTONE, M., KERAI, P., IBRAHIM., A., SANSUROOAH, K., SYED, N., PEACOCK, M. Future challenges for smart cities: Cyber-security and digital forensics. *Digital Investigation*. 2017, (22), 3-13. ISSN: 2666-2817
5. BJORNER, T. The advantages of and barriers to being smart in a smart city: The perceptions of project managers within a smart city cluster project in Greater Copenhagen. *Cities*. 2021, (114). ISSN: 1873-6084
6. CERRUDO, C., RUSSEL, B. Cloud Security Alliance. Cloud Security Alliance. 2015
7. CHATFIELD, A., K., REDDICK, C., G. A framework for Internet of Things-enabled smart government: A case of IoT cybersecurity policies and use cases in U.S. federal government. *Government Information Quaretrly*. 2019, (2), 346-357. ISSN: 1872-9517
8. CHEN, D., WAWRZYNSKY, P., LV, Z. Cyber security in smart cities: A review of deep learning-based applications and case studies. *Sustainable Cities and Societe*. 2021, (66), 2210-6715. ISSN: 2210-6707
9. CHEN, Z. Application of environmental ecological strategy in smart city space architecture planning. *Environmental Technology & Innovation*. 2021, (23). ISSN: 2352-1864
10. DEHDARIAN, A., TUCCI, C., L. A complex network approach for analyzing early evolution of smart grid innovations in Europe. *Applied Energy*. 2021, (298). ISSN: 1872-9118
11. DEHGHANI, M., NIKNAM, T., GHIASI, M., SIANO, P., ALHELOU, H., H., AL-HINAI, A. Fourier Singular Values-Based False Data Injection Attack Detection in AC Smart-Grids. *Applied Sciences*. 2021, (11).

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

12. FARD, S., M., H., KARIMIPOUR, H., DEHGHANTANHA, A., JAHROMI, A., N., SRIVASTAVA, A. Ensemble sparse representation-based cyber threat hunting for security of smart cities. *Computers & Electrical Engineering*. 2021, (88), 1879-0755. ISSN: 1873-2046
13. FENG, W., WEI, Z., SUN, G., ZHOU, Y., ZANG, H., CHEN, S. A conditional value-at-risk-based dispatch approach for the energy management of smart buildings with HVAC systems. *Electric Power Systems Research*. 2020, (188). ISSN:1873-2046
14. GHIASI, M. DEHGHANI, M., NIKNAM,T., KAVOUSI-FARD, A., SIANO, P., ALHELOU, H., H. Cyber-Attack Detection and Cyber-Security Enhancement in Smart DC-Microgrid Based on Blockchain Technology and Hilbert Huang Transform. *IEEE Access*. 2021, (9), 29429-29440.
15. GHIASI, M., DEGHANI, M., NIKNAM T., BAGHAEE, H., R.,PADMANABAN, S., GHAREHPETIAN, G., B., ALIEV, H. Resiliency/Cost-Based Optimal Design of Distribution Network to Maintain Power System Stability Against Physical Attacks: A Practical Study Case. *IEEE Access*. 2021, (9), 43862-43875.
16. HABIZAHEH, H., NUSSBAUM, B., H., ANJOMSHAA, F., KANTARCI, B., SOYATA, T. A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Societe*. 2020, (50). ISSN: 2210-6715
17. HASBINI, M., AYOUB, R., TOM-PETERSEN, M., FALLETTA, L., JORDAN, D., SEOW, A., SINGH, S. Smart Cities Cyber Security Management. *Securing smart cities*. 2017
18. IJAZ, S., SHAH , M., A. KHAN, A., AHMED, M. Smart Cities: A Survey on Security Concerns, *(IJACSA) International Journal of Advanced Computer Science and Applications*. 2016 (7), 612-624. ISSN : 2156-5570
19. JEONG, H., H., SHEN, Y., C., JEONG, J., P., OH, T., T. A comprehensive survey on vehicular networking for safe and efficient driving in smart transportation: A focus on systems, protocols, and applications. *Vehocular Communications*. 2021, (31). ISSN: 2214-210X
20. KASHEF, M., VISVIZI, A., & TROISI, O. Smart city as a smart service system: Human-computer interaction and smart city surveillance systems. *Computers in Human Behavior*. 2021, (124). ISSN: 1873-7692
21. KHAN, S., NAZIR, S., MAGARINO, I., G., HUSSAIN, A. Deep learning-based urban big data fusion in smart cities: Towards traffic monitoring and flow-preserving fusion. *Computers & Electrical Engineering*. 2021, (89). ISSN: 1873-2046
22. KHATOUN, R. S. Smart cities: Concepts, architectures, research opportunities. *Communications of the ACM*. 2016, (58), 46-57.
23. KOURGIOZOU, V., COMMIN, A., DOWSON, M., ROVAS, D., MUMOVIC, D. Scalable pathways to net zero carbon in the UK higher education sector: A systematic review of smart energy systems in university campuses. *Renewable and Sustainable Energy Reviews*. 2021, (147). ISSN: 1879-0690
24. LEBRUMENT, N., LEBRUMENT C., Z., ROCHETTE, C., ROULET, T. Triggering participation in smart cities: Political efficacy, public administration satisfaction and sense of belonging as drivers of citizens' intention. *Social Change*. 2021, (171).
25. LEE, K., SILVA, B., N., HAN, K. Algorithmic implementation of deep learning layer assignment in edge computing based smart city environment, *COMPUTERS & ELECTRICAL ENGINEERING*. 2021, (89). ISSN: 1879-0755
26. LI, P., LU, Y., YAN, D., XIAO, J., WU, H. Scientometric mapping of smart building research: Towards a framework of human-cyber-physical system (HCPS). *Automation in Construction*. 2021, (129). ISSN: 1872-7891

DOI: https://doi.org/10.53486/escst2023.19
International Conference, December 07-08, 2023, Chișinău, Moldova

27. LIU, L., ZHANG, Y.Smart environment design planning for smart city based on deep learning. *Sustainable Energy Technologies and Assessments*. 2021, (47). ISSN: 2213-1396
28. MARAHATTA, A., RAJBHAMDARI, Y., SHRESHTA, A., SINGH, A., GACHHANDAR, A., THAPA, A. Priority-based low voltage DC microgrid system for rural electrification. *Energy Reports*. 2021, (7), 43-51. ISSN: 2352-4847
29. MARUF, M., H., HAQ, M.A., DEY, S.,K., MANSUR, A.A., & SHIHAVUDDIN, A.S.M. Adaptation for sustainable implementation of Smart Grid in developing countries like Bangladesh. *Energy Reports*. 2020, (6), 2520-2530. ISSN: 2352-4847
30. QUAYYM, S., ULLAH, F., TURJMAN, F.,A., MAJTAHEDI, M. Managing smart cities through six sigma DMADICV method: A review-based conceptual framework. *Sustainable Cities and Societe*. 2021 (72). ISSN: 2210-6707
31. RAZMJOO, A., OSTERGAARD, P.A., DENAI, M., NEZHAD, M., M., MIRJALILI, S. Effective policies to overcome barriers in the development of smart cities. *Energy research and social science*. 2021, (79). ISSN: 2214-6326
32. SAID, O., & TOLBA, A. Accurate performance prediction of IoT communication systems for smart cities: An efficient deep learning based solution. *Sustainable Cities and Societe.* 2021, (69). ISSN: 2210-6707
33. SENGAN S., VELAYUTHAM, P. RAVI, L., V. S., & V. I. Detection of false data cyber-attacks for the assessment of security in smart grid using deep learning. *Computer & Electrical Engineering*. 2021, (91). ISSN: 1879-0755
34. TEMBLEY, M., ALSUMAITI, A., M., ALAMERI, W., S. Machine and deep learning for estimating the permeability of complex carbonate rock from X-ray micro-computed tomography. *Energy Reports*. 2021, (7), 1460-1472. ISSN: 2352-4847
35. THING, V. L.Cyber security for a smart nation. In *2014 IEEE International Conference on Computational Intelligence and Computing Research*. IEEE, 2015.
36. TOFT, P., DUERO, A., BIELIAUSKAS, A. Terrorist targeting and energy security. *Energy Policy*. 2010, (38), 4411–4421. ISSN: 1873-6777
37. V. S., K., PRASAD, J., & SAMIKANNU, R. Barriers to implementation of smart grids and virtual power plant in sub-saharan region—focus Botswana. *Energy reports*. 2018, (4), 119-128. ISSN: 2352-4847
38. VITUNSKAITE, M., HE, Y., BRANDSTETTER, T., JANICKE, H. Smart cities and cyber security: Are we there yet?A comparative study on the role of standards, third party risk management and security ownership. *Computers & Security*. 2019, (83), 313-331. ISSN: 1872-6208
39. WANG, W., HUANG, H., XIAO, F., LI, Q., XUE, L., JIANG, J. Computation-transferable authenticated key agreement protocol for smart healthcare. *Journal of Systems Architecture*. 2021, (118). ISSN: 1873-6165
40. ZHOU, X., LI, S., LI, Z., LI, W. Information diffusion across cyber-physical-social systems in smart city: A survey. *Neurocomputing*. 2021, (444), 203-213. ISSN: 1872-8286

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.20
International Conference, December 07-08, 2023, Chişinău, Moldova

THE IMPACT OF MARTIAL LAW ON THE ORGANIZATION'S INFORMATION SECURITY

Yuliia SYNYTSINA

PhD, Associate Professor
Dnepropetrovsk State University of Internal Affairs, Ucraine
ORCID 0000-0002-6447-821X
E-mail:ysynytsina0@gmail.com

Abstract: *The article examines the problem of the development of information and analytical activity (IAD) in domestic state and commercial institutions, which leads to the constant improvement of information security issues, which in turn is closely related to issues of economic security. Based on the results of the study, the analysis model was clarified and the practical aspects of the application of neural networks (NN) in the marketing information system (MIS) of the enterprise were clarified with the aim of improving the information system of the enterprise by implementing an intelligent decision support system (IDSS) using a neural network, as well as the concept of modeling the behavior of interacting agents, the basis of which is a three-level structure of modeling subjects and business processes of the contours of the organization's functioning and the security system, based on the modeling of the behavior of antagonistic agents. Modern trends and directions in the field of information security of state and commercial institutions of the present and the near future, which in one form or another use artificial intelligence in their arsenal, are defined, such as EDR / XDR solutions for end hosts, UEBA, SGRC products, Honey Tokens and other developments of the Deception class, IRP (Incident Response), TI- / TH-platforms, etc.*

Keywords: *Artificial Intelligence, Information Technology, informational security, economic security.*

UDC: *004.056:004.8*

JEL Classification: *K24, F52.*

INTRODUCTION

The rapid development of information and analytical activity (IAA) in domestic state and commercial institutions has become a characteristic trend in recent times. Its implementation is driven by certain objective factors: on the one hand, it is the democratization of social life, the development of market relations, legitimacy, the rapid development of entrepreneurial activity; on the other hand, the increasing importance of the intellectual component in decision-making in the management of social spheres, as well as the growing flow of information necessary for decision-making and the implementation of other types of social activities.

The development of information and analytical activity (IAA) in domestic state and commercial institutions leads to continuous improvement of information security issues, which is closely related to issues of economic security. The specifics of information security issues are also closely linked to the constant development of information technologies. Information technologies that incorporate modern methods of applying artificial intelligence to determine current information and economic threats are of particular importance.

The development of artificial intelligence (AI), data science, and machine learning systems already allows humanity to do what was previously only imaginable: image and speech recognition, personal identification, making complex decisions, predicting human behavior, autonomous vehicle control, and building universal routes, among other things.

DOI: https://doi.org/10.53486/escst2023.20
International Conference, December 07-08, 2023, Chișinău, Moldova

Digitization, as the digital transformation of everyday things, has become so ingrained in our lives that in 2001 a new indicator of the level of development of countries in the world was introduced – the Networked Readiness Index (NRI), which is designed to characterize the degree of development of information and communication systems of a country and is an important indicator of its development and investment prospects.

Therefore, the question of the application of artificial intelligence as a tool for information security in state and commercial institutions is currently relevant.

PAPER BODY

Over the past few years, IT technologies have been actively integrated into the business information security infrastructure. Last year, the global market volume of artificial intelligence technologies in information security reached $8 billion USD. By 2025, the growth of this industry is expected to reach $30 billion USD. This is not surprising, as most solutions in the field of information security are somehow based on artificial intelligence. Virtually any traditional antivirus utilizes some capabilities from the realms of machine learning and big data. It is no longer just local comparison of a suspicious file with the antivirus database of malware signatures. Behavioral analysis is also employed, capable of detecting dangerous objects whose signs are absent in the antivirus database, along with other advanced technologies.

Significant contributions to the study of legal issues related to the application of artificial intelligence have been made by O.A. Baranov, V.M. Bryzhko, K.S. Melnyk, V.G. Pylypchuk, and others. The role and place of artificial intelligence in the field of criminal law relations have been highlighted in the works of V.A. Myslivyi, M.V. Karchevskyi, and N.A. Savinova. However, with each restrained step of scientific research, even greater horizons of boundless reality cognition are revealed.

The principles and tasks of developing artificial intelligence technologies in Ukraine are one of the priority directions in the field of scientific and technological research. The goal of the Concept is to define the priority areas and main tasks for the development of artificial intelligence technologies to satisfy the rights and legitimate interests of individuals and legal entities, build a competitive national economy, and improve the public administration system. Ukraine, being a member of the Special Committee on Artificial Intelligence at the Council of Europe, joined the Organization for Economic Co-operation and Development (OECD) Recommendations on Artificial Intelligence (OECD/LEGAL/0449) in October 2019. The main task in the field of cybersecurity during the implementation of the state policy for the development of the artificial intelligence industry is to protect communication, information, and technological systems, information technologies, especially those used by operators (providers) of key services (including critical infrastructure objects) that are essential for the continuity of the state, society, and the safety of citizens [1]. The application of artificial intelligence technologies in ensuring information security is one of the factors that will contribute to safeguarding national interests. Specifically, monitoring social networks and online media resources using AI technologies allows for the detection of systemic trends and issues, proactive action, and analysis of target audiences.

- To achieve the goal of the Concept in this area, the following tasks should be ensured:
- Formation and use of an information resource, ensuring high rates of its content and specified criteria of quality (accessibility, reliability, timeliness,

DOI: https://doi.org/10.53486/escst2023.20
International Conference, December 07-08, 2023, Chişinău, Moldova

completeness).

- Creation of a secure national information space using artificial intelligence technologies.
- Detection, prevention, and neutralization of real and potential threats related to the dissemination through mass media of cultural elements of violence, cruelty, pornography, attempts to manipulate public consciousness, including through the spread of inaccurate, incomplete, or biased information.

The application of neural networks in an intelligent decision support system at an enterprise is described in the work [2, 3]. Based on the research results, a model of analysis was formulated, and practical aspects of applying neural networks (NN) in the marketing information system (MIS) of the enterprise were considered with the aim of improving the enterprise's information system through the implementation of an intelligent decision support system (IDSS) using a neural network [2, 3]. Currently, the foundation of existing DSS lies in artificial intelligence methods. The creation of an intelligent DSS became a natural extension of the widespread use of classical DSS. Intelligent DSS provides information support to all production processes and safety processes in the conditions of state and commercial organizations and institutions.

The authors of the work [4] propose a Concept for modeling the behavior of interacting agents, the basis of which is a three-level structure for modeling the subjects and business processes within the functioning contours of the organization and security system. This concept relies on modeling the behavior of antagonistic agents. The methodology for modeling the behavior of interacting agents, based on the Concept of antagonistic agent behavior, allows for the evaluation and enhancement of security levels by reducing the implementation of hybrid threats by 1.76 times. This results in a reduction of losses by 1.65 times and an increase in the time for selecting resistance tools by reducing the identification time of threats in online mode by 38%.

In summary, all methods and solutions can be divided into external, which analyze user actions and events outside the organization's protective perimeter, and internal, which analyze events and user behavior within the organization. Both external and internal methods currently extensively utilize machine learning, big data processing, and artificial intelligence. Systems similar to those described above are critically important for many industrial enterprises, insurance, banking, and financial companies, as well as numerous critical government institutions.

The use of artificial intelligence and machine learning typically involves connectivity both within a local network and over the Internet. Consequently, these technologies cannot be applied in situations where the probability of external attackers connecting needs to be minimized, such as in critical objects of the energy infrastructure or defense production. Regarding businesses, artificial intelligence technologies are essential for both governmental and commercial institutions dealing with large volumes of data, thousands of transactions, and tens of thousands of users. It's important to note that implementing machine learning and artificial intelligence technologies within small businesses may not always be justified. Also, it's crucial to recognize that artificial intelligence is not a panacea but an additional element in the overall toolkit of information security professionals. Simply connecting an artificial intelligence service to a security system does not solve all problems, and the final decision-making authority still rests with the information security expert.

DOI: https://doi.org/10.53486/escst2023.20
International Conference, December 07-08, 2023, Chişinău, Moldova

CONCLUSIONS

In conclusion, it is worth noting that there are currently numerous trends in the application of artificial intelligence for the protection of information systems, and the relevance of many of them will actively grow in the near future. The significant shift of a vast number of people to remote work during the ongoing pandemic and military actions in Ukraine makes a substantial contribution to the development of artificial intelligence application in optimizing information security in both governmental and commercial institutions. Many organizations find themselves having to restructure information security processes and utilize new tools for the recognition of "friend or foe." The workload on information security departments in various governmental and commercial institutions is gradually increasing, indicating that additional tools, including those based on artificial intelligence, are necessary. The risks in the context of a "blurred perimeter" become significantly higher.

When discussing trends and directions in the field of information security for current and near-future use in governmental and commercial institutions, which incorporate artificial intelligence in one form or another, these include EDR/XDR solutions for end hosts, UEBA, SGRC products, Honey Tokens, and other Deception class developments, IRP (Incident Response), TI/TH platforms, etc. There is a significant variety of solutions and directions, and it is crucial to apply them wisely and consciously.

BIBLIOGRAPHY

1. ON THE APPROVAL OF THE CONCEPT OF THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE IN UKRAINE: [online] order of the Cabinet of Ministers of Ukraine dated 02.12.2020 No. 1556-r // Cabinet of Ministers of Ukraine: official. site [viewed 01 december 2023]. Available from: <https://www.kmu.gov.ua/npas/pro-shvalennya-koncepciyi-rozvitku-shtuchnogo-intelektu-v-ukrayini-s21220>
2. SYNYTSINA , Y., ABRAMOV, S., MANOLE A. Improving the information system of the enterprise through the use of neural networks. *Philosophy, economics and law review Dnipropetrovsk State University of Internal Affairs.* [online] 2022. 2(1). 127 – 138. DOI: 10.31733/2786-491X-2022-1-127-138 [viewed 01 december 2023]. Available from: <https://phelr.dduvs.in.ua/wp-content/uploads/files/2_1/Pherl-2%2C%201%202022-127-138.pdf>
3. SYNYTSINA, Y., KAUT, O., FONAREVA, T. Intelligent decision support systems in the enterprise management process. *Infrastruktura rynku*, [online] 2019. 32. [viewed 01 december 2023]. Available from: <http://www.market-infr.od.ua/journals/2019/32_2019_ukr/32.pdf>
4. MILOV, O. et al. Development of the space-time structure of the methodology for modeling the behavior of antagonistic agents of the security system. *Eastern-European Journal of Enterprise Technologies*. [online] 2020. 6(2). 30-32. DOI: 10.15587/1729-4061.2020.218660 [viewed 01 december 2023]. Available from: <https://www.scopus.com/record/display.uri?eid=2-s2.0-85104142498&origin=resultslist>

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

AGILE TRANSFORMATION AND PERFORMING MANAGEMENT OF IT AND CYBER SECURITY PROJECTS, AT THE GOVERNMENT LEVEL

Marius ȘTEFAN

PhD student,
Doctoral School of Economic Informatics,
Bucharest University of Economic Studies, Romania,
ORCID 0000-0002-4967-6234
Email: marius.stefan@mfe.gov.ro

Abstract: *In an information society in which the quality of life, as well as the prospects for social change and economic development, depend to a greater extent on information and its exploitation, the institutional field of management of IT applications for European funds becomes a matter of national importance, with critical values for national security. Reinventing government can be achieved through digitalization and government computerization, which involves modernizing the current IT infrastructure through specific external funding sources such as European funds, doubled and secured by advanced cyber protection and defense capabilities against possible vulnerabilities or cyber-attacks.*

Knowledge and scientific information are of enormous importance in the global information society, by: supporting innovation, promoting economic development, making decisions in an efficient and transparent way, at the governmental level and especially for the implementation and use of intelligent technologies in the development of the degree of digitization of public services through financing provided by European funds and the National Recovery and Resilience Plan.

In order to move on to building the knowledge society, it is necessary to reduce the digital gap, which accentuates disparities in development, excluding groups and even countries, from the benefit of information and knowledge. The limiting factor in development will be related to the human capacity to assimilate and develop these technologies, to use them in new fields of activity, for new products and services.

Keywords*: synergy in innovations; intelligent technologies; e-business; digital transformation; cyber security awareness; agile transformation; automation of repetitive processes.*

UDC: *[004.056:005.8]:338.246.2(498)*

JEL Classification: *D83, L86, K22, M16, M21.*

INTRODUCTION

This will produce a re-classification of knowledge, so that the model of access to knowledge undergoes changes, the primary interest is no longer directed towards the universal aspect, the concern becomes centered on the local space, introducing migration from the word. to image, from speech to personality.

Postmodernist discourses thus speak of a multitude of local realities or of a global reality, or even of the lack of a reality, in conditions where an ideology can no longer convince large masses of individuals, as a fragmentation takes place at the level of the subdivided currents that are found in many local realities, in one it was marked by conflicts but not by struggle, by problems but not by contradictions, by unions but not by classes, and most importantly (by the fact that) no concrete utopia animates social movements.

Thus, through social changes, and the end of the modern world, certain major changes occur in the social life of the individual, postmodernity leading either to the emergence of a new type of society or to a new phase of capitalism, both based on two phenomena: the development of new technologies and the emergence of consumerism,

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chişinău, Moldova

crystallized as economic-social behavior. Postmodernity, this condition of the contemporary world, is defined as a term used by philosophers, social scientists, art critics, to refer to aspects of art, culture, economy or current social conditions, which are the result of features unique aspects of life in the late 20th and early 21st centuries.

Globalization, consumerism, the fragmentation of authority and the transformation of knowledge into an object of use, being included in the defining features of the postmodern condition. This is how the phrase information society appears in the specialized literature of post-industrialism, a notion that in sociology refers to a type of postmodern society, in which old norms and ways of thinking are replaced by new technologies and new lifestyles. A transformation of civilization is thus produced, leading to the information society through three scientific and technical revolutions: the traditional craft, the scientific organization of production and automation.

PAPER BODY

Starting from the growing role of science in production processes, combined with the emergence of information technologies and the need to automate repetitive processes, the economy and society become centered on the new central principle, called theoretical knowledge.

Within this computerized society, the new social context is based on telecommunications and computers, which become decisive for the way in which economic and social changes are produced, the way in which knowledge is created or recovered and the nature of work and the organizations in which people are employed.

Another relevant characteristic of the informational society is the way in which knowledge and information will replace work and capital, as central factors in the economy, IT, by shortening the actual work, diminishes the role of the individual in the production process, thus replacing work as the source of added value, within the national product.

In the information age, the information society is a society in which the quality of life, as well as the perspectives of social change and economic development, depend, to a large extent, on information and its exploitation. In such a modern society, living standards, work and leisure patterns, the educational system and the labor market are all significantly influenced by advances in information and knowledge.

In the evolution towards an informational society, where the role of informational technologies is decisive, the following major and determining criteria are followed: economic (services and informational goods); technological (telecommunications, computer and new technologies); social (information gets value); political (the flow of information and communication methods can create global realities in which individuals can be involved); cultural (the tendency to replace local culture with the so-called global economic culture).

The ambivalence of the information society, seen on the one hand as a global entity, and on the other hand as a mosaic made up of sub-societies spread around the world, is caused by electronic means of communication, which create a virtual global space, within which the notion of a foreigner loses its semantic consistency, creating a direct relationship between individuals, which will produce deterritorialization, through the creation of world markets, through the existence of a stock exchange accessible from anywhere and permanently, thus providing information about the circulation of capital in the world the whole In this way, a global environment is born, a global space structured on individual models of life.

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

Technologies produce a breakdown in local plans, by focusing attention on certain local sectors in the sphere of marketing, advertising and mass media, by resuming certain symbols and elements of culture and reaffirming local identities.

The fragmentation generated by telecommunications is seen as a hyperreal world, in which codes and digital systems are, in fact, simulations, which dissolve the individual's life. Thus we are dealing with the adaptation of the individual to information technologies or are they designed and realized in such a way as to serve the individual, the interdependence between the two actions being inherent in the process of using the technology, as well as the mastery of certain levels of knowledge, the changes continuous advances in technology, challenging and subjecting individuals to a perpetual specialization and discovery of ways of change and innovation.

The new environment of humanity is not so much hardware or physical, its essential poses are information and coded data configurations, which more quickly gives a software image to the environment, identifiable at all levels of the individual's life.

The use of intelligent technologies will result in the development of the degree of digital culture and cyber security, among civil servants, in the economic-social-political-post-pandemic context for e-business, as a result of changing the traditional work style by adopting the new methods developed through new emerging technologies.

The use of intelligent technologies will result in the development of the degree of digital culture and cyber security, among civil servants, in the economic-social-political-post-pandemic context for e-business, as a result of changing the traditional work style by adopting the new methods developed through new emerging technologies.

The Ministry of Investments and European Projects, in cooperation with institutional partners, is the main developer of the national IT exchange program between Romania, as an EU member state, beneficiary of non-reimbursable European funds, and the European Commission, according to the provisions of REGULATION (EU) NO. 1303/2013 of the European Parliament and of the Council of 2013.

The implementation of ensuring the security of the cyber infrastructure intended for the management of European funds, was and will be conditioned by a cooperation with the institutions that have the necessary expertise in the field, thus realizing the premises of some strategies, in accordance with the European legislation in force and transposed into projects financed from European funds , aimed at ensuring cyber security, as well as increasing the level of awareness of the importance of the state of security at the governmental level:

- project code - SMIS 48723 – Titeica 1 - The national system for the protection of IT&C infrastructures of national interest against cyberspace threats, financed by the Sectoral Operational Program for Increasing Economic Competitiveness 2007 - 2013.
- project code - MySMIS 127221 – Titeica 2 - Updating and developing the national system for the protection of IT&C infrastructures with critical valances for national security against threats from cyberspace", financed by the Competitiveness Operational Program 2014-2020. (ICIN\IVC 54 MIPE - project with national coverage, and the implementation period according to the financing contract - 23.08.2019 - 23.08.2022, with related maintenance services and support for applications and equipment until 23.08.2027).
- the Titeica 3 project - will be implemented through PNRR by the National Cyberint Center, intended for the development of the national cyber protection

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chişinău, Moldova

system, included in Component C7, Digital Transformation, through the National Recovery and Resilience Plan - resulting in the expansion of the protection area. of the Information Technology and Operational Technology infrastructures, as a beneficiary entity of cyber security and protection, as well as participation in training programs organized in the field of cyber security.

The objectives of the MIPE cyber security projects, being the updating and development of existing IT systems by including them in the national system, of new IT&C infrastructures with critical values for national security, in order to increase the capacities to identify possible cyber -attacks, as well as to increase the national level of ensuring cyber security, subject to a common approach of national and EU policies in the field of cyber security and interoperability, I sell the transition to a Government cloud as desirable.

Through the results obtained, the projects aim at increasing the cyber security of IT and communications services at the national level, increasing the availability and level of security offered to institutions and entities of public interest by modernizing the security systems related to the existing IT systems. Within the organizations, emphasis will be placed on achieving the interoperability of the security systems to be implemented and integrated, in terms of corroborating information, collaboration, analysis and reaction through the IT mechanism for rapid alerting and disseminating information in real time, thus obtaining effective results in a timely manner.

The outline of a national system of prevention and protection against cyber-attacks, through cyber defense activities, will create the premises for the development of innovation and the use of intelligent technologies, at the government level, with the aim of eliminating repetitive processes through automation and artificial intelligence. The operation in parameters that do not correspond to the performance, of the applications intended for the management of European funds, will generate a vulnerability, manifested in the decrease in the level of absorption of European funds, with implications in the national economy, constituting a real threat to the national security of Romania, due to the economic-financial repercussions , as well as social-political regarding the obligations assumed by Romania, from the perspective of the membership status of the European Union.

The national system of prevention and protection against cyber-attacks, through cyber defense activities, having a beneficial role in the implementation of the new National Cyber Security Strategy and in ensuring Romania's compliance with the commitments assumed at the international level, including those related to the implementation of the Cyber Security Strategy EU Cybersecurity, the NIS Directive and NIS 2.0, as well as in the activity of the European Center for Industrial, Technological and Research Competence in Cyber Security (ECCC) established in Bucharest.

In the undesirable situation of the blockage in this critical area of the national economy, constituted by the field of attracting European non-reimbursable funds, the balance specific to the state of national security will be restored by informing the competent minister as quickly as possible, as well as by adopting the appropriate measures to remedy the identified deficiencies.

Thus eliminating the risk of disengagement, through an automated and efficient management of European funds, fulfilling a better management of an objective of national strategic interest. The realization of national interests, as well as the acts of economic destruction, degradation or decommissioning of the structures necessary for the proper development of life and its quality, can constitute threats - even through the existence of a state of blocking the absorption of European funds, framed from the point of view of

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

information for national security, in the provisions of Chapter 3 related to the National Defense Strategy 2015-2019/National Defense Strategy of the country for the period 2020-2024, and art 3, letter f, Law 51/91.

In this newly developed branch of the national economy, represented by the field of European funds, the countering of these possible risks will be realized gradually, due to a high degree of persistence manifested, including through the lack of the necessary resources, as well as the necessary specialization in the efficient management of IT systems, located in continuous development, the focus being oriented towards the results obtained and efficiency in the creation of public values, including at the level of the national cyber critical infrastructure.

Impediments encountered in the functioning of the gear that is the basis of attracting funds, will bring damage both to the national budget and to the image at the community level, interoperability being a basic principle of the member states, necessary in the expected evolution process through transformation, reinvention and digitization.

Non-compliance with the obligations assumed as a member state can cause economic failures, manifested in the development of society and the increase of the quality of life depending on the evolution in the management of current financial resources and for the future, through the membership of the European Union and its specific financial exercises.

The analysis carried out on these aspects of national interest has an incidence in the current year - 2023, a favorable moment for cyber-attacks that are characterized by frequency and persistence, making it vital that both state and private organizations are armed with the most effective tools and knowledge of cyber security, to prevent, detect and respond to threats encountered. Permanent vulnerabilities will always escalate into possible threats materializing in future risks to national security. Thus, awareness through prevention being the most effective strategic approach of a governmental organization such as the Ministry of European Investments and Projects.

In the international geopolitical context, of the situation between Russia and Ukraine, a considerable increase in the number of attacks, registered in the virtual environment, on public institutions considered to be targets, by cyber attackers, was observed, thus making it imperative to ensure the cyber protection of workstations and mobile devices within MIPE - through the centralized administration of an anti-virus type solution, completing the purchases related to the project carried out in the Cooperation Agreement with Cyberint: Titeica 2 - Updating and developing the national system for the protection of IT&C infrastructures with critical valences for national security against cyber threats.

Ensuring the state of balance and security is increasingly important among organizational concerns, in the context of the exponential increase in the number and complexity of cyber threats (malware/ransomware/social engineering in particular). Deficiencies found in the development solutions, hardware and software used, as well as the lack of an appropriate modernized infrastructure, dedicated to the national IT system, can cause malfunctions in the electronic services offered to beneficiaries and the business environment in the process of developing future electronic business solutions.

As an area of application, the IT system acquires importance at the national level, but it can also slow down certain processes in the economy, such as the annual preparation of the national budget.

The inclusion of interoperability requirements in the relationship with the European Commission requires a clear focus on functional and secure reporting processes, automation of repetitive processes, increased processing of documents in electronic format,

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

and signing with digital certificates. The concentration of resources can only provide solutions under safe operating conditions, ensured by a balance specific to the state of cyber security.

In the national strategy for alignment with European standards, including harmonization with European provisions, this may constitute a vulnerability in the proper functioning of the activity, in the context of increasing rigors/requirements regarding interoperability in the EU.

It is necessary to ensure compliance with the requirements of the NIS2 European Directive and Law 362/2018 - regarding the wave of digital information that must be managed and controlled by technical security measures, as well as Law no. 3652/2018, which transposes the European NIS Directive, and regulates the necessary framework for developing the level of preparation of EU states to deal with possible incidents that may affect IT security.

The EU NIS (Network and Information Systems) Directive 2016/1148 is an essential legal piece launched at the EU level to increase the level of cyber security for critical infrastructure units, including critical infrastructure entities in the fields of utilities, transport, healthcare and digital services, as well as European funds. Establishing a set of principles and rules to define, measure and improve cyber security.

Given the expansion of cyber-attacks, compliance with the requirements of the NIS Directive is imperative. A cyber security strategy based exclusively on prevention is not enough, finding a need for maximum involvement, through rapid detection and use of effective emerging solutions.

An unforeseen attack on a critical cyber infrastructure of national interest, such as that intended for European funds, can occur as a result of security risks not properly treated, with possible results, data leaks, through exfiltration, or by causing syncope in operation, even leading to interruptions in the operation of essential and critical services for the national infrastructure.

According to current and long-term trends, the main frequent threats that should be monitored in an organization are malware and phishing attacks, especially in a government institution such as the Ministry of Investments and European Projects, representing a real area of interest for groups of cyber-crime, for the purpose of espionage activities or theft of strategic information, such as government information.

The measures implemented regarding the awareness of the importance of the activity of ensuring cyber security, especially among specialized personnel and intended for ICT activities as well as public officials, require preparation for combating the risks that the public institution will face, starting from the up-to-date software components according to security standards, and up to e-learning sessions on defense tactics in the cyber environment at the user level.

Adapting to periods with frequent technological changes, or decision-making in moments of calm observed in the governance process, can constitute vulnerabilities in terms of ensuring the necessary balance in the organization.

The behavior manifested in situations such as the loss or lack of administration credentials, access to work environments created through electronic tools, can create certain impediments in the process of administering the cyber security component.

Most of the time, political management changes within the institutional framework are also reflected in the specific activities of technical departments such as ITC, by slowing

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

down the decision-making and construction process, not representing a good institutional practice, especially in the case of ensuring cyber security.

The progress registered in the development of new technologies will establish the desire to align with the new standards of the future, through the use of new solutions such as the private or hybrid cloud, which will be adopted at the governmental level, from the point of view of budget efficiency, but especially for specific considerations of the cyber security component.

Through the analysis of the vulnerabilities described, we find the need to establish within the organization a specific post of cyber security administrator. He will have to possess the necessary specialization in the field, through certified resources in the field of Cyber Security with an emphasis on specific activities such as - National Security Information Management.

At the level of the Ministry of Investments and European Projects, this measure is being implemented, a first step, by signing the Cooperation Agreement, between MIPE and Cyberint, through a national level project of critical cyber infrastructure - ICIN\IVC 54 MIPE, linked to the structures of the European funds and the national critical infrastructure, succeeding in the unification through cyber security solutions of the majority of state institutions of national strategic importance.

The response to Cyber Security incidents, as an activity, requires the existence of its own specialized staff, through a Security-Operation-Center type team, specific to such situations, by nomination and inclusion in the Security Structure of MIPE, being extremely useful public institution, including in situations of cooperation with authorized authorities in the field of cyber defense. Awareness and training in cyber security is very useful within the organization, especially among users - public officials, promoting the use of solutions to protect them from incidents, respecting the regulations related to their own password, which should comply with certain current security standards.

Raising awareness of the importance of ensuring cyber security measures will be achieved by informing users, being the first measure of protection against increasingly frequent cyber-attacks in the post-pandemic context of the current information war, as a result of the events in the geostrategic area of Ukraine.

Error is human but can be avoided through awareness. Hacker attacks will be countered, through periodic information, through constant emails, courses, training, eliminating the possibility of more serious future problems, especially with regard to sensitive government information and data.

In the near future, public administration will evolve towards a new approach to the use of emerging technologies, being transposed into future strategies regarding innovation in development and ensuring cyber security, using solutions in cloud, on-premise, or hybrid cloud environments, depending on the available budgets and of advantages or disadvantages offered. For the efficiency of the activity or in the situation of permanent blocking of employment procedures in the public administration, the subcontracting of services by allowing access to these technologies, represents an effective way of managing platforms and IT systems, with a cost-benefit ratio in favor of the public institution, making the use of internal resources more efficient.

Security solutions used in the organization generate real benefits for the institution when they are configured correctly in accordance with current security standards, ensuring continuous protection of equipment, applications and users.

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

Intelligent and intuitive, easy-to-use management tools can optimize the time needed to implement new security policies, through appropriate monitoring and alerting. Also, the collaboration with the National Cyberint Center - the Romanian Information Service - ensures stability and access to the necessary knowledge in the activity of implementing these cyber security assurance systems at the organizational level.

The unified and integrated technologies offer a measurable advantage in efficient results, the organization benefiting from such consoles and tools adapted to the level of expertise, in accordance with the strategies built by the Security IT department. Cooperation with other institutions such as the National Cyberint Center - the Romanian Information Service, by participating in seminars and conferences in the field of cyber security, is an excellent tool for improvement and awareness, building at the local level the principles of an applied guide of good practices, assimilated in order to adopting the best decisions for the public institution.

The budget allocated to innovation in public administration will create and maintain the much-desired stability, especially in critical national areas, such as ensuring the absorption of European funds. In industry and the economy, the role of robotics and process automation will grow considerably, with technology-related changes bringing both benefits and vulnerabilities, particularly in cyber terms. A virtual parallel world will be created, in which the existence of the state, with all that it represents, must be protected, so that the environment is safe and secure, including for the individual. The consequences of competition in innovation produce major transformations including in society, simplifying the complex life of modern man, in the information society.

They will crystallize into a national interest for the Government Strategy, areas such as attracting European funds and ensuring cyber security, with the aim of modernizing, computerizing and digitizing the public administration in Romania.

The inclusion of interoperability requirements in relation to the European Commission requires a clear focus on functional and reliable reporting processes, with results such as increased processing of documents in electronic format, signed with digital certificates. The concentration of resources can only provide solutions under safe operating conditions, ensured only by a state of cyber security.

LITERATURE REVIEW

The new innovation trends in the use of intelligent technologies are reflected in the Cybersecurity Policies, applied at the level of the administration console of the anti-virus type solution, belonging to the Ministry of Investments and European Projects- The software product used is an integrated platform for the security management of the equipment (stations and physical / virtual servers) used and managed within MIPE - Bitdefender GravityZONE Single Central Administration Console.

The integrated device security management platform is based on a simple and integrated architecture with centralized management for both workstations and data centers. It thus allows the efficient and quick installation of the protection solution and requires less administrative effort after implementation, in order to obtain the highest possible degree of accuracy regarding the assurance of cyber security at the MIPE level.

Using machine learning capabilities and automatic incident investigation, certain activities that should have been performed by a security incident response team will be performed automatically in conditions where MIPE does not currently benefit from an internal SOC (Security Operation Center) structure. Integrated and automated response

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

flows will enable designated personnel to respond effectively by limiting lateral spread and stopping potential attacks. Threat visualization features enable focus on specific aspects of investigations, helping to understand complex detections, and identify the root cause of attacks, thus maximizing immediate response capability.

The result is threat prevention, deep visibility, accurate incident detection and intelligent response to minimize exposure to infection and stop unauthorized access. As an integrated workstation protection package, the integrated equipment security management platform ensures a uniform level of security for the entire IT environment, so that attackers cannot find a weakly protected workstation to use as an entry point. departure for dangerous actions against the organization.

As a result of cyber events, such as attacks such as those associated with the EMOTET and Andromeda Malware Campaigns, it was found the need to implement a centralized component to ensure cyber security at the MIPE level, by configuring the Central Antivirus Solution Administration Console, in order to come in the face of cyber-attacks and to have the possibility of automatic detection and analysis of cyber threats and related possible incidents. In the current geopolitical conditions and considering the possible cyber effects generated by the informational component of the current global state of war, it is necessary to ensure the cyber security component by using emerging machine learning technologies, cloud scanning features and sandbox analyzer to detect malicious activity that evades traditional endpoint attack prevention mechanisms.

Threat visualization features enable focus on specific aspects of investigations, helping to understand complex detections, and identify the root cause of attacks, thus maximizing immediate response capability.

The integrated central console provides automated alert prioritization with one-click remediation functions. It will thus achieve continuous analysis within the organization, using unique capabilities to identify risk based on hundreds of factors. Providing clear guidance for mitigating potential risks at the user, network and operating system levels.

For the administration of the 3400 licenses of the workstations, centrally from the console, it is necessary to consume a low effort for the maintenance activity of the automatic processes, being easy to implement and integrate into the existing security architecture.

The agent is resource-efficient, with low administrative costs in terms of disk space, memory, bandwidth, and CPU resources.

The flexibility, scalability and upgradeability of the complete endpoint protection platform and managed detection and response services are required in the process of ensuring the cybersecurity standard built at the MIPE level.

By using cutting-edge threat detection technology, including fileless attacks, ransomware and other zero-day threats.

In threat analysis, the event logging feature continuously filters events produced on the endpoint, compiling a prioritized list of incidents for further investigation and response.

In the event recording process, continuous monitoring allows data to be passed to the threat analysis module to visualize the results generated by the events involved in an attack.

The single management console automatically executes suspicious payloads in a controlled virtual environment. The threat analysis module then uses this analysis to make appropriate decisions about suspicious files, according to the automation achieved through the security policy implemented at the level of the single management console.

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chişinău, Moldova

Cyber Security incident investigation and response processes will be automated through the IoC search capability, querying the event database to discover possible threats through ATT&CK techniques and indicators of compromise as well as updated information on discovered threats or other possible malware.

METHODOLOGY

The research was carried out at the level of the Ministry of Investments and European Projects, with the main aim of creating scientific and technological excellence by analyzing the results obtained through the use of intelligent technologies at the central administration level, as well as obtaining advantages in the field of cyber security and resilience of systems, services and critical infrastructure of national importance, as well as increasing the degree of cyber security culture in the central public administration and among contractual users or civil servants, with the possibility of establishing within the organization at least 3 positions with specific tasks in the cyber field, in direct collaboration with the Ministry's Security Structure and in a cooperation agreement with the National Cyber Intelligence Center of the Romanian Intelligence Service.

The period included in the analysis activity is between the years 2013-2023, including two programming periods of non-refundable financing from European funds, facilitated by the European Commission, as well as the National Recovery and Resilience Plan.

The three projects carried out by the Cyber-int National Center, to ensure cyber security at the national level, constituting a security umbrella, over the critical infrastructure of national interest, which will be reinvented through the digital transformation generated with the help of emerging technologies, which have produced an evolution considerable in government digital transformation.

Emerging technologies and the integration of machine learning functionalities through artificial intelligence, at the level of the Ministry of Investments and European Projects, as a development measure through innovation, will produce positive effects including on the development of the national economy by increasing the absorption of European funds in a secure cyber environment.

RESULTS AND DISCUSSIONS

The cyber security policies, applied at the level of the administration console of the anti-virus type solution, belonging to the Ministry of Investments and European Projects, ensure a high degree of defense against current cyber threats.

The software product used is an integrated platform for the security management of equipment (stations and physical / virtual servers) used and managed within MIPE.

A complete workstation security solution, designed from the ground up as an integrated EPP and easy-to-use EDR, offering prevention, threat detection, automated response, pre- and post-compromise visibility, alert triage, investigation, advanced search and one-click fix.

Relying on highly effective prevention, automatic threat detection and response technologies, the antivirus software product (the IT solution) greatly limits the number of incidents that require manual analysis, reducing the operational effort required to use an EDR solution.

For the centralized solution, delivered on premise and designed with a single agent and a single console, it is also necessary to ensure the premises to ensure compatibility and

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

an easy way to install and integrate into the existing security architecture, by personnel authorized by the manufacturer.

Integrated device security management platform enables precise protection of digital assets against even the most difficult-to-detect threats by effectively responding to all phases of an attack.

The decisive step in the use of emerging technologies through the integration of Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of Investments and European Projects, was made within the projects financed from non-reimbursable funds, as a measure of the development through innovation, of a critical infrastructure of national interest, through -a cooperation agreement with the National Authority in the field of Cyber-intelligence - the National Cyberint Center - within the Romanian Information Service.

The result is potential threat prevention, deep visibility, accurate incident detection, and intelligent response to minimize infection exposure and stop unauthorized attacker access.

As an integrated workstation protection package, the integrated device security management platform ensures a uniform level of security across MIPE's IT environment, so that attackers cannot find a weakly protected workstation to use as an entry point for dangerous actions against the organization.

The security equipment used within the organization offers advanced management capabilities to prevent, detect and investigate cyber security incidents, by analyzing the risks generated by possible attacks, as well as timely automatic remediation of threats.

Increasing awareness of the importance of ensuring cyber security will be achieved by informing users, making the first measure of protection against cyber-attacks within the organization. Human error can be avoided through e-learning and the implementation of the security assurance component starting from the individual level.

These aspects implemented in the organization will counter the attacks of hackers, by ensuring regular information activities regarding good practices through constantly sent emails, organization of courses and training, eliminating the possibility of subsequent, much more serious problems, especially regarding the information and data belonging to the central administration.

The public administration will evolve towards a different approach to the use of emerging technologies, translating into future strategies, the need to use solutions in cloud, on-premises or hybrid cloud environments, depending on budgets and available advantages or disadvantages, fulfilling a strategy of innovation and development of digitization processes by using the funds related to the National Recovery and Resilience Plan.

In order to make the activity more efficient or to avoid situations of temporary blocking of the procedures applied in the public administration, a solution can be the subcontracting of the necessary services, which allow access to such intelligent technologies, constituting an efficient way of managing the platforms, with a cost-benefit ratio built in in favor of the public institution, with the aim of reducing the use of internal resources and decongesting the high degree of burden manifested in the activity of public officials from the central administration.

Public administration services can be optimized with the help of the use of advanced information technologies. The European Commission tries to set its own example in this sense, through the procedures and tools it uses in its day-to-day activity, in its links with the administrations of the member states and with its own decentralized agencies, marked by constant progress in innovation and computerization. The goal being

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

to facilitate citizens' access to public information through new technologies and computer applications, as well as to achieve better communication between all levels of public administration in the Union, thanks to the high-speed connection.

The development of the European information society requires a considerable financial effort, which is constantly growing, which cannot be fully assumed by the European Union and the governments of the member states.

Practical experience has shown that the private sector is the most capable of taking the necessary risks in operating and developing new adaptable markets, having the necessary capital to make such investments necessary for the digital transformation strategy.

The integration of machine learning and artificial intelligence functionalities, at the level of the Ministry of Investments and European Projects, can be seen in Tables 1 and 2 below, while the use of intelligent technologies such as Sandbox Analyzer and EDR - Endpoint Threat Detection and Response (ETDR) can be seen in Figures 1 and 3 below, and Computers – Endpoint policy compliance in Figure 2.

Table 1. Integrating Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects

Implementation period	Protected workstations	Increasing the degree of cyber protection	Automate responses to detected and remedied cyber attacks	Fixed vulnerabilities	Possible security risks
Cyber Project 1	250 to 450	200 Endpoints	About 50%	75%	25%
Cyber Project 2	450 to 1700	1250 Endpoints	About 75%	90%	10%
Cyber Project 3	1700 to 3400	3400 Endpoints	About 95%	95%	5%

Source: Author' own research

Table 2. Results of Integrating Machine Learning and Artificial Intelligence functionalities, at the level of the Ministry of European Investments and Projects

Automation period	Protected endpoints	Increasing the cyber protection	Automated detected and remedied cyber attacks	Security vulnerabilities	Security risks
2014-2017	450	200 Workstations	50%	75%	25%
2020-2023	1700	1250 Workstations	75%	90%	10%
2023-2027	3400	3400 Workstations	95%	95%	5%

Source: Author' own research

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

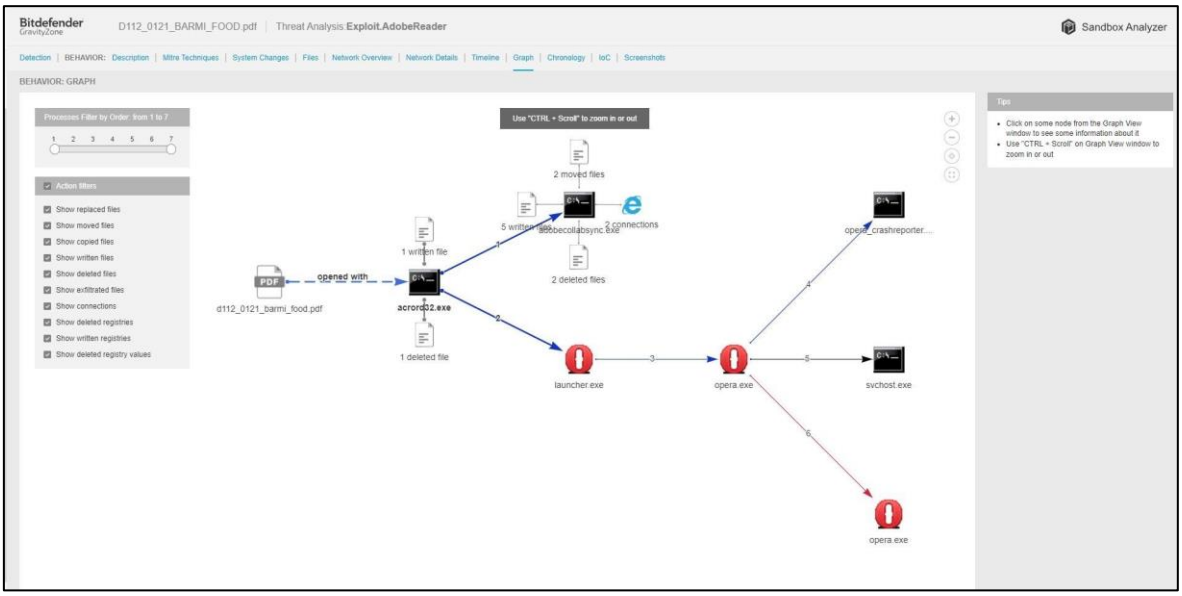


Figure 1. Sandbox Analyzer – Ministry of European Investments and Projects
Source: www.bitdefender.com

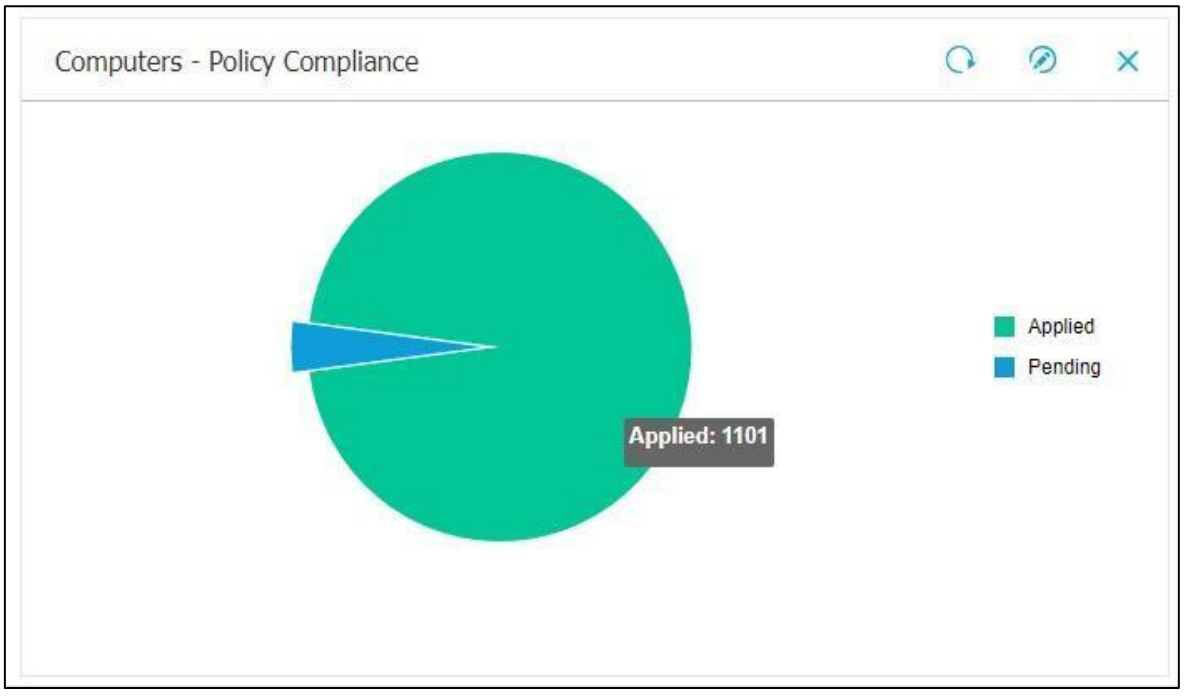


Figure 2. Computers – Endpoint policy compliance – Ministry of European Investments and Projects
Source: www.bitdefender.com

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

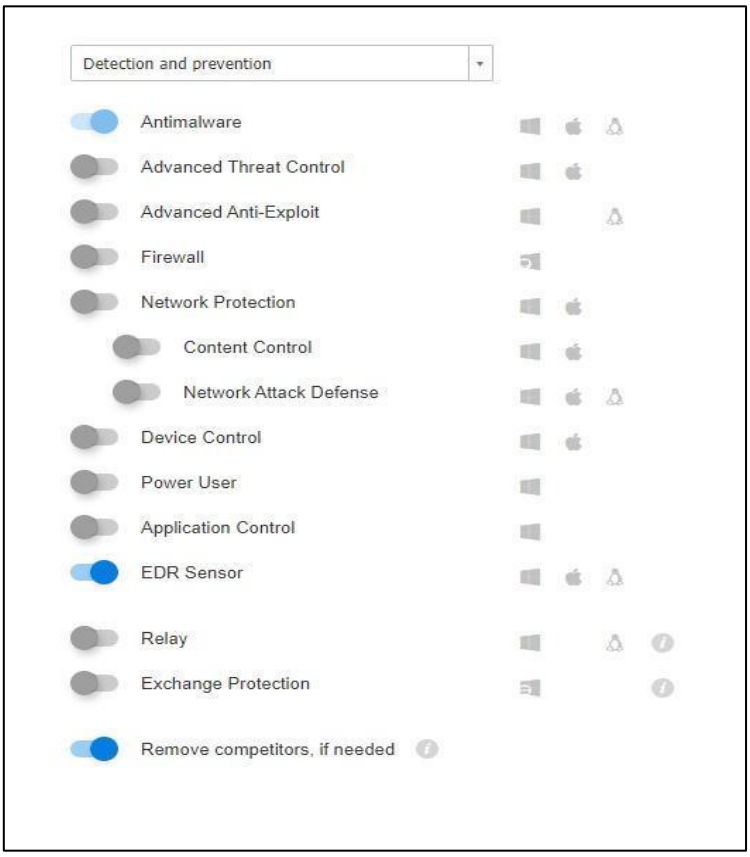


Figure 3. Endpoint Threat Detection and Response – Ministry of European Investments and Projects
Source: www.bitdefender.com

CONCLUSIONS

Using machine learning capabilities and automatic incident investigation, certain activities that should have been performed by a security incident response team will be performed automatically in conditions where MIPE does not currently benefit from an internal SOC (Security Operation Center) structure.

Integrated and automated response flows will enable designated personnel to respond effectively by limiting lateral spread and stopping potential attacks.

Threat visualization features enable focus on specific aspects of investigations, helping to understand complex detections, and identify the root cause of attacks, thus maximizing immediate response capability.

The EDR module provides automated alert prioritization with one-click remediation features. The EDR module will perform continuous analysis within the organization, using unique capabilities to identify risk based on hundreds of factors. Providing clear guidance for mitigating potential risks at the user, network and operating system levels. EDR administration requires low maintenance effort, being easy to implement and integrate into the existing security architecture, compatible with the antivirus solution used at the MIPE level.

The agent is resource-efficient, with low administrative costs in terms of disk space, memory, bandwidth, and CPU resources. The flexibility, scalability and upgradeability of the complete endpoint protection platform and managed detection and

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

response (MDR) services are necessary in the process of ensuring the cybersecurity standard built at the MIPE level.

By using cutting-edge threat detection technology, including fileless attacks, ransomware and other zero-day threats. In threat analysis, the event logging feature continuously filters events produced on the endpoint, compiling a prioritized list of incidents for further investigation and response. In the event recording process, continuous monitoring allows data to be passed to the threat analysis module to visualize the results generated by the events involved in an attack.

The Sandbox Analyzer component automatically executes suspicious payloads in a controlled virtual environment. The threat analysis module then uses this analysis to make appropriate decisions about suspicious files, according to the automation achieved through the security policy implemented at the level of the single management console.

Cyber Security incident investigation and response processes will be automated through the IoC search capability, querying the event database to discover possible threats through ATT&CK techniques and indicators of compromise as well as updated information on discovered threats or other possible malware.

The use of security solutions through intelligent technologies will generate real benefits within the organization through the necessary configuration in the secure operation standards. Intuitive emerging technologies will optimize the time required to implement new security policies to achieve better monitoring and accurate alerting.

The cooperation with the National CYBERINT Center - Romanian Information Service, ensures stability in the cyber defense component, as well as access to the necessary knowledge in carrying out the awareness activity of the importance of ensuring the state of cyber security.

Cooperation to ensure cyber security, participation in seminars and conferences in the field of cyber defense, represent excellent tools for improvement and innovation in the organization, creating the premises for the assimilation of good practices, in establishing the best decisions for the public institution.

The unified and integrated technologies offer a measurable advantage in obtaining more efficient results, benefiting from unique management consoles and tools adapted to the level of expertise held in the organization, completed with the cyber security strategies built by the Cyber Security department of the Ministry of Investments and European Projects.

The budget allocated to innovation in public administration, through specific European funding programs, will create and maintain the necessary stability, especially in critical areas of the national economy, such as the absorption of European funds.

The economy and society will undergo transformations, the role of robotics in industry and the automation of repetitive processes in organizations will increase considerably.

The revolution of emerging technologies brings both benefits and vulnerabilities, threats and risks, especially in cyberspace, regarding the need to ensure cyber defense.

By reinventing governance and computerizing public administration, a parallel virtual world will be created, in which the existence of the state, with the balance of the necessary security state, must be protected, so that the cyber environment is safe and secure even for the citizens.

The repercussions of competition in innovation produce major transformations through interoperability and synergy, including in society, simplifying the crowded life of modern man in the era of the information society.

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chişinău, Moldova

Strategic areas such as the attraction and absorption of European funds, by ensuring cyber security, aiming at the modernization and computerization of the public administration in Romania, constituting a national interest for the government's evolution in innovation.

Creating a global framework of security and trust in ICT, with an expansive trend towards automating repetitive processes, will generate the achievement of optimal efficiency.

These strategic objectives aim at the creation of scientific and technological excellence, obtaining advantages in innovation through the security and resilience of systems, services and critical infrastructure of national importance, as well as increasing the degree of cyber security culture among officials in the central public administration.

An important stage will be achieved in the inter-institutional collaboration, for the achievement of the fundamental objectives of the country strategy, the field of funds becoming a critical infrastructure of national interest, through the inherent implications generated in the national economy, all important plans of the current modern society being affected, from the financial - up to economic, social-educational, even political, with all the necessary risks assumed through the decisions applied at the level of future strategies.

The efficient management of the infrastructure and applications intended for the management of European funds, having a particular importance in the evolutionary process of increasing the quality of life, represents the first step towards knowledge, innovation and development of society in the information age.

BIBLIOGRAPHY

1. European Commission (2022) *Jobs and the economy during the COVID-19 pandemic* [viewed 01 dec 2023]. Available from: <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/jobs-and-economy-during-coronavirus -pandemic.ro.>
2. PUBLISHER:.FOUNDATION FOR EUROPEAN STUDIES, *European Information Society*, 2005.
3. JAN SERVAES, *The European Information Society – A reality check* – Bristol, UK Portland, OR, USA, 2003, ISBN 1-84150-893-4 / 1-84150-106-9.
4. European Commission - Brussels, 3.3. (2021) *One year since the outbreak of COVID-19: fiscal policy response* [viewed 02 dec 2023]. Available from: <https://ec.europa.eu/info/files/one-year-outbreak-covid-19-fiscal-policy-response_en.>
5. Presidential Administration - Bucharest (2020) Romania - *National Strategy for National Defense for the period 2020-2024.* [viewed 03 dec 2023]. Available from: <https://www.presidency.ro/files/userfiles/Documente/Strategia_Nationala_de_Aparare_a_Tarii_2020_2024.pdf>
6. European Council - Council of the European Union - March (2010) - *European Union Internal Security Strategy;* [viewed 04 dec 2023]. Available from: <https://www.consilium.europa.eu/ro/documents-publications/publications/internal-security-strategy-european-union-towards-european-security-model/.>
7. Decision of the Official Gazette no. 677 (2020 - August 14) - *on the approval of the National Program for the digitization of micro, small and medium enterprises, financed under the Operational Program Competitiveness 2014-2020.* [viewed 05 dec 2023]. Available from: <http://legislatie.just.ro/Public/DetaliiDocument/229226 - OFFICIAL GAZETTE no. 756 of 19 August 2020.>

DOI: https://doi.org/10.53486/escst2023.21
International Conference, December 07-08, 2023, Chișinău, Moldova

8. EU Directive 1148 / (2016) - *Measures for a high level of security of networks and information systems in the Union.* [viewed 06 dec 2023]. Available from: <https://cert.ro/pagini/ansrsi.>
9. Regulation (EU) (2016) / 679 - *on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC* (General Data Protection Regulation).
10. The European Union Agency for Cybersecurity (ENISA), (2021) September 13 - *Methodology for a Sectoral Cybersecurity Assessment*[viewed 07 dec 2023]. Available from: <https://www.enisa.europa.eu/publications/methodology-for-a-sectoral-cybersecurity-assessment.>
11. The European Union Agency for Cybersecurity (ENISA), (2020) April 15 - *Advancing Software Security in the EU*[viewed 08 dec 2023]. Available from: <https://www.enisa.europa.eu/publications/advancing-software-security-through-the-eu-certification-framework>
12. National Cybersecurity Directorate (DNSC) - (2021) September 30 - *European Cybersecurity Month – ECSM* [viewed 09 dec 2023]. Available from: <https://cert.ro/citeste/comunicat-luna-europeana-a-securitatii-cibernetice-2021>
13. Oracle Romania (2022) *Emerging technologies: IoT, EoT, AI, Blockchain* [viewed 10 dec 2023]. Available from: <https://www.oracle.com/ro/emerging-technologies/.>
14. Cloud Computing, Events - October 6, (2021 at 11:19 am) - *Cloud Conference brings new technologies to the forefront - (clubitc)* [viewed 11 dec 2023]. Available from: <https://www.clubitc.ro/2021/10/06/conferinta-de-cloud-aduce-in-prim-plan-noile-tehnologii/.>

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chişinău, Moldova

TOOLS AND MECHANISMS FOR ACHIEVING SUSTAINABLE PUBLIC PROCUREMENT IN THE CONTEXT OF ENSURING NATIONAL ECONOMIC SECURITY

Alina CODREANU

PhD student, Lecturer,
Academy of Economic Studies of Moldova, Moldova,
ORCID 0000-0001-9996-7630
E-mail: codreanu.alina.@ase.md

Abstract. *This study underscores the premise that national economic security is also described by the phenomenon of the public procurement contract, which will take into account the rigors imposed by the legislator, respecting the fundamental principles and capitalizing on concepts such as good management of public money, green procurement, wise procurement, control managerial quality, through the responsible involvement of all participating actors. The achievement of sustainable public procurement requires an extensive, complex process, which includes a set of effective tools and mechanisms. If we are to mention the public procurement contract and especially the procedures expressly provided by the Moldovan legislator, we can mention that this type of contract can be awarded through the following procedures: open tender; restricted tender; competitive dialogue; negotiated procedures; request for price offers; solution contest; acquisition in the case of social housing construction plans. The study includes a brief synthesis of the reasoned opinions of some authors, experts in the field of public procurement, regarding the development of the concept of ensuring economic security. The research methods used were varied: documentary analysis, comparative analysis, synthesis, the method of induction and deduction. The importance of knowing and capitalizing on tools and mechanisms for sustainable public procurement, in the context of ensuring national economic security, will take into account, first of all, the fundamental principle of the efficient use of public money, which will involve following a well-determined direction.*

Keywords: *public procurement, public procurement procedures, national economic security, effective tools and mechanisms, economic security viewed through the lens of the implementation of sustainable public procurement.*

UDC: *005.932.2:[658.727:347.451.6](478)*

JEL Classification: *H57, F52, K22.*

INTRODUCTION

This study was carried out with the intention of researching and analyzing what are the tools and mechanisms for achieving sustainable public procurement in the context of ensuring national economic security. The main beneficial changes in the given system, conditioned by the normative improvements, elaborated according to the provisions of the European directives and the harmonization of the national legal framework show that, despite some shortcomings, challenges, this set of instruments and mechanisms is continuously developing, the impact of which has a positive connotation both at national level and in relation to external evaluation mechanisms.

The social dialogue between the authorities responsible for carrying out sustainable procurements and the other actors involved, the involvement of civil society in monitoring the correct and efficient progress of procurements, the increasingly daring implementation of green public procurements, increasing the efficiency of the use of public money, the evaluation of management in the field of public procurements from the stage from initiation to control - all these tools, mechanisms, as well as others are to be addressed,

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chișinău, Moldova

tangentially, in this research. The study includes a brief synthesis of the reasoned opinions of some authors, experts in the field of public procurement, regarding the development of the concept of ensuring economic security, the emphasis being mainly on this aspect. The research methods used were various: documentary analysis, comparative analysis, synthesis, the method of induction and deduction etc.

DISCUSSIONS AND RESULTS

In accordance with art. 72 of the Law [1], which provides the essence of the principles of awarding the public procurement contract, we highlight the idea that the public procurement contract is awarded based on the following principles, namely: a) compliance with the law, legal order, good morals and professional ethics; b) selecting the most advantageous offer; c) ensuring environmental protection and supporting social programs in the process of executing the contract.

In the same way, we can mention the special conditions for the execution of the public procurement contract, which must be provided in the notice/invitation to participate or in the specifications. Therefore, they can have as their objective, in particular, the encouragement of professional training at the workplace, the employment of the unemployed, young people and people with integration difficulties, the reducing the number at the unemployment level, the professional training of the unemployed and young people, the protection of the environment, the improvement of working conditions and work security, the development of the rural environment and the professional training of farmers, the protection and support of small and medium-sized enterprises, including during the execution of the contract and under subcontracting conditions. [1, art. 73]

The authors Ulian G. and Mulic A. support the idea that "with the help of the public procurement system, important tasks are solved, such as respecting national security, creating and supporting state material reserves, ensuring the life of the population, etc.". [2, p. 39]

However, international experience reveals that the problem of corruption in public procurement can have a very diverse impact: financial, economic, on the environment, human health and safety, innovation, etc. Corruption in public procurement causes the erosion of human values and trust in government at the central and local level, when the danger appears for the competition and economic development of the country. [3, p. 242]

In France, the different stages of public procurement are governed by the fundamental principles characteristic of public procurement, expressly provided in art. 3 of the Public Procurement Code. It is about: freedom of access to public procurement; equal treatment of candidates and transparency of procedures. In this sense, the regulations applicable to public procurement are aimed at preventing violations of any nature, such as, for example, conflicts of interest, acts of corruption, favoritism, etc. These breaches of integrity could be of concern to all public procurement stakeholders. [4, p. 9]

Public officials have the obligation to exercise their functions with impartiality, probity, integrity, dignity and to ensure that any conflict of interest is prevented or stopped immediately. These principles apply to all public servants (public servants, especially those seconded to public institutions and contract workers in the three public services). [4, p.11]

Researcher Osmoschescu N. claims that "...from a legal point of view, the right to a healthy environment is a fundamental right from the category of social-economic rights, civil rights that ensure the material, physical and cultural development of the person, allowing him to participate as actively as possible, to social life". [5]

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chișinău, Moldova

According to the researcher Odainic M., in the Republic of Moldova, the propagation of the concept of sustainable public procurement among the contracting authorities remains a priority even today, so that it is absolutely necessary that the degree of awareness and implementation by the contracting authorities of the standards of sustainability in the processes of purchasing products , services and works to increase. We cannot deny that, in particular, public procurement legislation, together with the constitutional framework and subsequent national environmental legislation, regulate important standards that, if implemented, would increase the positive impact of public procurement on the environment. And this becomes a global emergency in the conditions in which every part of the globe already feels, more intensely or more attenuated, the effects of climate changes that have become a reality experienced today by each of us. [6, p. 52]

If we are to analyze, in essence, the institution of the public procurement contract and especially the procedures expressly provided by the Moldovan legislator, we can mention that this type of contract can be awarded through the following procedures: a) open tender; b) restricted tender; c) competitive dialogue; d) negotiated procedures; e) request for price offers; f) solutions competition; g) acquisition in the case of social housing construction plans.

Therefore, the basic procedures for awarding the public procurement contract *are the open tender and the restricted tender.* The contracting authority can use special award methods only in the cases expressly provided by law. It should be noted that the contracting authority has the right to use the following specific techniques and instruments for awarding public procurement contracts: *the framework agreement; the dynamic purchasing system; electronic auction; electronic catalogs.*

The choice of the award procedure denotes the ability of the contracting authority to describe its need/necessity, respectively to detail the technical specifications related to the goods/services/works it intends to purchase. We are also talking about the estimated value of the public procurement contract, but also about the level of competition on the market between the economic operators that can supply the goods/services/works that the contracting authority intends to purchase.

One of the basic procedures is the *open tender*. The open tender procedure includes offers from all economic operators who wish to participate in the tender. The rule is the awarding of the public procurement contract through an open tender, the other procedures can be used only by way of exception, under the conditions established by law. The notice of participation in the open tender is published in the Public Procurement Bulletin (BAP).

The period between the date of publication of the notice of participation and the deadline for submission of offers must be at least 20 days. If, for technical reasons, the award documentation cannot be published electronically, the contracting authority has the obligation to make the award documentation available to the economic operator as quickly as possible, within a period that must not exceed 2 days from receiving a request from him. [7]

The open tender is initiated by the transmission for publication of a notice of participation by which economic operators are requested to submit offers. This takes place in a single stage, it can be completed by an additional stage of electronic auction. It should be noted that it is recommended to be applied when the offer on the market is not surplus. Likewise, it can be organized entirely electronically. Open bidding is used for the awarding of most public procurement contracts, regardless of their subject matter.

Another basic procedure is the *restricted tender*, which is carried out according to the same rules as for the open tender, provided that a pre-selection procedure is applied,

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chișinău, Moldova

preceded by the publication of a notice of participation in the pre-selection. The restricted tender procedure is carried out in two stages: the selection of candidates, by applying the qualification and selection criteria; and the evaluation stage of the offers submitted by the selected candidates, by applying the award criteria. [art. 51, 1]

The limited tender is initiated by the publication in the BAP of a participation announcement, through which interested economic operators are requested to submit candidacies. The period between the date of publication of the notice of participation in the BAP and the deadline for submitting candidacies must be at least 20 days.

The contracting authority has the obligation to indicate in the notice of participation the selection criteria and appliable rules, the minimum number of candidates it intends to select and, if applicable, their maximum number. The minimum number of candidates, indicated in the notice of participation must be sufficient to ensure real competition and, in any case, cannot be less than 5. The number of candidates selected in the first stage of the restricted tender must be at least equal with the minimum number indicated in the participation notice. If the number of candidates who meet the selection criteria is lower than the minimum number indicated in the notice of participation, the contracting authority must cancel the restricted tender procedure. It is forbidden to invite to the second stage of the restricted tender an economic operator who did not apply in the first stage or who did not meet the selection criteria. [7]

The request for price offers represents the simplified procedure by which the contracting authority requests offers from several economic operators, in order to purchase goods, works or services, which are presented according to concrete specifications.

The contracting authority, through the request for price offers, can award contracts for public procurement of goods, works or services, which are presented according to concrete specifications, provided that the estimated value of the acquisition does not exceed 800,000 lei for goods and services and 2,000,000 lei for works. The contracting authority can establish, in addition to the price, other requirements that will be taken into account when evaluating the price offers. In this case, each such requirement and its relative value shall be indicated in the request for price offers. Each economic operator can submit a single price offer, without the right to change it, except for the cases provided for in para. (8) of the Law on public procurement. On such an offer, no negotiations take place between the contracting authority and the offeror. The bid that meets all the requirements according to the award criteria provided in the announcement/invitation to participate is declared the winner. [art. 57, paragraph 1-5, 1]

The procedure for requesting price offers for the purchase of goods and services for which the participation notice was not published in the BAP is considered to have been carried out only if at least 3 offers have been submitted. If, as a result of the invitation to participate, the required number of offers has not been accumulated, the results of the procurement procedure are canceled and it is organized repeatedly with the prior publication of a participation notice in the BAP.

If, during the repeatedly organized procedure, it is found that there are less than 3 qualified economic operators, the contracting authority is entitled to award the contract according to the initially established criteria, with the exception of the procedure for requesting price offers for works with an estimated value higher, less than or equal to 200,000 lei.

The contracting authority, within no more than 3 days after the establishment of the winning offer, will inform all participants with a note about the results of the COP procedure, as well as about the reasons for rejection in the case of rejected offers and about

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chișinău, Moldova

the reasons for disqualification in the case of disqualified bidders. The contract will be concluded no earlier than 6 days from the date of transmission of the communication regarding the result of the application of the award procedure. Within 5 days from the date of conclusion of the contract or additional agreement (regarding the modification/termination of the contract), the contracting authority will draw up and submit a report to the Agency for examination. In the event that no offer was submitted to the respective procedure, as well as in the event of its cancellation, the contracting authority, within 5 days after the deadline for submitting the offers indicated in the invitation/announcement to participate, will present to the Agency.

The legislator defined *the negotiation procedure* as the procedure in which the contracting authority consults the economic operators regarding their options and negotiates the contractual conditions with one or more of them. [art. 1, 1]

The negotiating procedures are the procedures in which, in order to identify the most advantageous offer, the contracting authorities negotiate with the bidders the offers presented by them in order to adapt them to the requirements expressed in the notice of participation, in the descriptive documentation and in any additional documents. It should be noted that the choice of this procedure does not depend on the estimated value of the contract.

The negotiation with the prior publication of an invitation to participate takes place in three stages: *the candidate qualification stage; the negotiation stage with qualified candidates; evaluation of the final offers submitted by them and designation of the winner*.

The negotiation with the prior publication of a tender notice is applied in the following cases: in the case of the presentation of incorrect or unacceptable offers within an open or restricted tender procedure, of a request for price offers or within a competitive dialogue, if they are not modified substantially the initial conditions of the contract. The contracting authority has the right not to publish a notice of participation if it includes in the negotiated procedure all bidders or only bidders who meet the qualitative selection criteria and who submitted, during the previous open or restricted procedure, the procedure for requesting price offers or the previous competitive dialogue, offers compliant with the official requirements of the award procedure. [7]

The application of the negotiated procedure in this case is possible only after the cancellation of the initial procedure. It is applied in the following cases: in exceptionally well-reasoned cases, if it is about goods, works or services whose nature or whose risks do not allow the prior and definitive establishment of prices; in the field of services, including intellectual ones, such as the design of works, to the extent that, due to the nature of the services to be provided, the contract specifications cannot be established precisely enough to allow the award of the contract by selecting the most advantageous offer, according to the rules regarding the open procedure or the restricted procedure; in the case of public procurement contracts for works performed or services provided exclusively for the purpose of research-development or experimentation and not to ensure a profit or to cover research-development costs.

Before the initiation of the negotiation procedure, the working group has the obligation to verify the meeting of the conditions provided for the conduct of this procedure. The result of the verification is concretized by drawing up the working group that becomes part of the public procurement file. The decision regarding the application of the negotiation procedure for the award of the public procurement contract is adopted with the majority of votes of the working group members and is recorded in a minutes. If there are separate opinions, they are recorded in the minutes. The negotiation procedure is

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chișinău, Moldova

initiated by submitting for publication in the BAP a notice of participation, by which the economic operators are invited to participate in the negotiation procedure. The period between the date of publication of the notice of participation in the BAP and the deadline for submitting candidacies must be at least 20 days.

In the negotiation procedure with the publication of a call for participation, the minimum number of invited candidates cannot be less than 3. In any case, the number of invited candidates must be sufficient to ensure real competition. In case, the number of candidates preselected is lower than the minimum number provided in the call for participation, either due to the fact that not enough applications were submitted, or due to the fact that some of the candidates did not meet the minimum qualification requirements, the contracting authority will cancel the negotiation procedure with prior publication of an announcement of participation. The period granted for the preparation of the preliminary offer must not be less than 10 days.

The negotiations continue until the moment when each participant in the negotiations declares that the preliminary offer he presented can no longer be improved, a fact that is explicitly recorded in the minutes of the meeting. During the final meeting, each participant has the obligation to present the final elements of his preliminary technical and financial proposal, for which the award criteria will be applied. As a result of the final meeting, the working group draws up the minutes of the final meeting, which ends with each participant separately. Within two days of the final meeting, the bidders are obliged to submit in writing to the contracting authority, for the attention of the working group, the final bid in full accordance with the aspects established during the negotiation rounds. The offer will be presented in the format required in the award documentation.

Negotiation without prior publication of a contract notice. The contracting authority has the right to apply the negotiation procedure without the prior publication of a tender notice only in the following cases: • no offer or no adequate offer or no candidacy has been submitted in response to an open tender or restricted tender procedure so while the initial conditions of the contract are not substantially modified; • to a strictly necessary extent, for reasons of maximum urgency as a result of unforeseeable events for the contracting authority in question. In this case, the reasons invoked to justify the urgency of the acquisition must not represent the result of the negligence of the contracting authority; • for technical reasons, creation or related to the protection of exclusive rights, a single economic operator has the necessary goods, works and services or a single economic operator has priority rights over them and there is no other alternative. [art. 56, 1]

In the case of public procurement contracts for works and services: for the additional works or services that are not provided for in the initial estimated project or in the initial contract and that have become necessary for the execution of the works or the provision of the services indicated therein, as a result of an unforeseeable situation : • if the respective additional works or services cannot be separated, from a technical or economic point of view, from the object of the initial contract without constituting a major inconvenience for the contracting authorities; or • if the respective additional works or services, even if they can be separated from the object of the original contract, are strictly necessary for its completion. The cumulative value of contracts awarded for additional works or services must not exceed 15% of the initial contract value.

The framework agreement represents an agreement concluded between one or more contracting authorities and one or more economic operators, with the object of establishing

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chişinău, Moldova

the conditions for the contracts to be awarded during a determined period, in particular the prices and, as the case may be, the stipulated quantities. [art. 61, paragraphe 1, 1]

The contracting authority has the obligation to conclude the framework agreement by applying the open tender or restricted tender procedure. The contracting authority does not have the right to establish that the duration of a framework agreement exceeds 4 years, except in exceptional cases, which it can justify in particular by the specific object of the contracts to be awarded based on the respective framework agreement.

Contracts that are awarded on the basis of a framework agreement can only be concluded between the contracting authority/authorities and the economic operator/operators that are part of the respective agreement. If the contracting authority concludes the framework agreement with several economic operators, their number cannot be less than 3, as long as there is a sufficient number of economic operators who have met the qualification and selection criteria and who have submitted offers admissible. If the number of economic operators who have met the qualification and selection criteria and who have submitted admissible offers is lower than the minimum number indicated in the notice/invitation to participate, the contracting authority is obliged to cancel the procedure for concluding the framework agreement. The contracting authority has the right to assign subsequent public procurement contracts to a framework agreement concluded with several economic operators: *either without resuming the competition; either by resuming competition between economic operators signatories of the framework agreement.* [7]

It is well known that green public procurement is a way in which public authorities can contribute to the protection of the environment through the process of acquiring the goods and services necessary to carry out specific tasks. This approach encourages the production and use of goods and services that meet environmental standards, as well as encouraging innovation and the development of clean technologies.

In the European space, ecological public procurement is considered to be a key element for achieving the objectives set by the European Union in the field of environment, such as reducing greenhouse gas emissions, conserving natural resources and promoting sustainable development. That is why, starting in 2008, the European Commission established an action plan for green public procurement. Therefore, ecological public procurement not only benefits the environment, but also the economy. They can reduce the operating and maintenance costs of purchased goods and services in the long term by reducing the consumption of energy and other resources. [8]

They can also stimulate innovation and the development of green technologies, thus providing business opportunities for companies that produce and provide such products and services. In addition, green public procurement can help raise public awareness of environmental issues and encourage behavioral changes among consumers. The European Union has developed and promotes the use of standardized environmental criteria for public procurement, through guidelines and environmental impact assessment tools. These criteria aim to ensure that public procurement is carried out in a way that minimizes the negative impact on the environment by selecting goods and services that are less polluting and more sustainable. Moreover, the use of standardized criteria facilitates the comparison and evaluation of offers, contributing to increased transparency and competition in the procurement process. [8]

The author Boguş A., in her own studies, brings plausible arguments such as "the Moldovan government has made considerable progress in optimizing the social dialogue with civil society, a significant actor in the democratization of society. Recently, the

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chişinău, Moldova

involvement of civil society, in the process of monitoring the use of public money, has accelerated. Civil society managed to bring to light a series of illegalities, frauds". [9, p. 422]

In the same study, the author mentions that increasing the role of civil society in the supervision of public procurement procedures represents an important step in increasing the degree of democratization of society, but in practice, there are still many problems. Civil society encounters many difficulties in this complex process, from restricting access to information to neglecting its role. [9, p. 421]

Through the objectives of the National Development Strategy "Moldova Europeană 2023" [10], a development vision centered on man is proposed, where he is a beneficiary and not a resource or instrument of development. The path to be implemented will have a direct positive impact on well-being and will capitalize on human potential on an entrepreneurial, educational, cultural and productive level. Thus, the efficient use of public money, through the effective capitalization of "wise" public procurement procedures, will constitute a good way to achieve all the objectives proposed by the Strategy.

CONCLUSIONS

In this study, an attempt was made to emphasize the importance and impact of some tools and mechanisms for achieving sustainable public procurement, in the context of ensuring national economic security. Or, as the result of the research carried out, the efficient use of public money requires following a balanced, well-determined route, from highlighting the best procurement procedures to effective control.

National economic security is also described by the phenomenon of the public procurement contract, which will take into account the rigors imposed by the legislator, respecting the fundamental principles and capitalizing on concepts such as good management of public money, green procurement, wise procurement, managerial quality control, by involving with the responsibility of all participating actors.

Undoubtedly, we can state that there are obvious benefits to the use of green public procurement, but their implementation may encounter certain challenges, such as the lack of knowledge and experience regarding the use of environmental criteria. For this reason, the EU green public procurement criteria are regularly updated to ensure that they reflect the latest technological and market developments.

BIBLIOGRAPHY

1. LAW No. 131 of 03-07-2015 regarding public procurement. Published: 31-07-2015 in Official Gazette No. 197-205 art. 402.
2. ULIAN, G., MULIC, A. *Optimizing the public procurement system in the Republic of Moldova by means of micro and macroeconomic instruments.* In: Conference "Modern paradigms in the development of the national and world economy", Chisinau, Moldova, October 30-31, 2020, pp. 38-41. [online]. [viewed: 02.12.2023]. Available from: <https://ibn.idsi.md/sites/default/files/imag_file/38-41_33.pdf>.
3. MOCANU, E. *Mechanisms to ensure integrity and transparency in the public procurement process.* [online]. [viewed: 04.11.2023]. Available from: <https://ibn.idsi.md/sites/default/files/imag_file/SPM_pp242-245.pdf>.
4. GUIDE de l'achat public: Maîtriser le risque de corruption dans le cycle de l'achat public, Juin 2020. [online]. [viewed: 02.12.2023]. Available from: <https://www.economie.gouv.fr/files/files/directions_services/dae/doc/Guide_maitrise_risque_corruption.pdf?v=1698052065>.

DOI: https://doi.org/10.53486/escst2023.22
International Conference, December 07-08, 2023, Chișinău, Moldova

5. OSMOCHESCU, N. *The right to a healthy environment in the Republic of Moldova – constitutional regulations.* In: Integration through research and innovation. Legal Sciences. Economics. September 26-28, 2013, Chisinau. Chisinau, Republic of Moldova: CEP USM, 2013, pp. 156-158.
6. ODAINIC, M. *Ecological* purchases - *one of the premises of insurance human right to a healthy environment*, pp. 51-58. [online]. [viewed: 02.11.2023]. Available from: <https://ibn.idsi.md/sites/default/files/imag_file/51-58_17.pdf>.
7. Public procurement: legal provisions and work practices. [online]. [viewed: 12.11.2023]. Available from: <https://tender.gov.md/sites/default/files/achizitii_publice_seminar_aap_legea_131.pdf>
8. Ecological public procurement in the EU space. [online]. [viewed: 10.11.2023]. Available from: <https://anap.gov.ro/web/achizitiile-publice-ecologice-in-spatiul-ue/>.
9. BOGUȘ, A. *Efficiency of the public acquisition system by consolidating the role of the security of the civil society.* [online]. [viewed: 03.11.2023]. Available from: <https://ibn.idsi.md/sites/default/files/imag_file/416-422_0.pdf>.
10. The National Development Strategy "Moldova 2030" [online]. [viewed: 10.11.2023]. Available from: <https://gov.md/ro/moldova2030>.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.23
International Conference, December 07-08, 2023, Chişinău, Moldova

EXAMINING THE ECONOMIC RESILIENCE AND SUSTAINABILITY OF TOURIST BUSINESSES: AN ASSESSMENT OF THE FACTORS INFLUENCING ECONOMIC SECURITY IN THE TOURISM SECTOR

Mariana STOICA

PhD, Associate professor,
State University of Moldova, Moldova,
ORCID 0000-0002-1624-7353
E-mail: stoicamarianamd@gmail.com

Abstract: *This scientific article aims to examine the economic resilience and sustainability of tourism businesses by assessing the factors influencing economic security within the tourism sector. The study provides a comprehensive analysis of the various determinants that contribute to the economic security of tourism businesses, considering both internal and external factors. By conducting a thorough literature review and utilizing empirical research methods, the authors identify key elements that impact the economic resilience and sustainability of tourism businesses, such as government policies, market demand, environmental considerations, technological advancements, and socio-cultural aspects. The findings of this research will contribute to a better understanding of the intricate dynamics involved in maintaining economic security within the tourism sector, thereby assisting policymakers and industry stakeholders in developing strategies and initiatives to promote long-term viability and growth in this important sector.*

Keywords: *tourism sector, sustainability, economic security, resilience, strategies, growth.*

UDC: *338.48:338.246.2*

JEL Classification: *Z38, Z 32, L83.*

INTRODUCTION

The tourism industry has emerged as a vital driver of economic growth and development worldwide. Its significant contributions to employment generation, foreign exchange earnings, and infrastructure development have made it a cornerstone of many economies. However, the sector is not without challenges, including the effects of political instability, environmental concerns, market fluctuations, and technological advancements. To ensure the long-term resilience and sustainability of the tourism sector, it is critical to understand and assess the factors that influence economic security within tourism businesses.

This article aims to examine the various factors that play a crucial role in determining the economic security of tourism businesses. Economic security refers to the ability of tourism businesses to withstand external shocks and crises, adapt to changing market conditions, and recover swiftly from disruptions. Achieving economic security is essential not only for safeguarding the livelihoods of those employed in the tourism sector but also for sustaining the overall growth and prosperity of the industry.

To analyze the factors influencing economic security in the tourism sector comprehensively, this article adopts a multidimensional approach. These factors include political stability and security, environmental sustainability, market diversification, technological innovations, human resources and skills development, infrastructure development, and effective governance and policy frameworks. By analyzing these dimensions, policymakers and industry stakeholders can gain insights into the key drivers of economic security and devise strategies to enhance the sector's resilience and sustainability.

DOI: https://doi.org/10.53486/escst2023.23
International Conference, December 07-08, 2023, Chișinău, Moldova

While previous studies have examined some of these factors individually, this article seeks to integrate them into a comprehensive framework that encompasses the diverse aspects of economic security. By doing so, it will not only provide a holistic understanding of the challenges faced by tourism businesses but also facilitate the identification of effective solutions and strategies.

Moreover, this article will present a series of case studies that examine real-world scenarios and explore the practices, policies, and innovations adopted by tourism businesses to enhance their economic security. These case studies will shed light on successful approaches, identify best practices, and highlight potential areas for improvement. This practical perspective will offer valuable insights to industry practitioners, policymakers, and academics looking to enhance the resilience and sustainability of tourism businesses.

Ultimately, the findings from this study will contribute to evidence-based decision-making and inform the development of policies and strategies aimed at fostering economic security within the tourism sector. By embracing these insights, stakeholders can ensure the long-term growth and success of the tourism industry while promoting a sustainable and resilient future.

THE ECONOMIC RESILIENCE AND SUSTAINABILITY OF TOURIST BUSINESSES

Economic resilience refers to the capacity of tourism businesses and destinations to withstand, adapt, and recover from shocks and disruptions. In the context of the tourism sector, economic resilience is crucial for maintaining a stable and sustainable business environment. Several studies have explored the concept of economic resilience in tourism, highlighting the role of diversification, flexible business models, and robust destination management strategies in fostering resilience. These studies emphasize the need for proactive measures to mitigate risks and build adaptive capacities within the tourism sector.

Sustainability has become an integral aspect of tourism development, recognizing the importance of balancing economic, environmental, and socio-cultural factors. Numerous studies have examined the sustainable practices adopted by tourism businesses, including resource efficiency, waste management, community engagement, and responsible tourism initiatives. Sustainable tourism practices not only enhance the long-term viability of businesses but also contribute to destination attractiveness and the overall well-being of local communities.

FACTORS INFLUENCING ECONOMIC SECURITY

The economic security of tourism businesses is influenced by various factors, which need to be understood and managed effectively. Political stability and security play a crucial role in attracting tourists and investment, as politically unstable destinations often experience declining visitor numbers. Environmental sustainability is becoming increasingly important, with travelers seeking destinations that prioritize conservation and responsible environmental management. Market diversification, including the identification of niche markets and diversification of source markets, helps mitigate risks associated with overreliance on specific segments or countries. Technological innovations, such as the use of online platforms, social media, and big data analytics, have revolutionized the tourism industry and can significantly impact economic security. Human resources and skills development are essential for ensuring a competent and

DOI: https://doi.org/10.53486/escst2023.23
International Conference, December 07-08, 2023, Chișinău, Moldova

adaptable workforce that can respond to changing market demands. Infrastructure development, including transportation and hospitality facilities, is critical for enhancing the competitiveness and attractiveness of tourism destinations. Finally, effective governance and policy frameworks provide a stable and enabling environment for tourism businesses, promoting investment, and supporting long-term growth.

Overall, the literature highlights the interconnectedness and complexity of factors influencing economic security in the tourism sector. By considering these factors collectively and implementing appropriate strategies, policymakers and industry stakeholders can enhance the resilience and sustainability of tourism businesses.

Several factors influence the economic security in the tourism sector. These factors can have both positive and negative impacts on the stability and resilience of tourism businesses. Here are some examples:

1. *External shocks and crises.*

Natural disasters, political instability, economic downturns, and global pandemics such as COVID-19 can significantly affect the economic security of tourism businesses. These events disrupt travel patterns, decrease tourist arrivals, and disrupt the operations of tourism-related industries.

For example, the global financial crisis in 2008 had a profound impact on the tourism sector, leading to a decrease in travel demand and spending, negatively affecting the economic security of tourism businesses. Similarly, the eruption of Eyjafjallajökull volcano in Iceland in 2010 resulted in a massive disruption of air travel, causing significant economic losses for several European tourism destinations.

2. *Seasonality and fluctuations in demand.*

Many tourist destinations experience seasonal variations in visitor arrivals, which can impact the economic security of tourism businesses. Businesses heavily reliant on peak season revenue may struggle during off-peak periods, leading to financial instability.

For instance, beach resorts in tropical destinations often experience a surge in visitors during the summer months but witness a significant decline in the offseason, impacting the financial health of hotels, restaurants, and other tourism-related businesses.

3. *Destination attractiveness and competitiveness:*

Destinations that have established effective public-private partnerships, implemented crisis management strategies, and fostered cooperation between government and industry stakeholders are better equipped to handle potential threats and ensure the long-term economic security of tourism businesses.

These factors, among others, interact and influence the economic security of tourism businesses in complex ways. Understanding and addressing these factors is vital for promoting resilience and sustainability within the tourism sector. The attractiveness and competitiveness of a tourist destination can greatly influence the economic security of businesses within the sector. Factors such as natural and cultural resources, infrastructure, marketing efforts, and the overall quality of the tourism product contribute to a destination's appeal.

For example, a destination known for its pristine beaches, rich cultural heritage, and well-developed tourism infrastructure is likely to attract more tourists and generate more revenue, thereby ensuring greater economic security for tourism businesses. On the

DOI: https://doi.org/10.53486/escst2023.23
International Conference, December 07-08, 2023, Chișinău, Moldova

other hand, less attractive destinations may struggle to maintain a steady flow of tourists, leading to financial challenges for businesses operating within them.

4. *Diversification and innovation.*

The ability of tourism businesses to diversify their products and adapt to changing market trends plays a crucial role in their economic security. Diversification reduces dependence on singular revenue sources and provides resilience when faced with shocks or changes in demand.

For instance, a hotel that offers additional services like spa facilities, adventure activities, or conference amenities can attract a wider range of tourists and sustain its competitiveness even during periods of low demand.

5. *Collaboration and cooperation.*

The level of collaboration and cooperation among tourism stakeholders, including businesses, government bodies, local communities, and industry associations, significantly influences the economic security of the sector.

6. *Government policies and regulations.*

The policies and regulations implemented by governments have a significant impact on the economic security of tourism businesses. Favorable policies that support tourism development, provide incentives, and ensure a conducive business environment can enhance the resilience of tourism businesses.

For example, tax incentives for tourism investments, streamlined visa procedures, and supportive infrastructure development can attract more tourists, promote business growth, and improve the economic security of tourism establishments.

7. *Technological advancements.*

Technological innovations play a crucial role in shaping the economic security of the tourism sector. The adoption of digital platforms, online booking systems, and customer relationship management tools can enhance operational efficiency, improve marketing strategies, and facilitate better customer experiences.

For instance, a tourism business with a robust online presence and the ability to leverage technology for personalized marketing and direct customer engagement is more likely to thrive in today's digital era, ensuring greater economic security.

8. *Environmental sustainability.*

The sustainable management of tourism resources, including natural and cultural heritage, is essential for ensuring long-term economic security in the tourism sector. The conservation and responsible use of resources not only protect the destination's appeal but also contribute to the overall sustainability of tourism businesses.

For example, implementing sustainable practices such as waste management, energy conservation, and promoting responsible tourism behavior can enhance the reputation of a destination, attract eco-conscious travelers, and contribute to the economic security of businesses that prioritize sustainability.

It's important to note that these factors are interconnected, and their influence on economic security may vary depending on the specific context and characteristics of the tourism industry in a given destination. Addressing these factors in a comprehensive manner is crucial for fostering economic resilience and sustainability in the tourism sector.

DOI: https://doi.org/10.53486/escst2023.23
International Conference, December 07-08, 2023, Chișinău, Moldova

To deduct findings about the economic resilience and the sustainability of the tourism sector, the author is bringing the conclusions of some case studies as it follows:

- ✓ Research conducted by K. Podhorodecka examined the economic resilience and sustainability of tourism businesses in the Maldives. The study found that the Maldives, a popular tourist destination highly dependent on international arrivals, faced significant challenges during the global financial crisis in 2008. However, through diversification strategies such as targeting niche markets, expanding tourism offerings beyond beach resorts, and promoting sustainable practices, the Maldives was able to rebound and maintain its economic security. The study concludes that diversification and sustainable tourism practices are crucial for enhancing the resilience and sustainability of tourism businesses in destinations highly dependent on international visitors [6].
- ✓ After the devastating earthquake in Christchurch in 2011, the tourism sector in New Zealand faced substantial disruptions. A research study by Becken S. et al. examined the economic resilience of tourism businesses in the Christchurch region. The study found that effective crisis management strategies, close collaboration between tourism businesses, industry associations, and government bodies, as well as strong support for the recovery and rebuilding process, played a critical role in ensuring the economic security of the tourism sector. The study concludes that collaborative efforts and effective crisis management are essential for enhancing economic resilience in the aftermath of a major crisis [7].
- ✓ A case study by Guttentag & Smith (2019) focused on the economic resilience of tourism businesses in Barcelona, a destination grappling with overtourism issues. The study explored the relationship between community engagement and the economic security of tourism establishments. It found that businesses that actively engaged with local residents, encouraged sustainable practices, and supported local economic development initiatives were more likely to withstand the negative impacts of overtourism and maintain their economic security. The study concludes that community engagement and responsible tourism practices are vital for sustainable economic growth and resilience in destinations facing overtourism challenges [5].

These case studies highlight the importance of various factors such as diversification, crisis management, collaboration, sustainability, and community engagement in ensuring economic security and resilience in the tourism sector. By studying these real-world examples, researchers and practitioners can gain valuable insights and lessons that can inform strategies to promote sustainable economic development in tourism destinations.

CONCLUSIONS

1. External shocks and crises pose significant threats to the economic security of tourism businesses. The ability to effectively manage and respond to such shocks is crucial for maintaining stability and resilience.
2. Diversification plays a crucial role in enhancing economic security in the tourism sector. Tourism businesses that offer a range of products and services can mitigate risks associated with seasonality and fluctuations in demand.
3. Collaboration and cooperation among stakeholders, including businesses, government bodies, and local communities, are essential for fostering economic

DOI: https://doi.org/10.53486/escst2023.23
International Conference, December 07-08, 2023, Chișinău, Moldova

security in the tourism sector. Public-private partnerships and effective crisis management are key aspects of this collaboration.

4. Sustainable practices, including environmental conservation and responsible tourism behavior, are integral to ensuring long-term economic security. Destinations that prioritize sustainability are more likely to attract tourists and maintain a positive reputation.
5. The role of technology in enhancing economic security cannot be underestimated. Adopting technological advancements, such as online platforms and digital marketing, enables tourism businesses to improve operational efficiency and attract a broader customer base.

These conclusions emphasize the interconnectedness of various factors influencing economic security in the tourism sector and highlight the need for comprehensive strategies that address these factors to promote resilience and sustainability.

BIBLIOGRAPHY

1. TYRRELL, T. J., JOHNSTON, R. J. Tourism sustainability, resiliency and dynamics: Towards a more comprehensive perspective. *Special Issue: Innovation for Sustainable Tourism: BEST EN Think Tank VII (JANUARY 2008),* Vol. 8, No. 1 , pp. 14-24
2. WATSON, Ph., DELLER, S., Tourism and economic resilience. *Tourism economics*, Vol. 28, Issue 5, august 2022, pp. 1193-1215
3. OECD (2022), *OECD Tourism Trends and Policies 2022*, OECD Publishing, Paris, https://doi.org/10.1787/a8dd3019-en.
4. OECD GLOBAL FORUM ON TOURISM STATISTICS, KNOWLEDGE AND POLICIES, Reshaping tourism for a more resilient and sustainable tomorrow, OECD, 3-5 November 2021. Available from: Final Draft: Guidelines for resilient, sustainable and inclusive tourism (oecd.org)
5. GUTTENTAG, D. Transformative experiences via Airbnb: Is it the guests or the host communities that will be transformed? *Journal of Tourism futures*, ISSN: 2055-5911, Vol. 5 No. 2, 2019, pp. 179-184. https://doi.org/10.1108/JTF-04-2019-0038
6. PODHORODECKA, K. Tourism economies and islands' resilience to the global financial crisis. *Island Studies Journal*, 13(2), 2018, pp.163-184
7. BECKEN, S., SCOTT, N., RITCHIE, B., The Development of New Tourism Networks to Respond to and Recover from the 2011 Christchurch Earthquake, *Tourism crisis and disaster management in Acis-Pacific.* DOI:10.1079/9781780643250.0190

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chișinău, Moldova

INNOVATIONS IN TOUR OPERATIONS AS A RESPONSE TO GEOPOLITICAL CHALLENGES IN CREATING TRANSCORDON ROUTES

Svitlana TYMCHUK

PhD, Associate Professor,
Uman National University of Horticulture, Ukraine,
ORCID 0000-0003-0331-1173
E-mail: svtumchyk@gmail.com

Liudmyla NESHCHADYM

PhD, Associate Professor,
Pavlo Tychyna Uman State Pedagogical University, Ukraine
E-mail: n_lydmila@ukr.net

Iryna KYRYLIUK

PhD, Associate Professor,
Pavlo Tychyna Uman State Pedagogical University, Ukraine
ORCID 0000-0001-9814-195X
E-mail: i.kyryluk@udpu.edu.ua

Abstract: *This article examines the innovative strategies employed by tour operating companies in response to geopolitical challenges, particularly focusing on the creation of transborder routes. In a world marked by geopolitical transformations, the tourism industry faces diverse risks that necessitate adaptive measures from tour operators. The study assesses the risks linked to transborder tourist routes and investigates the proactive role of tour operators in mitigating these challenges.*

Geopolitical factors, such as political and economic instability, terrorism threats, diplomatic disputes, migration crises, and changes in infrastructure and access, significantly impact the safety and stability of transborder routes. The article highlights the dynamic nature of these challenges and emphasizes the need for flexible and responsive strategies from tour operators.

In this context, the research delves into the role of technological innovations, including digital technologies, the Internet of Things (IoT), artificial intelligence (AI), and blockchain, in enhancing the quality, safety, and adaptability of transborder tourist routes. It explores how these technologies contribute to efficient logistics, personalized tourist experiences, and real-time analysis of geopolitical risks.

Furthermore, the article discusses the importance of collaboration among stakeholders in the tourism industry. It underscores the significance of information exchange and best practices among tour operators to overcome geopolitical challenges effectively. The study concludes by emphasizing the critical role of innovation in ensuring the sustainability and success of tour operators amidst geopolitical uncertainties.

Keywords: *innovations in tourism, tour operating, geopolitics, transborder routes, tourism industry, technologies, blockchain.*

UDC: *[338.482:005.591.6]:005.334*

JEL Classification: *O32, F50, R58.*

INTRODUCTION

In a world where geopolitical transformations not only become an inevitable reality but also emerge as a defining factor in the global economy and international relations, the tourism industry finds itself at the epicenter of these changes. Open borders and

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chișinău, Moldova

transborder routes, serving as bridges between cultures and nationalities, often become subjects of strained geopolitical relations, necessitating a balanced and innovative response from tour operating companies.

There is an escalation of conflicts, shifts in political alliances, and economic instability that impact the tourism industry through restrictions, sanctions, and other geopolitical challenges. In this context, innovations in tour operating are identified as a key element for successful resilience and adaptation to changes, ensuring the stability and efficiency of transborder tourist routes.

DISCUSSIONS AND RESULTS

Geopolitical factors significantly impact the tourism industry, shaping the circumstances and conditions for the development and functioning of transborder tourist routes. Some key aspects include international relations, political conflicts and instability, trade and economic factors, trade agreements, economic relations, and geographic changes.

Changes in political alliances and diplomatic relations between countries can affect tourist flows. Simultaneously, political events such as the imposition of visa restrictions or political conflicts may restrict access to certain regions. Positive changes in international relations stimulate tourist flows by promoting transborder cooperation and the development of joint tourism initiatives.

In the context of unfolding political conflicts, key factors are the safety of tourists and the mitigation of various risks. The deployment of political conflicts, terrorist threats, or economic instability leads to a reduction in tourist demand and restrictions on the movement of tourists through specific transborder routes. Additionally, the imposition of international sanctions often limits the opportunities for tourism enterprises and affects their collaboration with other countries.

Trade and economic factors also play a crucial role in tourism. Changes in exchange rates and economic difficulties impact the cost of travel and the choice of transborder routes for tourists. Furthermore, trade agreements and economic relations between countries can stimulate tourism by facilitating visa regimes and increasing tourist services.

Therefore, relying on numerous studies in the field of tourism conducted by UNWTO, the international share of all trips is expected to reach an impressive figure of 1,800 billion by 2030, from 1.4 billion since COVID-19. It is noteworthy that despite this, international travel was only accessible to 5-7% of the world's population at that time, as indicated by small print publications [2].

Geopolitical transformations sometimes provoke geographical changes, leading to specific environmental and migration processes. Climate change and natural disasters adversely affect the accessibility and attractiveness of certain transborder regions for tourists. A negative phenomenon in these processes remains population migration, influencing the cultural and social dynamics of regions, which may impact tourist interests and demand. Therefore, geopolitical factors shape and define the tourism industry, including the consideration of transborder routes and the response of tour operating companies to these challenges.

In the modern world, where geopolitical turbulence is not only the focus of politicians and diplomats but also a significant factor influencing the global economy and sociocultural relations, the tourism industry finds itself in a particularly complex situation. Political conflicts, sanctions, terrorist threats, and economic instability can have a considerable impact on transborder routes, which serve as the foundation for the operation

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chișinău, Moldova

of tour operators. Changes in international relations, political conflicts, and other geopolitical phenomena can trigger not only economic and political challenges but also force tour operators to reconsider their approaches to safety and route planning.

The most complex and multi-stage process is the innovative implementation of the tourist product (updating the manufactured product) and the technological process of creating the tourist product (updating the technology). It is during its implementation that the features and difficulties faced by tour operators are most fully defined [5].

In the context of contemporary geopolitical instability, tour operators face challenges that require not only adaptation but also strategic reconsideration of their activities. Geopolitical turbulences, such as political conflicts, sanctions, terrorist threats, and economic instability, inevitably impact tourist routes, determining both their safety and stability.

Despite geopolitical challenges, there is a group of tourists who can always afford to travel. According to a UNIDO study conducted earlier this century, three groups of travelers are distinguished: the elite, the banking circle, and those effectively excluded from the global system (Henryk F. Handszuh, 2023). Global events and conflicts influence the choices of such tourists and shape their expectations. Tour operators are tasked with ensuring the safety of their clients and maintaining the attractiveness of routes even in unpredictable conditions.

Tour operators, in turn, seek to respond to geopolitical transformations by developing strategies aimed at preserving the safety and resilience of their routes. This includes reviewing partnership relations, implementing security technologies, and developing crisis management plans [6].

To overcome geopolitical challenges and effectively adapt to changes in modern tour operating, various innovative approaches are utilized. The aspects studied and employed in this field are outlined in Figure 1.

The use of modern technologies allows tour operators to ensure more precise tracking of routes and tourist safety. IoT can be utilized to monitor group movements, control safety conditions, and exchange real-time data. Artificial intelligence algorithms are employed to analyze geopolitical trends and forecast potential impacts on the tourism industry. Additionally, data analytics enables tour operators to make informed decisions and adapt to changes in real-time.

The use of geodata for personalizing marketing strategies is relevant for the work of tour operators. Furthermore, location data analysis allows tour operators to create targeted offers and individual routes, considering geopolitical conditions.

In the era of digital technologies and big data, the use of geodata becomes a key element of an effective marketing strategy in tourism. This approach allows tour operators not only to better understand their clients but also to create personalized and targeted offers, taking into account geopolitical and location conditions. Geodata allows collecting client location data. Tour operators can use this information to create personalized offers, considering individual interests and needs of tourists. Geodata helps identify demand and popular locations, which can be used for effective audience segmentation and the creation of specialized tours.

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chișinău, Moldova

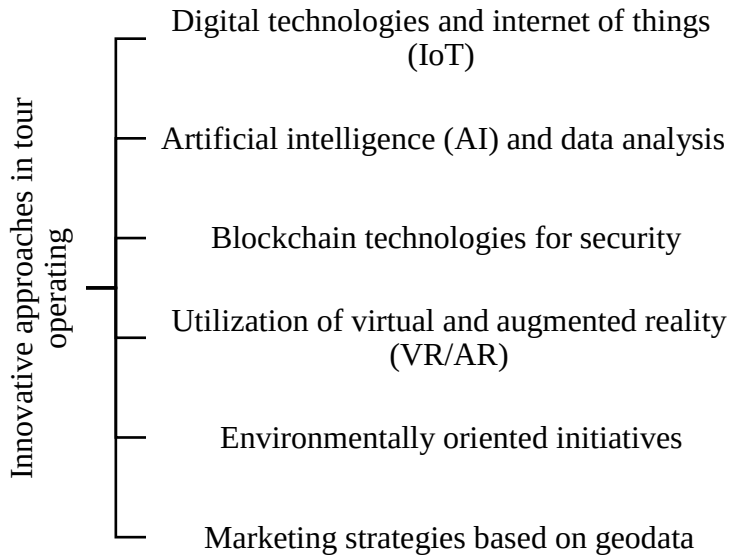


Figure 1. Innovative approaches in tour operating amid geopolitical challenges
Source: author's development

Geodata also allows analyzing and predicting changes in geopolitical conditions and adapting marketing strategies accordingly. This facilitates a more responsive approach to challenges and opportunities. The use of geodata for creating interactive routes and excursions that can be accessed through mobile applications or websites. Through geodata, advertising campaigns targeting specific locations can be organized, making them more effective and ensuring a higher level of interaction.

Geodata can be used to interact and attract the audience through social media, utilizing geotagging and location-based features. The use of geodata in the marketing strategies of tour operators contributes to the increased effectiveness of advertising campaigns, audience expansion, and the creation of unique personalized routes that meet modern tourist demands and expectations.

The use of blockchain technology for ensuring the security and tracking of transactions is beneficial in providing information transparency, preventing fraud, and enhancing trust in tour operator services. Blockchain technologies are known for their reliability, resistance to manipulation, and the ability to create decentralized and secure systems. The use of blockchain in tourism can significantly improve the security and tracking of transactions, influencing trust and information openness. Additionally, blockchain can establish a secure and transparent mechanism for processing and storing tourists' personal data, ensuring their confidentiality and integrity.

Recording all operations and rewards in the blockchain makes the loyalty system more transparent and resistant to manipulation. Blockchain allows tracking the supply chain of products and services, determining their origin and quality. It also enables the creation of unique and immutable records of tours and packages, avoiding falsification and ensuring the accuracy of information. Recording personal data and documents in the blockchain ensures their security and immutability. Using blockchain for forming secure and immutable contracts in booking systems. Nowadays, most tourist and transportation organizations have transitioned to electronic documents, enabling the creation of contracts and issuance of travel documents to tourists without leaving home or the office [1]. All

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chișinău, Moldova

these aspects contribute to ensuring a high level of security in tourism, reducing the risk of manipulation and fraud, and enhancing trust among participants in the tourism process. Creating virtual tours and interactive explorations for tourists remains relevant today to increase interest and attractiveness of transborder routes, even during periods of geopolitical turbulence. In modern tourism, virtual and augmented reality technologies play a crucial role in creating unparalleled tourist experiences and drawing attention to transborder routes, especially during periods of geopolitical turbulence. Key aspects of using VR/AR in tourism include virtual tours and excursions, interactive explorations, virtual museums and architectural objects, promoting lesser-known places, tourism marketing and advertising, tour products, and route planning.

The creation of virtual tours allows tourists to visit landmarks, museums, or natural areas without leaving their homes, which is particularly relevant during periods when physical mobility is limited. The use of AR to overlay information on the real world enables tourists to obtain additional data about the history, architecture, and cultural features of a specific region. Additionally, creating virtual museums and architectural objects allows tourists to enjoy cultural heritage without being physically present.

VR/AR can be used to present lesser-known or exotic places, contributing to the expansion of the tourism potential of different regions. Creating immersive virtual stories and advertising campaigns enhances emotional engagement with a specific route or region. Using AR for virtual placement of objects and determining optimal routes for travel.

Given the limitations of physical movement during geopolitical turbulence, VR/AR serve as important tools for attracting tourists and maintaining interest in transborder routes. These technologies create opportunities for impressive and safe virtual journeys, contributing to the preservation and development of the tourism industry amid uncertainty [3].

Modern tourism is confronted with a growing understanding of the importance of nature conservation and sustainable development. In response to this, tour operators worldwide are increasingly focusing on the development of environmentally friendly and sustainable routes that not only meet the needs of tourists but also actively contribute to the preservation of natural resources and ecosystems. Key aspects of development include environmentally friendly transportation, energy-efficient hotels and infrastructure, water resource conservation, local cooperation, and social responsibility, education and ecopedagogy, as well as environmentally friendly activities and experiences. The ecological efficiency of tourist movement and entrepreneurship helps preserve and gradually restore the integrity of the environment and cultural heritage [5].

The development of eco-friendly routes not only ensures the sustainability of natural resources but also creates competitive advantages for tour operators actively implementing such approaches. Tourists are increasingly interested in vacationing in places where ecological cleanliness is maintained, and nature is supported and protected. The development of environmentally friendly and sustainable routes is an important step towards more responsible and ecologically sustainable tourism. The balance of all components of sustainable tourism development as a socio-ecological-economic system. There are limitations in the exploitation of natural tourist-recreational resources in developing countries, to some extent relative, as they are related to the biosphere's ability to cope with the consequences of human activity [4].

These innovative approaches enable tour operators to effectively counter geopolitical challenges, ensuring the safety and stability of transborder routes while simultaneously creating new opportunities for development and competitiveness. Any innovative

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chișinău, Moldova

processes in the tourism industry at the regional level serve as a mechanism for investment activity throughout the tourism sector. For the tourism sector, the implementation of innovative processes should be based on the concept of project management as the most flexible system that adequately influences changes in the external environment, especially in a market economy [4].

In a world undergoing constant geopolitical and economic changes, tourist routes become vulnerable to a vast spectrum of risks. Transborder tourist routes, extending across country and regional borders, pose unique challenges and dangers, particularly in times of geopolitical tensions. Recognizing and properly addressing these risks are crucial tasks for the tourism industry, governmental structures, and tourists themselves. In the context of geopolitical tensions, travel can become not only a source of pleasure but also a challenge to safety, stability, and comfort. Furthermore, tour operator activities are controlled by global corporations and conglomerates, typically having the character of integrated structures [1].

Geopolitical tensions can significantly impact tourist routes, creating challenges for their safety and stability. In a climate of uncertainty and changes on the global stage, tourism becomes an industry that requires not only creative approaches to development but also sophisticated risk management strategies. Effective management of these risks demands concerted efforts from authorities, tour operators, and local communities. National and regional authorities must study and respond to changes in the geopolitical environment, developing strategies aimed at supporting and protecting tourist routes (table 1).

Table 1. Risks of transborder tourist routes in conditions of geopolitical tensions

Risks	Description
Political and economic Instability	Political and economic turbulence affect the safety and stability of routes, altering conditions for tourists and businesses.
Terrorist threats and security	Geopolitical conflicts increase the risk of terrorist threats, casting doubt on the safety of tourists on transborder routes.
International relations and diplomatic disputes	Diplomatic disputes lead to restrictions on transborder routes, causing uncertainty for tourists and businesses.
Migration crises and border security	Migration crises put pressure on border security and result in changes to routes.
Infrastructure and access changes	In conditions of geopolitical tensions, there may be alterations to infrastructure and restrictions on access to certain territories, impacting tourist routes.
Currency risks and economic limitations	Changes in the economy and currency exchange rates affect the cost and availability of tourist services.
Environmental and conservation issues	Geopolitical conflicts worsen the environmental situation and lead to restrictions for tourists.
Changes in migration and visa policies	Changes in migration policies complicate the travel process and reduce the attractiveness of transborder routes.

Source: author's development

Tour operators, in turn, must be flexible and responsive to geopolitical transformations, seeking new opportunities, and implementing innovative methods to ensure the safety and stability of their routes. Collaboration among tour operators, based on information exchange and best practices, can prove crucial in overcoming geopolitical challenges.

The diversity of our world unites us and provides an opportunity to explore, utilize, and experience the best that local cultures and communities have to offer. This is especially true for developing countries, contributing to job creation (especially for women

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chișinău, Moldova

and youth), enabling people to build better lives, generating resources for the protection of cultural heritage and the environment, fostering the revitalization of rural and urban areas, bringing people together, and making us better [5]. Therefore, local communities also play a crucial role in ensuring the stability and safety of tourist routes. Involving citizens in planning and problem-solving processes can contribute to mutual understanding and support, promoting the development of sustainable tourism that takes into account the interests of all stakeholders. Thus, the harmonization of efforts among various stakeholders in the tourism industry is a significant step in preserving and developing transborder tourist routes in times of geopolitical turbulence.

In today's world, where geopolitical turbulence and changes in international relations pose a considerable challenge to the tourism industry, the use of technology becomes a crucial factor in ensuring the stability and quality of transborder tourist routes. In the context of geopolitical challenges, technology plays a vital role in creating safe, accessible, and exciting transborder routes. Digital tools allow not only the optimization of logistics and marketing for tour operators but also the improvement and personalization of the tourist experience itself.

Technology plays a defining role in the development of transborder tourist routes amid geopolitical challenges, and its impact is crucial for enhancing the quality and safety of the tourist experience in conditions of geopolitical instability. Studying the role of digital technologies, artificial intelligence, and other innovations becomes a necessary aspect of scientific research in this context. Digital technologies, such as mobile apps, web platforms, and geospatial systems, enable tourists to receive up-to-date and personalized information about transportation, attractions, restaurants, and other objects on the route. This contributes to the convenience and safety of travel, helping tourists avoid potential dangers and difficulties associated with geopolitical turbulence.

Artificial intelligence, in turn, can be used to analyze large volumes of data on geopolitical events and risks in real-time. Machine learning algorithms can predict possible consequences and provide recommendations for the optimal route in conditions of geopolitical instability, thereby ensuring effective risk management for tourists.

Innovative approaches, such as the use of virtual and augmented reality to create secure virtual tours or blockchain technology to enhance the security and transparency of transactions, are also crucial aspects that can improve and ensure the tourist experience in geopolitically unstable conditions. In the context of geopolitical transformations, the tour operator business is presented with significant opportunities that can contribute to the development and strengthening of their positions in the market. Examining the advantages and opportunities for tour operators in geopolitically complex regions can serve as a foundation for forming strategies that promote the sustainable and successful operation of the agency (figure. 2).

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chișinău, Moldova

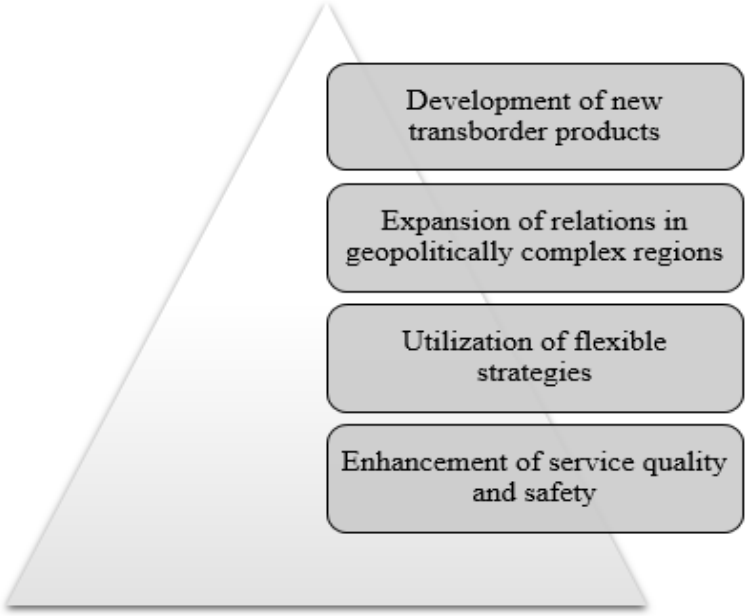


Figure 2. Opportunities for the operation of tour operators in geopolitically complex regions.
Source: author's development

Geopolitical transformations can serve as a stimulus for tour operators to develop and offer new transborder products. Identifying unique routes that take into account changes in political and economic conditions allows not only to increase competitiveness but also to attract a new segment of tourists.

In the context of geopolitical transformations, tour operators have opportunities to expand partnerships in regions where others may see only risks. Establishing and improving collaboration with local businesses, non-governmental organizations, and governmental structures can contribute to resolving difficulties and ensuring stability in the business.

Geopolitical transformations require flexibility and quick responsiveness to changes from tour operators. The use of flexible strategies allows adapting tour packages to changing circumstances, quickly entering new markets, and adjusting products to meet tourist demands. In times of geopolitical transformations, tourists prioritize the quality and safety of their travels. Tour operators can leverage innovative technologies, such as security and monitoring systems, to ensure a high standard of service and protect tourists from potential risks. All these opportunities create perspectives for the tour operator business in geopolitically unstable conditions, demanding not only adaptation but also active formulation of strategies to maximize positive outcomes.

CONCLUSIONS

Therefore, geopolitical factors exert a significant impact on the tourism industry, determining the conditions and opportunities for the development of transborder routes. International relations, political conflicts, sanctions, and other geopolitical phenomena create a turbulent environment in which tour operators and other industry participants operate.

DOI: https://doi.org/10.53486/escst2023.24
International Conference, December 07-08, 2023, Chişinău, Moldova

Tour operators, in turn, respond to geopolitical turbulence by implementing innovative strategies and practices. They actively leverage new technologies, study market trends, and adapt their services to changing conditions.

Innovations in tour operating become a key tool for overcoming geopolitical challenges. The use of advanced technologies, marketing strategies, and innovative approaches helps tour operators adapt to changes in the geopolitical environment and ensures the stability of their business processes.

Transborder tourist routes, despite their development potential, carry risks in the conditions of geopolitical tensions. Analyzing these risks is necessary for effective management and minimizing potential negative consequences. Meanwhile, technologies emerge as a crucial catalyst for the development of transborder routes in the face of geopolitical challenges. Using geodata, blockchain technologies, virtual and augmented reality allows ensuring safety and providing an innovative experience for tourists.

Overall, geopolitical transformations pose challenges for the tour operator business, but at the same time, they open a wide range of opportunities for those who are ready to respond innovatively to changes in the global tourism environment.

BIBLIOGRAPHY

1. ATAMANCHUK Z. *The network tourist industry formation asa form of global integration of countries* [online]. Economic space, (141), 2019 P. 49-64. [viewed 26 november 2023]. Available from: <http://www.prostir.pdaba.dp.ua/index.php/journal/article/view/6>
2. HENRYK F. HANDSZUH. *The prospects of tourism in its geopolitical context* [online]. Tourism, crises and innovations. 2023 [viewed 27 november 2023]. Available from: <https://doi.org/10.4000/etudescaribeennes.28054 >
3. HUMENIUK V., KAZIUKA N., SHEKETA Y., SEMYRGA L. *Information technologies as a mean of modernization of tour operating and innovative development of the hotel and restaurant business*. *Galician economic journal (*Tern.), 2023, vol. 81, no 2, pp. 106-114. ISSN: 2409-8892
4. PIDVALNA O., BOGUSLAVSKA S. *Development of the modern tourism industry in the region on the basis of innovative processes* [online]. Economic space, 2021, (168), P. 93-96. [viewed 27 november 2023]. Available from: < https://doi.org/10.32782/2224-6282/168-16>
5. PODLEPINA P. O. *The impact of international tourism on the contemporary priorities of sustainable development in developing countries. Collection of scientific papers of Cherkasy State Technological University. Series: Economic sciences*. 2019, № 54. С. 17-24. ISSN 2306-4420
6. TYMCHUK S., KOZHUKHIVSKA, R.B. *The Role of Tour Operators in Ensuring Tourism Security and Promoting Peace and Stability through Military Tourism* [online]. Economics and Society. 2023, Issue 52. [viewed 28 november 2023]. Available from: <https://economyandsociety.in.ua/index.php/journal/article/view/2531/2450 >

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.25
International Conference, December 07-08, 2023, Chişinău, Moldova

SECURITY IN TOURISM

Mihaela TUDORICĂ

PhD student,
Doctoral School of Economic Sciences, University of Oradea, Romania,
ORCID 0000-0002-0776-9950
E-mail: ellatudorica@yahoo.com

Abstract: *Until recently, the tourist market was actually a physical space, where the seller of tourist packages and the buyer met and the transaction was carried out. So the contacts were physical both locally and internationally. Security meant, therefore, to protect people from extremely tangible threats such as theft, fraud, etc. But now we face different challenges because the tourism market is becoming a cyberspace where sellers, intermediaries and buyers can meet without the need for physical contact. Security therefore has a different meaning, as we need to protect ourselves from cyber threats that can materialize in identity theft, internet fraud, etc. So, in order to deal with the problems that appear, and which may not have attracted much attention from experts, we want to study the importance of cyber security for the development of tourist destinations.*

Keywords: *Cyber Security, Safety, Tourism, Destination.*

UDC: *[338.48:004.056.5]:005.334*

JEL Classification: *F52, M15, O33, Q55, Z32.*

INTRODUCTION

We all realize how important cyber security is to economic development. People want to be able to exchange goods and services only if they themselves feel protected against violence and abuses of power; Without security, a market economy cannot flourish. Security must also mean protecting people from cyber threats. This new challenge involves all cyberspace users: public authorities, ordinary citizens, companies. All over the world, schools and universities are actively involved in educational programs that aim to increase the awareness of citizens and organizations exposed to cyber threats, all of which can be achieved by implementing new security plans. By the term cyberspace we mean the complex of all interconnected hardware and software infrastructure, starting with the Internet and including data and mobile devices. We view cyber threats as a complex of malicious behaviors that can be perpetrated throughout cyberspace.

SAFETY AND SECURITY - DEFINITION & DIFFERENCES

Idso and Jakobsen (2000, citing Albrechtsen 2003) from the Norwegian University of Technology and Science defines safety as protection against unintended incidents and security as protection against incidents where people act deliberately [1].

In the New Oxford Dictionary, Pearsall and Hanks (2001, citing Albrechtsen 2003, p. 2) explain safety as "the condition of being protected so that you are unlikely to be in danger of risk or injury" and security is defined as “the state of not being in danger. or threat".

Albrechtsen (2003) also says that the thought behind both of the terms is to take care of people by eliminating any hazards and threats and ensuring a safe and secure environment. Furthermore she states that the difference between them is that safety is concerned especially with the protection of human lives and health while security adverts to the protection against criminal activities.

DOI: https://doi.org/10.53486/escst2023.25
International Conference, December 07-08, 2023, Chișinău, Moldova

As safety science involves the well-being of human people in every aspect of their lives it has its roots in high-risk industries such as nuclear plants were human caused and technological failures often occur. Nowadays this area is wide spread because of ongoing improvements within these sectors and international tourism may often be the carrier for catastrophes like outbreaks of epidemic plagues.

Albrechtsen (2003) furthermore explains that safety incidents do not only endanger the overall level of humans' well-being but also material objects as well as the environment might be affected. Moreover she argues that incidents within the field of safety are often unplanned criminal acts that derive from a thoughtless action.

In this case, most people act deliberately without the intention to achieve a particular effect. Due to the fact that these hazards are often tangible and observable it makes it easier to get a general idea of the problem and therefore makes it easier to prevent or at least control them (Albrechtsen, 2003).

The field of security is more complex and for that reason it makes it more difficult to control it. As Albrechtsen, 2003 states "today the field covers everything from personal to national security including financial crime, information protection, burglary and espionage among others."

In addition Albrechtsen (2003) points out that any incident within the field of security is a planned act caused by the motivation of an individual or a group.

In contrast to safety, security acts are malicious, criminal actions planned by people with the ulterior motive to achieve a wanted outcome.

The high level of uncertainty on security threat is often created through interaction that cannot be foreseen, and is therefore difficult or impossible to predict. (Albrechtsen, 2003).

A NEW APPROACH AND DEFINITION OF SAFETY AND SECURITY IN THE ERA OF GLOBAL TOURISM

Security and safety issues have been addressed by tourism researchers such as an element of major importance in tourism. Michalkó characterized security as a fundamental condition of hosting tourists, while others realized the changes occurring in global security [2]. Security has undergone a significant change from a more or less passive factor to an extremely active element of tourism, creating an imperative need to act to protect tourists and their goods as well as the entire industry.

Despite the achievements in studying security and safety issues in tourism, there are several challenges for tourism researchers specializing in this field:

- consequences of the indivisibility of security issues in the global world;
- security issues created by the Internet;
- security in travel and tourism versus human freedom and rights.

Research and education in tourism and hospitality must deal with the new issues of security and safety in tourism so as to prepare future industry specialists by incorporating new research themes into academic programs. This could be done by introducing new topics (e.g. risk management in tourism) or supplementing existing content with security and safety topics.

THE RELATIONSHIP BETWEEN SECURITY AND TOURISM DESTINATIONS

So, the real tourism product is the destination. We define tourist destination as a large or small physical space with lots of attractions. Prospective tourists leave their place

DOI: https://doi.org/10.53486/escst2023.25
International Conference, December 07-08, 2023, Chișinău, Moldova

of residence for a short period of time and venture on a dream trip because they are attracted to a certain destination, be it cultural, natural, recreational or otherwise.

Destinations can be extremely different and can be analyzed in many ways. Perhaps the most important criterion that should make the difference is the nature of the tourism product. There are corporate destinations and community destinations. The first category is similar to businesses, including theme parks or ski resorts, so corporate destinations only offer a service, managers aim for the efficient allocation of resources, in the second category we are talking about public goods, common resources, etc.

According to the World Economic Forum (2013), the competitiveness of tourism systems is closely related to: prices, natural resources, cultural resources, safety and security, and ICT infrastructure [3].

We believe that cyber security is a new challenge for the tourism economy. In fact, if the actual tourism product is a destination, and if a destination is a mixture of different tourism goods and services, then it is easy to realize that many of these goods and services are exposed to cyber threats.

Let's imagine a typical trip, where the tourist buys using travel intermediaries, transport services and accommodation, therefore uses several applications and wi-fi devices, each of which is exposed to a cyber threat.

To assess and monitor cyber security in tourism it would be interesting to develop some special tools. For example, it would be useful in the tourism sector to select a few companies to provide us with some cyber security indices in this field, the companies should provide information on intermediaries, transport, accommodation, food and agreement.

So competitiveness depends on several factors, including safety and security that must also be extended in cyberspace.

In fact, as we have seen, the following aspects appear:

a. the destination, which is the real tourist product, offers a variety of goods and services mostly exposed to cyber threats, so it is no longer enough to protect tourists only from physical attacks;
b. the cyber threat seems to be continuously expanding over the entire economy, including the tourism sector;
c. cyber threats can only be countered with a new and broader policy built on greater awareness among all actors interested in playing a role in the economic market.

Tarlow correctly argued that in tourism it is difficult to distinguish between safety and security and it is more appropriate to use the term guarantee. Thus we try to show the relevance of the guarantees we seek both in terms of physical security and in the case of cyber security.

Perhaps we should even add that in this case, it is difficult to establish the limits of the two dimensions, because the attackers also use cyber tools in the physical space. So the first step is awareness: "Be aware, be safe."

CONCLUSIONS

Considering the different factors that influence tourists' travel decision, it can be seen that both tourism and personal characteristics play a major role in the decision-making process.

The stability of a destination's political situation has been shown to have a great influence on tourists' travel decision, as pointed out by Sönmez and Graefes (1989), so political instability could be an obstacle to tourism demand. Since risk perception also

DOI: https://doi.org/10.53486/escst2023.25
International Conference, December 07-08, 2023, Chișinău, Moldova

plays a crucial role in the decision-making process, it can be concluded that safety and security are important issues for tourists [4].

The fact that consumer behavior is strongly shaped by the image of a destination, as stated by Bolan and Williams (2008), cannot be verified because it seems to have only a slight influence on the decision-making process [5].

Risk perceptions are strongly shaped by external communication channels such as the media, friends and relatives, and travel intermediaries. Although the media and recommendations from friends and relatives have been shown to have a major influence on knowledge of potential risk factors in this region, travel intermediaries do not seem to be among the significant sources of information in this context.

The importance of safety in the travel industry needs to be highlighted. The travel industry as a tourist industry has a strong and direct impact on all other sectors of tourist activities, such as accommodation, catering, conference tourism, and also on other sectors of the economy that depend on business trips and visits.

If in a particular country or a destination a security crisis occurs, it has a great impact on tourism. The desire of every tourist industry is to restore the confidence of tourists and safety in their country or destination as soon as possible after such crisis.

The more the destination's (country, region) administrative, technical, social and political environment is regulated and stable, the easier it will be to cope with preventive measures for safety crises or counter the consequences of the crises and create the original state.

BIBLIOGRAPHY

1. ALBRECHTSEN ENHED, *Security vs. Safety*. NTNU-Norwegian University of Science and Technology. Department of Industrial Economics and Technology Management, 2003.
2. MICHALKO GÁBOR, *Turizmusföldrajz és humánökológia*, KJFMTA Földrajztudományi Kutató Intézet, Budapest-Székesfehérvár, 2005.
3. WORLD ECONOMIC FORUM. *The Travel & Tourism Competitiveness Report 2013*, Geneva, 2013.
4. SOMNEZ SEVIL and GRAEFE R. ALAN, *Influence on Terrorism Risk on Foreign Tourism Decisions*. Annals of Tourism Research, 25 (1), 112-144, 1998.
5. BOLAN PETER and LINDSAY WILLIAMS, *The role of image in service promotion: focusing on the influence of film on consumer choice within tourism. International Journal of Consumer Studies*, Vol. 32, Issue 4, pp. 382-390, 2008.
6. TARLOW E. PETER, *Tourism Security. Strategies for Effectively Managing Travel Risk and Safety*, London: Elsevier 2014.

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chişinău, Moldova

ETHICAL CHALLENGES IN MEDICAL SERVICES

Doina-Monica AGHEORGHIESEI

PhD Student
Alexandru Ioan Cuza University of Iasi, Romania,
ORCID
E-mail: agheorghiesei.doina@feaa.uaic.ro

Ana-Maria BERCU

PhD Hab., Professor.
Alexandru Ioan Cuza University of Iasi, Romania,
ORCID 0000-0001-8954-8520
E-mail: bercu@uaic.ro

Abstract: *We live in an era that offers more and more different healthcare alternatives: innovative technologies, high-standard medical interventions, state-of-the-art treatments, all to give people the greatest possible life expectancy. In order to put medical ethics into practice, it is important both to recognize the problems involving ethical norms and principles and to resolve them. The structural and practical challenges of medical ethics lie in policy making and ethical management planning activities.*
Our work proposes to answer the issue of the importance of ethics in the medical sector in the age of new technologies. The research methodology used consists in the study and analysis of specialized literature with a scientific and transparent approach, identifying existing and relevant research of recent date, regarding ethics and ethical challenges in the Romanian medical sector, the security of medical services and the implications regarding the use of artificial intelligence. The preliminary conclusions indicate the need to improve the quality management system in the medical sector, which should be oriented towards the application of ethical principles and norms, especially in the context of the use of new information technologies.

Keywords: *ethics, ethical issues, medical security, artificial intelligence*.

UDC: *614.2:[174+004.8](498)*

JEL Classification: *I23, I25.*

INTRODUCTION

Cognitive and educational challenges in medical ethics can influence the uptake of educational programs aimed at improving the qualitative and quantitative aspects of medical ethics education for health professionals, from students to practitioners.

Patients and their families are concerned about the many challenges faced by the healthcare system, including medical errors, long wait times for diagnostic and treatment services, terminal complications and illnesses for terminally ill patients, and ethical challenges in decision-making in healthcare institutions [1].

Medical ethics is the branch responsible for the principles and values that should govern medical practices. These principles are based on respect for human dignity, patient autonomy, ethics, based on sound principles, do good, do no harm, autonomy and justice, guide health professionals in their mission to treat, care and cure.

Improving the quality of health care services in response to the growing health needs of patients depends on how attentive medical professionals are to ethical principles (Çinar and Eren, 2013) and openness to new technologies [2]. The lack of these could undermine patient's confidence and trust in the community of medical professionals.

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

Our paper aims to identify and analyze some studies on ethics education, ethical issues in the medical sector, security of medical services, including the ethics of artificial intelligence.

The research methodology is empirical and analytical, based on studies and articles that will answer the research question: what are the ethical aspects generated by the education for ethics and the use of artificial intelligence in the provision of medical services?

The paper is structured as follows: introduction, analysis of specialized literature, research methodology, results and discussions, research conclusions.

The paper addresses issues related to the concepts of ethics, ethics education, ethical issues, continuing with an analysis of the role and importance of ethics in the provision of medical services, taking into account both the medical data on patients and the medical records made with the help of new technologies. The issue of artificial intelligence is another point of analysis based on studies and research from the specialized literature.

LITERATURE REVIEW

Education for ethics. Ethical issues.

According to the Explanatory Dictionary of the Romanian Language (DEX, 2016 edition), ethics is the science that deals with the theoretical study of human values and condition from the perspective of moral principles.

Ethics education is essential to the training of doctors and health professionals. Educational disciplines in the faculty and the code of ethics in medical institutions play an important role in preparing doctors to understand and apply ethical principles in their daily work. Medical ethics constantly highlights that medicine is not only a science, but even an obligation towards society.

Considering that the purpose of medical services is to help and heal the sick, doctors can put their knowledge, skills, and dedication at their disposal, not only in the interest of the health of the individual, but also in terms of society, having the moral obligation to follow one's conscience and faith. A conscious attitude towards these assumed duties which arise from the essential conditions of human life constitutes medical ethics.

Ensuring the effectiveness of medical care is based on the ethical principles of the principle of doing good and helps doctors make the right decisions that protect the health and quality of life of their patients. The protection of patients' rights is based on the ethical principles of autonomy and justice that patients can make decisions about their health care and have access to the care they need. Patients' confidence will increase if they can be sure that doctors act responsibly and ethically.

Ethical problems in daily medical practice arise for various reasons and represent a threat to ethical values. If these threats are not managed properly, both patients and employees in the medical sector risk moral and material damage.

When does an ethical problem arise in the medical sector? Usually when one has to recognize what is good or bad, when one has to choose between several options that can have very serious implications for patients. Even the decision to do something or not to do something is an ethical dilemma, the basic principle of ethics in medicine today being the respect for the autonomy of the patient. At least four main ethical principles have been defined in the literature: beneficence (doing good), non-maleficence (doing no harm), autonomy and justice (Varkey, 2021) [3]. Informed consent, truth-telling and confidentiality stem from the principle of autonomy.

Medical ethics is implemented by both the doctor and the patient. Controversies and ethical conflicts arise in the practice of medicine, especially in the decision-making

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

process. Rarely, these conflicts arise in joint decision-making, because such conflicts arise when doctors' and patients' decisions go against medical ethical principles (Astărăstoaie, 2021) [4].

According to the codes of ethics (eg. Code of ethics of Sf. Spiridon Hospital in Iasi, Romania, Code of ethics and professional deontology of the Timișoara Municipal Emergency Clinical Hospital, The Code of Medical Ethics of the American Medical Association) from various healthcare organizations, it is simpler to categorize ethical issues according to the problems that may arise, looking at:

- ***actions:***
  - to do good/to act properly;
  - to do no harm/ to harm no one.
- ***the patient:***
  - autonomy;
  - the fundamental principle of informed consent;
  - data confidentiality;
  - the right to refuse treatment;
  - the right to medical information;
  - confidentiality.
- ***the professionals:***
  - defense of the dignity of the profession;
  - recognition of the responsibility and trust conferred by society;
  - collaboration in the interest of the patient with all actors involved;
  - providing services at the highest quality standards possible, based on a high level of skills, practical skills and professional performance without any discrimination;
  - avoiding all that is incompatible with individual and professional dignity and morality;
  - respecting the patient's dignity;
  - respecting the confidentiality of information and private life;
  - respecting the right to medical treatment and care;
  - the obligations to the patient;
  - protection of patients' rights;
  - compliance with professional obligations.

Another question is whether the employees of the health sector are prepared to fulfill their ethical obligation and how can their ethical skills be improved? This is where ethical education comes in.

Learning and developing ethical skills is important in healthcare professionals, starting from student years. In medical practice, ethical issues appear as ethical challenges, conflicts or dilemmas that influence the medical act (Zafar, 2015) [5]. Recognizing and solving ethical problems is about protocols, about doing what is right and in the patient's interest, about decisions, about actions and last but not least about behavior.

In the researched studies, ethics education refers to the educational elements that include learning activities that promote the recognition, understanding, and resolution of ethical issues, emphasis on ethics training found in both universities and medical institutions. Ethical issues and value conflicts are inherent in medical practice, but this does not necessarily mean that medical staff or students have done something inappropriate or that the

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

structures are inadequate. Regardless of the cause, ethical issues can lead to conflicts between principles, values, and behaviors (Beauchamp and Childress, 2019), which involve discrediting moral integrity and can generate moral distress (Torabi *et al.*, 2018) [6]-[7].

Solving ethical issues involves several factors. First of all, the legal one along with the correct identification of medical problems, treatment options and the clear objectives of care by professionals. They must consider the patient's preferences regarding treatment options and care goals, which are influenced by family, religious, cultural or even economic factors.

The quality of care and treatment depends not only on knowledge and skills or adherence to protocols; they depend on personal moral values, beliefs and ethical knowledge (Trobec and Starcic, 2015) [8]. Ethics education is one such way to develop ethical competences (Poikkeus et al., 2014) [9]. Ethics training often raises questions about the content and, especially, the methods relevant to medical practice. Numminen proposes as an alternative to theoretical courses and seminars in ethics, a teaching/learning process based on simulation. (Numminen et al., 2011) [10].

The teaching/learning process involves challenges for evaluating ethics education. Theoretical education in ethics is not exactly a realistic context or situation, and theoretical knowledge of ethics does not necessarily lead to good application of ethics (Godbold and Lees, 2013) [11].

In current university programs we find ethical principles presented and the recommendation to know ethical codes. These must be combined to avoid the risk of health professionals and students adapting to ethical practice without passing through the filter of their own beliefs. Thus, ethical competence risks being hindered by a limited attitude and a sharp moral reasoning on the situation as a whole (Mpeli, 2018) [12]. Learning ethical skills can help professionals and students orient their attention to ethical issues of which they were previously unaware, sometimes involving unfamiliar attitudes, approaches or emotions or different reactions to everyday ethical issues in healthcare. This study of ethical skills focuses on difficult and realistic situations such as: conflicts regarding informed consent or tensions between the patient's wishes and needs. All of these are related to professional norms, when honesty and respect for the patient are not present, or when there is a lack of trust in care services (Sherer et al., 2017) [13].

Employees and students are constantly faced with ethical issues regarding patients, physicians, colleagues, and the organization of the workplace.

Dealing with such problems means first and foremost thinking about what is right and good to decide what to do in a given situation, doing what is right in the patient's interest which may lead to conflict with the interest of others patients and may not be ethically or legally permissible, thus jeopardizing the approach and resolution of the problem. Doing the right thing based on the patient's best interest can sometimes jeopardize the management of ethical issues, as they may conflict with the interests of other patients, or may not be ethically or legally correct.

If there is a conflict between what is perceived to be best for the patient and their right to autonomy, ethical dilemmas can arise that present two orientations: legal and ethical (Schonfeld et al., 2015) [14]. Most of the time, there is at least one way to solve a situation, which makes handling the ethical issues that arise create a feeling of inadequacy or discomfort in making perfect decisions (Lin et al., 2013) [15]. Therefore, ethics training should be designed to include both medical and ethical reasoning in all situations (Torabizadeh, Homayuni and Moattari, 2016) [16].

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

The reviewed articles identified the need for support to enable the learning of ethical skills, which in the long term was considered to promote the ability to manage ethical issues. Learning ethical skills has been shown to be useful to health professionals and students in drawing attention to ethical issues of which they were previously unaware. When professionals deal with ethical issues, they think first of all about the protocol that aims at what is right and in the patient's interest, along with making decisions about what to do in a given situation. To support learning, education is also meant to provide the opportunity to receive the necessary instruction and create added value from the information received, to shape one's moral values and social attitudes, and to assume the consequences of one's actions. Collaboration with professionals is important because it can be a valuable source of knowledge, especially for students, in having the conviction that something is right. At the same time, ethics education is influenced by experienced professionals but also by students' personal expectations and strategies. (Andersson et al., 2022) [17].

Cited studies indicate that those with less experience in the hospital are more sensitive to ethical issues than their colleagues with more experience, possibly counteracting potential inexperience (Ulrich *et al.*, 2010) [18].

Medical ethics remains the compass that guides professionals in these complex situations. (Collier et *al.*, 2012) [19].

From the participants' point of view, a major challenge in medical ethics is the gap between theory and practice regarding ethical issues (BMA, 2012) [20]. Professionals, although they have knowledge of ethics, do not present ethical practice, do not have the right attitude towards human dignity, do not involve patients in their related decisions and do not respect patients' autonomy.

The regress of moral practices is an important factor, empathy being an element that seems to disappear with the advancement in the career. Medical students have high moral aspirations upon entering medical school, dreaming of being successful doctors with ethical and moral principles until they are old. But as time goes by, they notice inappropriate things, receive rather negative feedback and change their ways and mindsets to think only of their own benefit.

Another issue nowadays regarding medical ethics could be some structural flaws that automatically lead to ethical challenges in the practice of professionals, for example, financial problems of doctors, lack of new technologies, lack of access to innovative technologies (Mashayekhi *et al.*, 2021) [21].

Many of the actors involved in public health services believe that medical ethics has not been "widespread" enough in the health system, it has not yet been fully introduced in the community, and it seems that it has not been sufficiently publicized.

Medical ethics issues are similar to computerization issues, for example, so digitalization and ethical aspects should be understood the same.

Information about the patient's medical condition is considered private. Violating a patient's privacy can harm the patient and have legal and ethical consequences for healthcare workers. Laws also determine who can see the information and who cannot, especially through the use of new technologies, the entry of digitization even in this public sector.

There are also the ethical issues related to the use of artificial intelligence in promoting medical services. They appeal to data confidentiality, patient surveillance, subjectivity and sometimes discrimination in the medical act. Wherever there is technology, there is always the risk of inaccuracy and data breaches, and healthcare errors can have devastating consequences for patients. This is an important topic to consider as

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chişinău, Moldova

there are no clearly defined regulations regarding the legal and ethical aspects of AI and its role in healthcare.

Artificial intelligence has the ability to transform healthcare systems by providing new and important insights from the vast amounts of digital data that can be accessed much faster and more efficiently than humans.

Medical Ethics and Artificial Intelligence

Advances in artificial intelligence (AI) in healthcare are advancing rapidly, and there is a growing debate about how to guide its development. Many AI technologies will eventually be owned and controlled by private companies. The nature of AI implementations means that these companies, clinics and public agencies can play a bigger role than usual in obtaining, using and protecting patient health information. This raises privacy issues related to implementation and data security.

Many technological breakthroughs in the field of AI are made in academic research projects, subject to ethical principles.

The European Commission has proposed legislation containing compliant rules on artificial intelligence, delineating a principle of organizational responsibility for privacy and data. This fact is similar to that found in the European General Data Protection Regulation (European Commission legislative acts, 2021) [22].

AI has several unique characteristics compared to traditional health technologies. In particular, they may be prone to certain types of errors and sometimes not easily supervised by human healthcare professionals, and thus ethical issues may arise in how health information is used and handled and with personal character, if there are no adequate protective measures. Google, Microsoft, IBM, Apple, and other companies are "in their own way preparing bids on the future of health and various aspects of the global healthcare industry" (Powles *et al.*, 2017) [24]. Information sharing agreements can be used to give medical facilities access to patient health information.

To make medical AI trustworthy at the ethical level, the orientation to the ethical value of promoting human health should be considered first and foremost as a top-level concept of utmost importance. Legally, current medical AI has no moral status and the human side remains the bearer of duty. At the regulatory level, it is proposed to strengthen the management of data quality and security, improve its transparency and regulate and review the entire process of AI for risk control. Also, the social impact that its development could have must also be targeted.

The use of artificial intelligence in medical care has brought technological advances, especially in diagnostics and traditional treatment, at the same time coming with challenges and risks, both ethical and security. These negative effects are also considered ethical issues and need to be addressed through identification, prediction and monitoring as they influence trust in medical AI (Zhang *et al.*, 2023) [25].

This is an exciting time for the development and implementation of AI in healthcare, and the patients whose data is being used by these AIs should benefit greatly, if not significantly, from the health improvements these technologies produce. However, implementing commercial AI in healthcare faces serious privacy challenges. Given that personal health information is some of the most private and legally protected, there is great concern about how AI will change its access, control and use by business entities over time (Murdoch, 2023) [26].

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

The main factors that affect the trust of medical AI include: safety, technical reliability, usability. Data security includes its retrieval, processing and storage, involving issues such as informed consent, data quality and confidentiality.

Technical reliability, through the involved technicians, should strengthen ethical self-discipline and imprint an orientation towards ethical value in the research and development process.

Safe use targets both patients, but especially professionals, in the way it respects fundamental human rights and conforms to universal human values. One of the key values is the knowledge of ethics and especially its application. Legally, current medical AI has no moral status and humans are still responsible.

METHODOLOGY

The analysis of the specialized literature provides valuable information about the issues of medical ethics, being essential to substantiate our research. A literature review is a comprehensive analysis of the available literature, in this case medical academic publications relevant to the topic and to the research question on ethical issues arising from the education for ethics to the use of artificial intelligence in the provision of medical services. All studies deal with different ethical issues related to data security, autonomy, and accountability.

The identified studies are from different areas of the world, namely Europe, the USA, Asia, and the Middle East, having as common points ethical issues and reflect the concern of the last years, starting from 2019 and until 2023, for this topic and the attempt to involve both professionals, patients as well as those responsible for the implementation and construction of AI.

Empirical studies on ethical issues

For sustaining the theoretical approach, the following studies were analyzed for exploring the main ethical issues concerning the use of AI in healthcare systems.

a. Tenzin Wangmo, Mirjam Lipps, Reto W. Kressig and Marcello Ienca in the study "Ethical concerns with the use of intelligent assistive technology: findings from a qualitative study with professional stakeholders" from 2019, assessed the ethical issues that the professional stakeholders in Switzerland, Germany and Italy perceive them in the development and use of AI in the care of the elderly with dementia.

As a method, they conducted a multi-site study involving semi-structured qualitative interviews with health researchers and employees. They used descriptive thematic analysis to explore relevant ethical challenges inductively. Interviews of 20 researchers and health care professionals on ethical concerns related to the use of intelligent assistive technology highlighted ethical issues related to autonomy, accessibility, human interaction, and privacy.

By exploring the views and needs of both patients and stakeholders, we can ensure that technology and healthcare development is seen as a useful way of prospectively assessing practical, technical, clinical and ethical challenges. They emphasized the importance of ensuring the focus of specialists when designing AI, end user acceptance. Stakeholders recognize the AI technologies available and their applicability, but cite existing obstacles that prevent widespread adoption by end users. Impediments to implementation include the relatively high cost and lack of knowledge about using these technologies to improve health outcomes. Participants discussed informed consent and deception, all through the filter of the principle of autonomy.

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

Accessibility is discussed as an equal access concern, with data access and data sharing discussed in terms of privacy and autonomy principles. Most of the participants discussed the issue of data management, collection and storage, regarding ensuring protection when using AI, proposing the transmission of this information to third party services. Thus, two aspects were significant within this theme: access to data and data sharing that call into question the privacy and autonomy rights of people with dementia.

A relevant ethical issue has been the idea that AI, at least in its current state of technological innovation and readiness for the medical market, should complement human care, not replace it. Since it is about deeply human things, based on emotions that technology cannot replace, direct doctor-patient contact and empathy being important features in effective and morally accepted medical care, technology must come to their aid.

AI must be integrated, not replace the human part. There is the ability to make everyday life easier, but if it ends up replacing human care altogether, then there is a loss of human closeness, a loss of empathy, and a loss of emotional exchange.

Some interviewees even emphasized the financial side, regarding the current costs.

In conclusion, a partial mistrust of currently available AI technological capabilities and whether they can achieve human-comparable levels of efficacy, adaptability and flexibility in the short and medium term has been highlighted by identifying doubts in technology development and clinical implementation.

Some respondents supported the normative ethical position that care provided by humans cannot and should not be replaced by AI, making the association with medical deontology, particularly the moral obligations of the principles of beneficence and non-maleficence and the importance of maintaining the doctor-patient relationship.

b. Charlotte Blease, PhD, and other colleagues from General Medicine and Primary Care, Beth Israel Deaconess Medical Center, Harvard Medical School, in the 2018 exploratory qualitative study" Artificial Intelligence and the Future of Primary Care: Exploratory Qualitative Study of UK General Practitioners' (GP) Views' following a survey of 720 general practitioners had the ethical issue of AI responsibility and safety in the future of primary care.

Although AI technology can provide more accurate diagnoses and prognoses than humans in some cases, medicine still relies on the physician's clinical judgment in decision-making, as well as their experience in explaining medical information to patients and providing care. It has been argued that the use of technology threatens the quality of patient-centred care, with those involved in the study arguing for the continued need for face-to-face, professional-patient interaction. Scepticism prevailed among those surveyed, with most GPs believing that the scope of the innovation in general practice would be significantly limited.

In particular, some respondents argued that empathy and communication are considered essential human skills and that patients always want health care.

Other participants believed that an effective medical information gathering process requires doctor-patient interaction. Similarly, clinical acumen is often assumed to be a uniquely human skill.

This exploratory study suggests that UK GPs and computer scientists have very different views on the impact of machine learning in primary care.

In contrast to primary care physicians, AI health researchers predict that wearable devices with real-time monitoring capabilities will improve the accuracy of information gathering and reduce unnecessary appointments and medical costs.

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

GPs expressed three types of comments about future technologies: limitations of future technologies such as lack of empathy and communication, lack of direct patient-centred clinical decision making, increased efficiency benefits, and social benefits and ethical concerns.

Social and ethical concerns include some dissenting ideas, mostly related to uncertainties regarding patient acceptance of such technologies, safety and liability, lack of a larger number of physicians trained in new technologies.

The findings raise important questions about the ability of medical programs to prepare future physicians for potential changes in clinical practice, thus driving and shaping important discussions about the future of patient care. Improving education could help bridge the gap between current health AI researchers and practitioners.

c. Omar Mushabi, in the study published in 2021, in the United Kingdom, "Public patient views of artificial intelligence in healthcare: A nominal group technique study", using the nominal group technique (four groups with seven participants each), validated focused group interview which promotes the generation of AI ethics ideas and issues related to security, bias, data quality, human interaction and accountability.

All participants saw the use of AI in the healthcare sector as a benefit: faster service, 24/7 availability, reduced workload, equality in healthcare decision-making. However, participants also identified issues regarding data security, AI data quality, lack of human interaction, algorithm errors and accountability, technology errors. All of these points fall under three common themes: healthcare data automation, data security, and AI as a decision aid.

AI is a major step in recognizing the importance of ethics, emphasizing human rights. In addition to digital skills training, it is important to design AI systems to reflect the diversity of socioeconomic and health circumstances.

Other important ideas are protecting human autonomy, protecting privacy, inclusion, ensuring security and accuracy, and promoting responsive and sustainable AI. The findings of the study promote the need to further explore the human-computer interface and how human variation and psychosocial need can be accommodated in AI algorithms.

d. Department of Health Research Methods, Evidence, and Impact, McMaster University, Hamilton, Ontario, Canada by researchers Jason D. Morgenstern, Laura C. Rosella, Mark J. Daley, Vivek Goel, Holger J. Schünemann and Thomas Piggott have published in 2021 the fundamental qualitative descriptive study of the implications of artificial intelligence for public health "AI's gone have an impact on everything in society, so it has to have an impact on public health" dealing with ethical issues such as bias, fairness and equity. They used semi-structured interviews of 15 public health and AI experts as their method.

In the medical field, it has been reported that the application of AI is equal to or even better than that of doctors in various fields such as radiology, dermatology and pathology. Although AI has received much attention in the medical field, its impact on public health has received less attention. Still, researchers and public health experts are beginning to use AI for a variety of projects, including new Internet searches, suicide prediction using electronic medical records, and risk factor identification.

Participants will explore the potential of AI-based applications to integrate different types of unstructured data in disease surveillance, to integrate more continuously and in a timely manner, and to make better use of large, connected databases.

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

As AI has the potential to enable completely new approaches to public health, continued creative thinking could help maximize its benefits. In particular, the combination of artificial intelligence and big data will enable new and precise characterizations of decision-makers and their impact on health.

Opportunities for improving public health interventions were also highlighted, including new forms of automated disease screening, personalized health promotion, and the use of social media for health promotion.

As suggested by the participants, investments in artificial intelligence should ideally focus on areas that could reduce inequalities, such as improving access to public health services and health information.

Therefore, there is growing optimism about AI's potential to improve public health. However, very few AI systems are actually deployed in public health agencies. Going forward, there are serious concerns about the impact of AI on privacy, interpretability and the potential for bias.

Barriers to adoption, such as confusion about the applicability of AI, limited capacity and poor data quality, and risks, such as potential subjectivity/injustice/inequity and weak regulation.

e. The study conducted in China by Jie Zhang and Zong-ming Zhang and published in BMC Medical Informatics and Decision Making this year takes a multidisciplinary approach to ethical issues related to data quality, algorithmic errors, safety and security of AI, and attribution responsibilities, the ethical framework of ethical values-ethical principles-ethical norms being used to propose appropriate ethical governance countermeasures for an ethically and legally trustworthy medical AI.

From the title "Ethics and governance of trustworthy medical artificial intelligence" we understand the topic addressed, namely the assessment and analysis of existing and potential AI risks.

Data quality has a direct impact on the quality of medical AI. Medical data mainly comes from heterogeneous data from multiple sources, such as literature data, clinical trial data, real-world data, and health data collected by numerous with the help of smart technologies.

AI systems work only by inputting data, and the responsibility remains with humans. The safety aspects of medical AI present risks and harms that occur during its implementation. Covering a variety of legal and ethical issues, including bugs, cyber security breaches, the need for proper testing and software certification becomes difficult.

While no technology is 100% fool proof, the goal of medical AI should be dedicated to protecting and promoting human health. Limited digital power in healthcare facilities also makes it difficult to ensure data security.

The relevant legal system has not yet been improved, leading to a lack of effective regulations and restrictions on the collection, use and protection of privacy through the protection and streamlining of medical data. Therefore, sharing medical data and protecting patient privacy is also an ethical issue in medical AI applications, as medical data is sensitive information about individuals and has privacy implications. Respect for privacy is an important ethical principle in health care, as privacy is linked to personal identity and autonomy.

It is therefore essential that appropriate steps are taken to obtain patient consent for the use of personal health information. Ethical values lead to ethical principles, and ethical principles result in ethical codes. By combining the influencing factors, the authors

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

propose appropriate governance measures for reliable medical AI from ethical, legal, and regulatory aspects.

It was found that there are no quality standards, access systems, assessment systems or assurance systems for the application of AI in the medical field, and that the related guidelines and regulatory systems are not yet well established.

Only with the participation of all relevant sectors of society and many parties can we develop ethical and acceptable medical AI.

In order to develop an ethical, acceptable and accessible medical AI, the participation of all the relevant sectors of society is needed. Common to these studies is the fact that all researchers have found the need for informed consent when using data even as a database for AI. The legal system and regulations regarding AI security are necessary, and quite under-addressed, regardless of country. The existence of algorithm errors directly lead to ethical issues such as accessibility, safety and security. Also, a common conclusion is that the responsibility still remains with the human part, not the technology.

What made the difference was the degree of trust in AI, which was better seen and accepted in the US by both professionals and patients. Whether or not AI is useful in care is still being questioned in Europe, but it is recognized as leading the way in investigations and diagnostics.

DISCUSSIONS

The analysis reveals ethical issues generated by the use of artificial intelligence in the provision of medical services. Even if it is about different cultures, different medical systems from the point of view of AI, the studies of recent years highlight the fear that AI could replace the human part of medicine, the suspicion regarding the privacy and security of data.

Just as in China new policies and regulatory systems have been proposed regarding AI, in which all interested sectors participated, so it is recommended that all medical systems implement and update the social and legislative part, so that the beneficiaries have confidence in new technology.

Some doctors have a superficial and unscientific view of the field of medical ethics and mistakenly believe that they have sufficient knowledge and good awareness of medical ethics. One of the biggest challenges in ethics is the lack of adequate education in medical ethics. The existence of negative models represents a potentially significant obstacle to the emergence of a professional and ethical behavior among young professionals, which is mostly due to the gap between theory and practice in terms of ethical aspects, even when it comes to new technologies with which they are more accommodating than experienced professionals.

Responsibility rests entirely with the human side, although sometimes errors may come from algorithms or the lack of quality standards, access systems, evaluation systems, and assurance systems for the application of AI in the medical field.

In a technological and computerized world, doctors face challenges related to data privacy and decision-making supported by artificial intelligence, modern medicine poses new ethical dilemmas.

Across healthcare organizations, there is a growing trend towards the development and use of smart technology. This fact leads to the improvement and efficiency of the services provided to patients, and even to the reduction of costs. As digitization develops, gaining more and more ground even in health services, the risk of cyber-attacks can also increase proportionately, leading to the loss of sensitive patient data, blocking some medical services and even endangering patient safety (EHB, 2022) [27].

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

From the point of view of ethical and information management, cyber security measures are required in the health system, implemented according to security objectives specific to the health sector, starting with the protection of the confidentiality of medical data, ensuring the integrity of the data, compliance with legal regulations, securing the services of telemedicine and remote monitoring of patients, which following the pandemic have developed significantly. Establishing incident management practices and increasing staff awareness and training, healthcare data integrity systems are in the midst of an ongoing, high-impact digital transformation to interventional practice and, by implication, to patients.

Technological innovations in surgery such as advanced imaging, minimally invasive techniques and automation have brought many benefits, affecting the accuracy of patient operations, reducing intervention time and increasing, most of the time, the efficiency of medical services.

Regarding the state of security in the public health system, both deficiencies and risks can be found, generated by the technological factor (the complexity of the IT infrastructure, outdated equipment) and the human factor (lack of specialists, lack of specialized departments and deficiencies in backup, insufficient training), lack of IT and non-IT personnel training, non-compliance with standards and recommendations regarding ethics and security (Mertoiu, 2020) [21].

This fact would require a continuous training of the employees of the public medical sector, as a result of the introduction of new intelligent technologies in the application of the medical act, both for the provision of medical services from the intervention side, and from the prevention or education side.

The introduction and use of everything that is innovative and equipped with an intelligent component, is seen by some of the actors of the medical services as a vulnerability to the confidentiality and integrity of the medical act, but the trust in the new intelligent technologies is also evident at the institutional level of public health, who managed to overcome some obstacles caused by lack of financial resources or lack of confidence.

Ethical issues and risks associated with technology addiction are ever-present and require additional measures to reduce their impact.

In modern medicine, these can be found in areas such as telemedicine, artificial intelligence, forced testing, involuntary hospitalization, vaccination, end-of-life care, priority testing, biotechnology, medical education and e-health.

The increasing use of medical technologies in all areas of healthcare raises ethical challenges. Similar to the relationship between doctors and medical companies, the relationship between doctors, hospitals and companies that produce medical technologies is necessary, but also involves ethical issues. They appear in educational institutions, where doctors only theoretically learn how to use new equipment from representatives of manufacturing companies, in personal research projects, where doctors collaborate with corporations. Many medical devices are designed to prolong life when drug treatments have failed, so they are often used for patients in very critical situations (BMJ, 2006) [28].

Meanwhile, advances in diagnostic technology allow doctors to detect diseases earlier and more accurately and, in some cases, prevent complex diseases from developing. These technologies promise a new age of preventive medicine. It is important to temper public and physician enthusiasm for the potential of such technology with accurate patient information and appropriate use by physicians (Gelijns *et al.*, 1998) [29].

Recent innovations in medicine and biotechnology can lead to great speculation about what advances will come next. While it is probably true that all doctors, scientists

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

and bioengineers design and implement medical devices with only good intentions, the pace of development and integration of medical devices into medical practice and other medical fields is slowing. The speed of development makes it impossible to predict all possible outcomes (Gelijns, 1998) [29].

The pace of development and integration of medical devices in practice is slowed by distrust, even if researchers, doctors, bioengineers design quite quickly, which sometimes makes it impossible to predict the results, the implementation of medical technologies being only with good intentions.

For example, a stethoscope symbolizes the connection between the patient and the doctor, but the use of new equipment is seen as weakening the close bond between the two. The use of electronic health records can be involved in scientific studies, improving the quality of medical services and optimizing patient care. This comes with the risk of data being "hacked" and shared for the wrong purposes. In response to the question of when and if consent, even formal consent, is necessary, other ethical considerations arise including ownership of a person's medical records and patient history, with whom it will be shared and who has access to it.

CONCLUSIONS

The purpose of our research study was to identify the medical ethics aspects involved in the use of artificial intelligence in the provision of medical services and the necessity of ethical education. The investigation covered several elements of medical ethics based on ethical principles, ethics education, the existence of ethical issues, and the benefits and drawbacks of new technologies.

Morality and compassion, as a preamble to care, are expressed by doing good. Discernment is especially valuable in decision making, especially when ethical principles collide, and ethical issues arise. Trust begets trust and is a necessary virtue when patients, at their most vulnerable, place themselves in the hands of doctors. Integrity involves the coherent integration of emotions, knowledge, and aspirations, while preserving moral values. Professionals need both professional and personal integrity.

Improving the quality of healthcare services in response to the increasing health needs of patients depends on how careful medical professionals are about ethical principles and openness to new technologies.

Updating regulations and introducing new policies in the medical sector to address the safe implementation and use of AI is a way forward to increase the trust of beneficiaries and professionals, to improve cybersecurity and quality standards, assessment systems and safety systems for the application of AI in the medical field.

Ethics education is essential to support the learning and development of ethical competences in professionals and students training to become professionals.

We believe that medical ethics has not yet been sufficiently disseminated in the health system and it seems that it is not yet sufficiently implemented or well presented in society, even if more emphasis is placed on the existence of ethical codes, on knowledge and education.

There are also ethical issues surrounding the acceptance and use of artificial intelligence in promoting health services. They claim data confidentiality, a better understanding of the patient's condition, but subjectivity or discrimination in medical practice can also occur. Wherever technology exists, there is always the risk of inaccuracy and data breaches, and errors in healthcare can have devastating consequences for patients. This is an

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chişinău, Moldova

important issue that needs research because there are no clearly defined regulations regarding the legal and ethical aspects of artificial intelligence and its role in healthcare.

Medical artificial intelligence has no moral status, so the responsibility rests entirely with professionals and patients.

Solutions to security and the acceptance of AI for good could come from collaboration between relevant sectors of society and a concern for continuing education on ethics.

BIBLIOGRAPHY

1. BRESLIN J.M., MACRAE S.K., BELL J., SINGER P.A. *Top 10 health care ethics challenges facing the public: Views of Toronto bioethicists,* University of Toronto Joint Centre for Bioethics Clinical Ethics Group.. BMC Med Ethics 2005;6:E5
2. ÇINAR F., EREN E. *Innovative approach to the ethics in health care organizations: Health staff perspective*. Procedia Soc Behav Sci 2013;99:719-25
3. VARKEY B. *General Medicine, Principles of Clinical Ethics and Their Application to Practice,* Med Princ Pract. 2021. 30 (1): 17–28.https://doi.org/10.1159/000509119
4. ASTĂRĂSTOAE V, *Dileme etice în medicină*, Art-emis, 2021, <https://uzpr.ro/04/03/2021/dileme-etice-in-medicina/>
5. ZAFAR W. *Moral experience and ethical challenges in an emergency department in Pakistan: emergency physicians' perspectives*. Emerg Med J. 2015;32:263–8
6. BEAUCHAMP T, CHILDRESS J. *Principles of biomedical ethics*. 8th ed. New York: Oxford University Press; 2019.
7. TORABI M., BORHANI F., ABBASZADEH A., ATASHZADEH-SHOORIDEH F. *Experiences of pre-hospital emergency medical personnel in ethical decision-making: a qualitative study*. BMC Med Ethics. 2018;19:95. https://doi.org/10.1186/ s12910-018-0334-x.
8. TROBEC I., STARCIC A. *Developing nursing ethical competences online versus in traditional classroom.* Nurs Ethics. 2015;22(3):352–66.
9. POIKKEUS T., NUMMINEN O., SUHONEN R., LEINO-KILPI H. *A mixed-method systematic review: support for ethical competence of nurses.* J Adv Nurs.2014;70(2):256–71.
10. NUMMINEN O., LEINO-KILPI H., VAN DER AREND A., KATAJISTO J. *Comparison of nurse educators' and nursing students' descriptions of teaching codes of ethics*. Nurs Ethics. 2011;18(5):710–24.
11. GODBOLD R., LEES A. *Ethics educations for health professionals: a values based approach*. Nurse Edu Pract. 2013;13:553–60.
12. MPELI M. *Analysis of self-evaluated ethical competence of midwifery students at a selected nursing college in the* Free State. Curationis.2018;41(1):e1–9. https://doi.org/10.4102/ curationis.v41i1.1925.
13. SHERER R., DONG H., CONG Y., WAN J., CHEN H., WANG Y., ET AL. *Medical ethics education in China: lessons from three schools.* Edu Health.2017;30:35–43.
14. SCHONFELD T., JOHNSON K., SEVILLE E., SURATT C., GOEDKEN J. *Differences between two methods of ethics education: focus group results*. Ethics Soc Welf. 2015;9(3):240–54.

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

15. LIN Y-C., CHAN T-F., LAI C-S., CHIN C-C, CHOU F-H, LIN H-J. *The impact of an interprofessional problem-based learning curriculum of clinical ethics on medical and nursing students' attitudes and ability of interprofessional collaboration: a pilot study*. Kaohsiung J Med Sci. 2013;29:505–11.
16. TORABIZADEH C., HOMAYUNI L., MOATTARI M. *Impacts of Socratic questioning on moral reasoning of nursing students.* Nurs Ethics. 2016;25(2):174–85.
17. ANDERSSON H, SVENSSON A, FRANK C, RANTALA A, HOLMBERG M. AND BREMER A. *Ethics education to support ethical competence learning in healthcare: an integrative systematic review*, BMC Medical Ethics, 2022; 23:29 https://doi.org/10.1186/s12910-022-00766-z.
18. ULRICH C.M., TAYLOR C., SOEKEN K., O'DONNELL P., FARRAR A., DANIS M., ET A.L.*Everyday ethics: ethical issues and stress in nursing practice.* J Adv Nurs.2010;66(11):2510–9.
19. COLLIER R., *Professionalism: The importance of trust*, CMAJ. 2012 Sep 18; 184(13): 1455–1456, PMCID: PMC3447012, PMID: 22927515, doi: 10.1503/cmaj.109-4264.
20. British Medical Association. *Medical ethics today: the BMA's handbook of ethics and law*. John Wiley & Sons. 2012.
21. MERTOIU G.B., MEȘNIȚĂ G., *Machine Learning pentru securitatea cibernetică în sistemul de sănătate publică*, 2020.
22. European Data Protection Supervisor. Accountability. [online]. [viewed 19 December 2023]. Available from: < https://edps. europa.eu/data-protection/our-work/subjects/accountability_en>
23. European Commission. *Proposal for a regulation of the European parliament and of the council laying down harmonised rules on artificial intelligence (artifcial intelligence act) and amending certain union legislative acts.* 2021. [online]. [viewed 21 December 2023]. Available from: < https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206>
24. POWLES J, HODSON H. *Google DeepMind and healthcare in an age of algorithms*. Health Technol. 2017;7(4):351–67.
25. ZHANG J, ZHANG Z-M. *Ethics and governance of trustworthy medical artificial intelligence*. BMC Med Inform Decis Mak. 2023 Jan 13;23(1):7. doi: 10.1186/s12911-023-02103-9. PMID: 36639799; PMCID: PMC9840286.
26. MURDOCH B., *Privacy and artifcial intelligence: challenges for protecting health information in a new era* BMC Med Ethics, 2021.
27. Healthcare under siege: the need to improve cybersecurity in the near future, IEEE International Conference on e-Health and Bioengineering, EHB 2022 - 10-th Edition, Faculty of Medical Bioengineering, U.M.F. "Grigore T. Popa" Iasi, Romania, November 17-18, 2022.
28. Startling technologies promise to transform medicine BMJ 2006; 333 doi: https://doi.org/10.1136/bmj.39049.453877.BE (Published 21 December 2006) Cite this as: BMJ 2006;333:1308 Accessed 5 Dec 2023.
29. GELIJNS A.C., ROSENBERG N., MOSKOWITZ A.J. *Capturing the unexpected benefits of medical research.*. N Engl J Med. 1998;339(10):693-698.

DOI: https://doi.org/10.53486/escst2023.26
International Conference, December 07-08, 2023, Chișinău, Moldova

30. MASHAYEKHI J., MAFINEJAD M.K., CHANGIZ T., MOOSAPOUR H., SALARI P., NEDJAT S., LARIJANI B., *Exploring medical ethics' implementation challenges: A qualitative study*, J Educ Health Promot. 2021; 10: 66.doi: 10.4103/jehp.jehp_766_20
31. WELCH G.H, SCHWARTZ L. AND WOLOSHIN S., *What's Making Us Sick Is an Epidemic of Diagnoses* ByJanuary 2, 2007.
32. *Codul de etică și deontologie profesională*, [online]. [viewed 21 December 2023]. Available from: < https://www.recuperarecluj.ro/documente/etica.pdf>
33. *Codul de conduită etică și profesională al personalului contractual din Spitalul Clinic Județean de Urgență "Sf.Spiridon" Iași*. [online]. [viewed 21 December 2023]. Available from: < https://www.spitalspiridon.ro/docs/ Cod_conduita_etica_pers_Sp_Sf_Spiridon_Iasi.pdf >
34. *Cod de etică și deontologie profesională a Spitalului Clinic Municipal de Urgență Timișoara*, [online]. [viewed 5 December 2023]. Available from: <https://www.spitalul-municipal-timisoara.ro/public/data_files/media/etica/ 2023/202306281127-condul-de-etica-28-06-2023.pdf>
35. Code of Medical Ethics [online]. American Medical Association, [viewed 12 December 2023]. Available from: <https://code-medical-ethics.ama-assn.org>

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.27
International Conference, December 07-08, 2023, Chişinău, Moldova

FROM THE EXPERIENCE OF USING WEBQUESTS IN TEACHING INFORMATION SECURITY

Violeta BOGDANOVA

PhD, University lecturer,
"Ion Creangă" State Pedagogical University, Moldova,
ORCID 0000-0003-4140-6317
E-mail: bogdanovaleta@gmail.com

Liubomir CHIRIAC

Habilitated Doctor, Professor,
"Ion Creangă" State Pedagogical University, Moldova,
ORCID 0000-0002-5786-5828
E-mail:llchiriac@gmail.md

Abstract: *The article describes modern educational technology webquest, its features, stages of implementation. The methodology for implementing a web quest in the discipline "Information Security" for students of economic specialties is described in detail. Areas of research, such as information security at home, office or state, are identified. The roles of a lawyer, psychologist, analyst, practitioner, administrator, errorist are indicated. Specific results that should be obtained by each role are formulated. Instructions for teachers and students on organizing a webquest are presented. Thus, the technology of organizing project activities when studying the basics of information security by future economists is shown in detail. The capabilities of the website builder GoogleSites are described.*

Keywords: *webquest, information security, Information Security for Economists, teaching methodology, independent work, educational activities, website builder.*

UDC: *004.056.5:[378.147:33]*

JEL Classification: *JEL: I23.*

INTRODUCTION

Studying the basics of information security is necessary at all levels of education in all specialties, since information threats are increasingly appearing at the level of the state, organization and in a person's personal life.

Training economists in information security is associated with certain difficulties: an insufficient number of hours to study this area, different levels of ICT competencies among school graduates.

As part of the study of the discipline "Information Security", future economists need to consider various aspects of information security: legal, organizational, software, moral and ethical, software, technical and physical.

Along with traditional didactic methods and techniques, it is important to use new methods. One of these didactic methods is a web quest technology, proposed by Bernie Dodge, professor of educational technology at San Diego State University (USA), in 1997. Within its framework, the teacher can shape the search and cognitive activity of students on the Internet, taking into account relevance, adequacy and safety [1].

METHODOLOGY FOR CONDUCTING THE WEB QUEST "INFORMATION SECURITY FOR ECONOMISTS"

Webquest is an information and communication pedagogical technology that refers to game-based teaching methods. Students choose pre-suggested roles and work in an

DOI: https://doi.org/10.53486/escst2023.27
International Conference, December 07-08, 2023, Chişinău, Moldova

individual direction. As a result, each student receives the entire amount of information, but along his own individual "path of knowledge." At each stage, the teacher sets specific tasks and determines deadlines for completion. Students move on to the next stage, having successfully completed the tasks of the previous one. Work within the webquest consists of obtaining information on the World Wide Web under the guidance of a teacher.

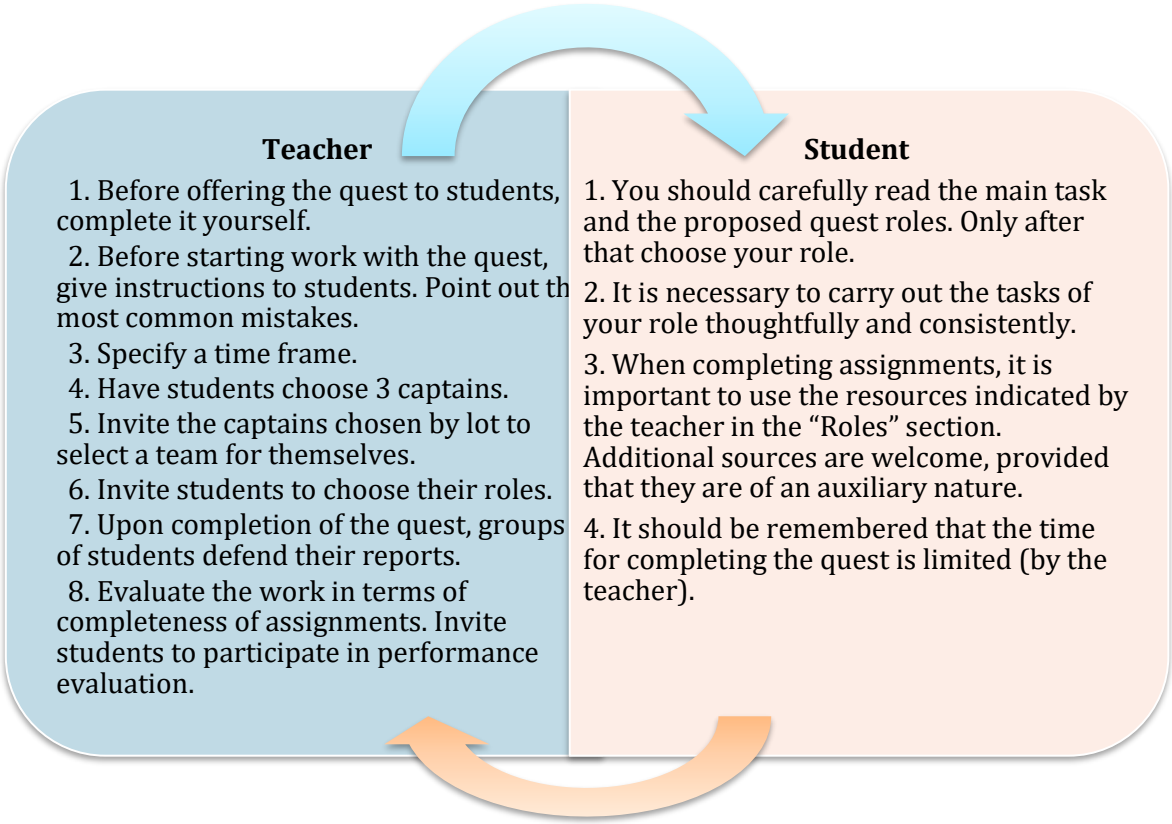


Figure 1. Instructions for organizing a webquest
Source: designed by the authors

The thematic web quest on the topic "Information Security for Economists" is intended for students studying in the bachelor's degree program in the discipline "Information Security." It is also advisable to use this quest in students' independent work when studying information cycle disciplines. In the state standard for training bachelors in the field of Economics, the graduate must have, among others, such general professional competence as "the ability to solve standard problems of professional activity on the basis of information and bibliographic culture with the use of information and communication technologies and taking into account the basic requirements of information security".

The use of webquest technology in teaching requires some information competencies on the part of the teacher. GoogleSites – free website builder and hosting. No knowledge of web programming is required to work with it. It can be used for collaborative editing. The developer is provided with many tools such as YouTube videos, calendars, maps, forms, links, images, documents, HTML, CSS, or JavaScript code.

The thematic quest on information security contains sections (tabs): main, roles, deadlines, test, is located at sites.google.com/view/bogdanova-zki/home.

DOI: https://doi.org/10.53486/escst2023.27
International Conference, December 07-08, 2023, Chişinău, Moldova

On the *Home* tab there is a video about one of the current threats to humanity - information security. There is also a link to guidelines developed by the author using the digital platform Joomag. These tasks help to develop practical information security skills.

To participate in the webquest, students need to be divided into three groups, each of which studies and prepares materials from the point of view of information security: information security at home, information security at office, information security at the levels of states.

The *Roles* tab contains a set of fixed tasks for the roles selected by students. To perform tasks efficiently, you need to follow the link of the corresponding role, where the teacher selected information resources taking into account relevance, adequacy and safety [2].

The quest provides such roles for students as lawyer, psychologist, practitioner, administrator, analyst and errorist. A lawyer studies in more depth the legislative aspects of working with information, determines what and how to protect from the point of view of legal norms. The psychologist examines in detail the moral and ethical standards for using information. The practitioner delves into software information security tools, the administrator into technical ones. The analyst studies organizational means of information security, in particular international and Russian standards in the field of information security. An error investigator searches for typical vulnerabilities in an information security system.

Each quest participant generates a report (in the form of a computer presentation, diagram, table, memo, etc.), on the basis of which the final report of the group is prepared (Table 1).

Table 1. Final results of the group

The ***lawyer*** prepares: - list of legislative and regulatory acts in the field of information security; - basic summary of the topic "Legislative means of information protection"; - a structural diagram of the system of concepts of information types of access.	The ***psychologist*** prepares: - a memo on ethical standards for the use of information technologies; - a reminder of protection from the influence of a social engineer. - comparative analysis of ethical standards of different countries.
The ***practitioner*** prepares: - a map of freely distributed software in the field of information security; - a selection of freely distributed antiviruses.	The ***Errorist*** prepares: - a bank of typical errors in the field of information security; - memo "This is not how you work with information"
The ***analyst*** prepares: - chronology of the creation of standards in the field of information security; - a list of the international standards in the field of information security, indicating the scope of their application.	The ***administrator*** prepares: - presentation "10 ways of technical interception of information"; - memo "10 golden rules of technical information security."

Source: designed by the authors

A list of materials that the participants prepare, depending on the role and taking into account the specialization of the team (information security at home, office or state).

As a result of completing the webquest, students should learn:

– regulatory and legal aspects of information security;

DOI: https://doi.org/10.53486/escst2023.27
International Conference, December 07-08, 2023, Chişinău, Moldova

– moral and ethical standards, aspects of information security;
– organizational means of information security;
– technical, software and physical means of information protection.

The *Deadlines* tab contains deadlines for completing the task. Upon completion of the quest, the groups defend their reports and the students, together with the teacher, mutually evaluate the work done.

The *Test tab* is intended for participants to take the test individually after completing the webquest. The password must be obtained from the teacher. This was done so that it was possible to analyze who solved the test and how many questions they answered correctly, which questions were answered by all participants, and which ones caused the greatest difficulties.

CONCLUSIONS

Information security is a fairly new discipline with a distinct interdisciplinary aspect. From the point of view of studying the theoretical aspects of cybersecurity, you can turn to legislation, international standards, and many bibliographic sources. Forming practical skills for future economists has certain difficulties: most workshops are focused on studying software and hardware security tools. It is important for future economists to develop skills in organizational, legal and ethical methods of protecting information. The webquest "Information Security for Economists", developed and presented in this article, is aimed at developing these skills.

BIBLIOGRAPHY

1. DODGE, B. WebQuests: A technique for internet-based learning. *Distance Educator*. 1995, nr. 1, pp. 10-13. ISSN-1084-6972
2. ДАРИЕНКО, М. С., БОГДАНОВА, В. А. Возможности интеграции Web-квест технологии на этапе обобщения и систематизации знаний обучающихся. В: *Сборник статей участников Международной научно-практической конференции "Общекультурные и естественнонаучные аспекты образования в интересах устойчивого развития".* Арзамас: Арзамасский филиал ННГУ, 2018, с. 34-138. ISBN 978-5-6040222-9-0

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chişinău, Moldova

ANALYSIS OF INTEREST GROUPS THAT MAY MATTER AT THE LEVEL OF THE REFORM PROCESS OF THE MOST RELEVANT INTERNATIONAL ORGANIZATIONS

Corneliu-George IACOB

PhD student,
University of Economic Studies, Bucharest, Romania,
ORCID 0009-0009-7466-4612
E-mail:iacobcorneliu2022@gmail.com

Dumitru MIRON

PhD Habilitat, Professor,
University of Economic Studies, Bucharest, Romania,
ORCID 0000-0003-0606-6329
E-mail:dumitru.miron@rei.ase.ro

Abstract: *The current international environment, viewed from a geopolitical and geoeconomic point of view, is characterized by unpredictability and heightened dynamism. After the Second World War, the theoretical and doctrinal landscape was marked by an increasing openness to the concepts of harmony, cooperation, structural peace, prohibition of war. The UN is a symbol of multilateralism and sustained worldwide efforts for peace, security and sustainable development. Strategic autonomy, national security and other non-economic objectives (environmental sustainability, protection of workers and human rights) motivate calls for collaboration between countries with similar political-economic values and systems. In today's conditions, security considerations have already become more prominent in trade relations. Since the end of the 90s, several scenarios have been proposed for the reform of the United Nations: the reform of the Security Council, the reform of the UN Secretariat, the financial reform, the reform of human rights, the reform of operational activities and, last but not least, the reform of the Economic Council and Social. The research methodology uses various research methods: the logical analysis method, the systemic method, the comparative method, the historical method, the situation analysis used in geopolitical theory and the stakeholder analysis to understand the positions and perspectives of the players (stakeholders) who have an interest and/or likely to be affected by a particular reform, as well as to outline the prospects for reform and how particular states/organizations might influence the outcome of the process.*

Keywords: *reform of international organizations, stakeholders analysis, geopolitics, geoeconomics*.

UDC: *339.73:341.1*

JEL Classification: *F13, F02.*

INTRODUCTION

After the Second World War, the theoretical and doctrinal landscape was marked by a growing openness to the concepts of harmony, cooperation, structural peace, the prohibition of war. In 1944, at the Monetary and Financial Conference of the United Nations at Bretton Woods, it was agreed to place the international geo-economic system on three pillars - the financial-monetary, the banking and the commercial. For this, the participating states agreed to create three modern institutional architectures: the International Monetary Fund (IMF), the International Bank for Reconstruction and Development (IBRD) and the International Trade Organization (OIC). The first two institutional structures became operational in a very short time, while the third encountered difficulties in its establishment, which led to a long temporary one in the form of the General Agreement on Tariffs and

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chișinău, Moldova

Trade (GATT) formalized only in 1995 when it was established World Trade Organization (WTO). Currently, at the level of the UN system, six main bodies are operational (the General Assembly, the Security Council, the Economic and Social Council, the Guardianship Council, the International Court of Justice and the Secretariat) which have an important role in maintaining international peace and security, but also for the orientation of the activity of modern societies towards a sustainable and balanced development.

The current international environment, characterized by unpredictability, viewed from a geopolitical and geoeconomic point of view, is much different from the existing international environment at the level of 1945. Against the background of large-scale transformations in the economic-financial mechanisms and in the relations of forces existing worldwide, the reform of international institutions is a necessary condition for them to be able to adapt to the new geopolitical and geoeconomic realities. The purpose of this research is to facilitate the understanding of the positions and perspectives of actors (stakeholders) who have an interest and/or are likely to be affected by a certain reform, as well as to highlight the reform perspectives and how certain states/organizations could influence the result of the process. The research methodology assumes a gradual approach, in two steps: first, the general context of the international environment in which the most important organizations appeared and operate is presented, also pointing out the need to reform these organizations, then the analysis of the interested parties is carried out. Various qualitative research methods are used: historical method, logical analysis method, systemic method, comparative method, situational analysis used in geopolitical theory and stakeholder analysis.

ANALYSIS OF INTEREST GROUPS THAT MAY MATTER AT THE LEVEL OF THE REFORM PROCESS OF THE MOST RELEVANT INTERNATIONAL ORGANIZATIONS

➢ CONSIDERATIONS REGARDING THE REFORM OF THE MAIN INSTITUTIONS OF THE UNITED NATIONS SYSTEM

The urgency of the need for UN reform

The UN system, as it is today, is much different than originally planned. Its role is quite mitigated compared to the provisions of some important documents from 1974; Despite the fact that emerging/developing economies have been the main "engines" of global growth in the last decade, their voting power in the IMF and the World Bank does not reflect their economic power. Since the late 1990s, several scenarios for reforming the United Nations have been proposed. However, there is little clarity or consensus about what reform might mean in practice. The current stage of the UN reform is a multi-level one: firstly, within the UN development system, the way of working at the global, regional and country level is addressed; this ranges from UN strategic planning approaches and tools to accountability systems, administrative arrangements and budgetary practices.

Reform of the United Nations Security Council

The Security Council (SC) represents the institutional component of the United Nations Organization which, according to the Charter of the United Nations, has the main responsibility for maintaining international peace and security. Currently, four groups of states have emerged in the reform process: the Group of 4 (G4), the Uniting for Consensus Group (UFC), the African Union and the ACT (a trans-regional group of 21 states promoting the need revising the working methods of the SC, in order to increase the responsibility of its members in front of the entire UN community and to increase the transparency of its activity). The main controversy concerns the total number of members that the reformed

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chișinău, Moldova

Council should have and their distribution by category (permanent and non-permanent members). At the UN level, there were debates on 5 major themes: categories of members, the right of veto, the magnitude of the expansion, working methods and the relationship with the General Assembly. In 2015, there was an intensification of the work of the Working Group for the reform of the SC, but a consensus solution was not reached.

IMF and World Bank reform

As early as 2004, within the Report prepared by a group of experts led by the American scholar Meltzer, the reform of international financial institutions was discussed, the major changes that took place or that should have taken place in order for these institutions to become more effective in achieving their goals. Much of what the IMF and World Bank charter states about goals and objectives is outdated. The IMF's current mandate should be to reduce global risk to the lowest possible level. The mandate of the World Bank should be to facilitate social and economic development as a means of reducing poverty.

WTO reform

The multilateral trade system, with the World Trade Organization (WTO) as its main institutional vector, is the most complex panel of economic management and development tools. The institutional progress recorded over 70 years is notable and takes shape in the creation of well-being in industrialized countries, the accommodation of the rural economies of developing countries with supercompetitive commercial giants and the laying of sustainable foundations for economic and technological progress in all regions of the world. A growing number of voices question many of the successes attributed to a national economy's participation in the multilateral trading system, arguing that it has become a victim of its early successes. Criticisms of the current state of affairs within the multilateral trade system are multiplying, emphasizing that it has not firmly switched to the new logic of global governance. Part of the criticism is a reflection of the perception that the WTO's institutional mechanisms are not adequate to face the new challenges fueled by a set of sources of economic, technological and even socio-cultural instability [1]. Against this background of profound and unpredictable change, the idea of reforming the regulatory framework and institutional architecture of the international trade system has slowed down. Many reform proposals have focused on the WTO's current decision-making mechanisms.

Five areas of WTO reform have been highlighted in recent multidisciplinary research on strengthening the WTO's effectiveness as a forum for trade cooperation: revising the organization's working practices; improving transparency: collecting and reporting information on relevant (challenged) policies and supplementing them with analysis of policy side effects; preparing the ground for the negotiation of new agreements through evidence-based deliberations and support for plurilateral initiatives where there is no consensus to proceed on a multilateral basis; reforming the WTO dispute settlement system; and, last but not least, addressing what is called the "China Inc" problem [2].

In general, the reform proposals focus on three aspects of the functioning of the WTO: rule-making; transparency and monitoring; and dispute resolution. Two major issues stand out: the status of developing countries, i.e. Special and Differential Treatment (SDT), and free market-distorting policies in terms of state involvement, mainly targeting China [3].

- **STAKEHOLDER ANALYSIS**

The analysis of Interest Groups focuses on 3 (three) basic elements:

a. The interest that the groups/actors have in achieving the objectives of the Process;

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chișinău, Moldova

b. Power of groups/actors (influence and importance) over the Process;
b. The amount and type of resources they can mobilize to influence the results of the Process and their ability to mobilize resources.

Interest groups can be structured into 3 important categories:

- Key interest groups - are those that can significantly influence a project or a program whose success directly depends on them (in accordance with the major objectives of the policy and the purpose of the respective program);
- Primary interest groups - which are formed by people, groups of people or institutions (depending on the level of analysis), which are affected, either positively (beneficiaries) or negatively, by a certain project or program that has an impact on them;
- Secondary interest groups – are various intermediary entities that carry out certain activities within the program or project that may or may not take part in the decision-making process and that may also be affected positively or negatively.

Identification of Interest Groups

The main Interest Groups identified can be structured as follows:

a. Key interest groups:
- The European Union (represented by its institutions);
- The Russian Federation;
- USA, China, Japan, India, Brazil, Turkey;
- International Organizations (eg: UN, WTO, World Bank, International Monetary Fund, etc.).

b. Primary interest groups:
- The countries of the Middle East;
- African countries.

c. Secondary interest groups:
- Pressure groups (lobby)/ economic agents (potential investors);
- Consumers and Labor Unions.

It must be taken into account that the political environment has a considerable influence on the reform of international institutions. Also, there are certain pressure groups (lobbies), which, in turn, exert pressure on public decision-makers, in order to obtain decisions in line with the interests they represent.

Analysis of Interest Groups

The interest in the process of reforming the most relevant international organizations depends on how the reform directions will be formulated and, at the same time, the implications of these changes on the targeted organizations, but also on each member state, will be highlighted.

According to [4] - [6], the main positions of some states regarding the reform of the United Nations system can be summarized as follows:

USA - contributes the most to the UN budget among the member states, their contribution amounting to 22% of the total UN budget. The United States Congress has shown a constant concern for reforms related to the effectiveness of the UN. The official position: "The administration is focused on UN management reform. As the largest financial contributor, we have the largest financial stake in sound management and operational efficiency ... and it is essential that we refocus the efforts of all UN member states on the need to reform this institution."[4]

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chișinău, Moldova

China - is among the most prominent proponents of multilateralism and actively participates in global governance reform and improvement. Chinese diplomacy appreciates the value of "the international system built around the United Nations (UN), the international order supported by international law, and the multilateral trade system centered on the World Trade Organization (WTO). There are a number of different points of view between China and Western countries regarding UN reform. Compared to Western countries, China takes a more cautious stance, stressing the need for proper consultation and coordination among all member states. According to official statements, China does not want to rush reform as long as there are still significant disagreements between developing and developed countries. China prefers a gradual and cautious reform of the UN system. China supports UN reform to achieve the goal of coherence and efficiency in the UN operational system. The difference is that Western donor countries emphasize "a single UN system" and China appreciates "flexible approaches" according to "diverse national needs and requirements", believing that the reform should lead to an increase in the ability of UN activities to meet the different requirements of beneficiary countries in an integrated and flexible way and that reform should not be strictly limited to certain areas.

European Union - The influence of the Union within the UN derives not only from its official status, but also from its ability to coordinate the positions of its member states, to take advantage of the diplomatic influence it exercises over third countries and to present different positions through representatives his. The status of the Union in the various entities of the United Nations system varies from membership (FAO, WTO) to being non-status (Security Council and some specialized institutions), through privileged observer status (General Assembly) or simple observer status (ECOSOC and many specialized institutions). The Union and its member states contribute about a third of the budget of the United Nations system, although they account for less than 15% of the membership of the United Nations. This contribution increases the visibility and influence of the Union in the organization. In the context of the UN reform debate, it has been proposed several times since the 1990s to grant the Union a seat on the Security Council. For now, this eventuality is unlikely. The European Union is a full member of the WTO and is, to date, the only international organization that enjoys such status. The European Union can also exert significant informal influence. For example, it has no formal status within the IMF but, under an unwritten rule, Europe nominates the person to head the IMF and the United States does the same for the World Bank. In practice, the Union can exert considerable influence on the activities of the specialized agencies of the United Nations due to its coordination with Member States, its normative weight and its essential role as a financial contributor. The EU is committed to strengthening and maintaining the UN's credible position on the international stage. As such, the EU's priority at the 2018 UN General Assembly was to support UN reform. The EU favors a rules-based global order with the UN at its core. The commitment to effective multilateralism is a central element of the EU's external action, as enshrined in the Treaty of Lisbon. The three pillars of UN reform run in parallel with the eight EU-UN strategic partnerships for peace operations and crisis management for the period 2019-2021. The interest of the European Union for the reform of international institutions is very high, and power can be exercised through its institutions in various ways**.**

Russian Federation - The latest version of the Foreign Policy Concept of the Russian Federation, approved in March 2023, clearly links the current official understanding of Russia's role in the modern world to its Soviet past: Russia's place in the world is determined by its significant resources in all areas of life, its status as a permanent

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chișinău, Moldova

member of the United Nations Security Council, a participant in the main intergovernmental organizations and associations, one of the two largest nuclear powers and the successor (continuing legal personality) of the USSR. Russia, taking into account its decisive contribution to the victory in the Second World War and its active role in shaping the contemporary system of international relations and eliminating the global system of colonialism, is one of the sovereign centers of global development. Overall, Russia's actions in Ukraine and its ability to block any response from the Security Council have contributed to an increasingly radical set of demands for reform. Many states are now calling for the complete abolition of the veto, as well as more frequent recourse to the General Assembly to avoid the use of the veto in the Security Council. For its part, Russia has presented itself as generally sympathetic to Security Council reform, declaring its general support but remaining vague and cautious on the details. At the opening of the 77th UN General Assembly in September 2022, Russian Foreign Minister Sergei Lavrov spoke in favor of better representation from Africa, Asia and Latin America in the Security Council, naming India and Brazil as "worthy candidates to become permanent members of the Council". Given the realities of contemporary Russian foreign policy, it is hard to be optimistic about Russian support for Security Council reform. Russia may eventually be open to a limited expansion of the Security Council — including additional permanent members — provided those candidates do not expect to receive veto power. One possible solution could be to designate places for regional groups rather than specific countries through an internal selection mechanism. While such measures would fall short of what some UN member states are demanding, they would be the first major step forward in reforming the Security Council since its expansion in 1965 [6].

Japan - joined the UN in 1956 and is a major contributor to the regular UN budget, second only to the United States. Since 2005, Japan has been a strong supporter of United Nations Security Council reform in a joint campaign with Germany, India and Brazil. While countries such as Britain, France and the United States support Japan's bid for a permanent seat in the UNSC, the country faces strong opposition from its two closest neighbors, China and South Korea. The Ministry of Foreign Affairs of Japan (2014) pointed out that this country was a major donor in the period 2004-2014, providing more than 20% of the total volume of public assistance for development. In addition, Japan is one of the largest donor countries in the world for the translation into practice of the main Millennium Development Goals (MDGs), in areas such as education, health, water and environment. Japan has contributed significantly to the socio-economic development of developing countries through programs based on the concept of "ownership of developing countries and their partnership with developed countries". Based on these principles, Japan aims to fully cooperate in efforts to achieve the internationally agreed development goals of the MDGs. [4]

India - as a founding member of the UN, India strongly supports the objectives and principles of the UN and has over time made significant contributions to the implementation of the objectives of the UN Charter, UN specialized programs and agencies. India has been a member of the UN Security Council for seven terms (a total of 14 years) and is a member of the G4 (Brazil, Germany, India and Japan), a group of nations that support each other for a permanent seat on the Security Council. Security of the UN, advocating in favor of its reform.

Brazil - Since the founding of the UN nearly eight decades ago, the Brazilian government has advocated for its own permanent seat on the UN Security Council. Although the willingness and ability of successive national administrations to properly

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chișinău, Moldova

lobby for reform has waxed and waned over the years, the goal has become one of the most entrenched pillars of Brazilian grand strategy. The belief that Security Council reform is necessary for the international order to be legitimate – and that Brazil is an obvious candidate for any expanded membership – has been stated so many times and repeated in so many documents that it is taken for granted understood throughout foreign policy. From a financial point of view, Brazil's position is not consistent with its desire for a seat on the Security Council. Between 2018 and 2022, Brazil's annual budget allocations to the UN fell from $92 million to $56 million, and as of December 2022, Brazil's outstanding debt to the UN stood at $300 million. [6]

Turkey - "The world is bigger than five" is a slogan first coined by Turkish President Erdoğan in 2013. Almost a decade later, it remains the central message of Turkey's ongoing campaign to reform the UN Security Council. As the size of the Security Council has not kept pace with the growth of the UN, Turkey has consistently criticized the exclusivity of the council. The absence of permanent members representing South America, Africa and the Islamic world not only attests to a representative injustice, but also demonstrates a failure to reflect multiculturalism. "Strengthening regional representation at the Security Council is a must." Turkey is also proposing a formal review of the relationship between the General Assembly and the Security Council, with the ultimate goal of expanding the authority of the General Assembly. Turkey's most radical—indeed, revolutionary—proposal is the complete abolition of permanent members' veto rights as a "first step toward UN reform." A more constructive and plausible reform agenda would be to create a new category of semi-permanent members, with longer-term and potentially renewable seats. Under this scheme, certain countries would be eligible for periodic elections (and re-elections) on a rotating basis. This could provide an attractive option to key regional powers such as Turkey, which aspire to play a more active role in global affairs. Eligibility criteria for this category could include, among other factors, a nation's overall financial contribution to the UN, its contributions to UN peacekeeping operations, the share of national GDP it allocates to development and humanitarian assistance, and the rate his participation in various specialized agencies. Ensuring fair representation of the Global South and the Islamic world would undoubtedly greatly enhance the credibility of this reform initiative. This new category of semi-permanent members should include at least some seats allocated to socioeconomic groupings such as least developed states or small island developing states, just as non-permanent member seats are designed to improve the geographical representation of different regions. The Russia-Ukraine war is widely seen as ushering in a new period defined by great power competition. Unlike the bipolar nature of the Cold War, however, the ongoing era is anticipated to be multipolar, with key regional powers such as Turkey expected to play more assertive roles in regional and global issues. These powers are generally inclined to act as so-called swing states, keeping channels and options open to all great powers while taking advantage of great power rivalries to maximize their own interests. [6]

Middle East - On the 75th anniversary of the UN, many leaders from the Middle East criticized in their speeches the way the United Nations and the international community is organized, functions and acts in the face of various problems in the region. Some of them stepped forward and came up with proposal and regarding the reform of the organization and especially of the UN Security Council.

African countries- African states have long advocated for the expansion and reform of the Security Council. The Security Council must be adapted to meet new and evolving challenges such as climate change, new pandemics and global terrorism. Such threats can be

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chișinău, Moldova

resolved, African leaders argue, only by an institution that represents the interests and perspectives of all humanity. African states have long lobbied the council to include development and poverty reduction, as well as controlling the flow of small arms, as key conflict prevention strategies. The African Union (AU) in March 2005 adopted a common position known as the Ezulwini Consensus. It called, among other things, for Africa "to be fully represented in all decision-making bodies of the UN, especially the Security Council", where the continent should have no less than two permanent seats, "with all the prerogatives and privileges of permanent member, including the right of veto", as well as five non-permanent seats. In June 2005, the AU issued the Sirte Declaration, reaffirming that Africa should be given two permanent veto seats and two non-permanent seats on a twenty-six member council. The Ezulwini Consensus and the Sirte Declaration pitted Africa against the G4 (Brazil, Germany, India and Japan), the main contenders for permanent seats on an enlarged council. In 2004, the G4 proposed expanding the Security Council to twenty-five members. Unlike the AU, however, the G4 has signaled some willingness to give up its veto power (at least during a transitional period) in exchange for a permanent seat on the Security Council. South Africa and Nigeria have tried to bridge the gap between the G4 and the AU, hoping that a common position will ensure their proposal gets the necessary two-thirds majority in the General Assembly. The two groups were unable to reach a consensus. Previous failed efforts to reform the Security Council have also exposed fault lines between African states themselves. Egypt, Nigeria and South Africa have been touted as the main contenders for permanent seats on an enlarged council. However, Egypt's dual identity as an African and Arab state has led many African nations to question its proper character. Nigeria and South Africa, as Africa's two largest economies, are generally accepted by non-African observers as having the most compelling cases to represent Africa, particularly because Nigeria has the continent's largest population and Africa's South the most sophisticated economy. However, other regional powers such as Kenya, Algeria, Ethiopia and Senegal contested the two countries' claims to continental leadership. [6]

Regarding Lobby/Economic Agents (Potential Investors), Potential Investors represent an interest group that generally supports the reform process, as it actually allows them to expand into new markets. Pressure groups (lobbys) exert pressure on political power to obtain decisions in line with their interests, influencing political power in sectoral decisions. In general, their power is relatively small, but the interest and impact of the reform on them is important.

Consumers and Labor Unions represent an important interest group, showing a high interest in the reform process. Instead, they have a less significant power and influence on this process because they do not have important resources nor the ability to mobilize resources. Unions are, in general, hostile to reforms for fear of repercussions on affiliated employees.

Stakeholder analysis can include a range of forms of analysis, from the very simple to the more sophisticated. A very simple stakeholder analysis technique is the Readiness/Power Matrix. This assesses, on an incremental scale from zero to high, how ready different stakeholders are to participate in an activity and how much power they have to influence its success. A Stakeholder Table can be combined with an Importance/Influence Matrix. The Table is used to set out the primary and secondary stakeholders, detail the interests of each and assign a value to the priorities of these interests (relative to the aims/priorities of the action being contemplated), and to assess the likely impact of any activity on them. The matrix takes the stakeholders and, using the data from the table, situates them in a two-by-two grid where one axis ranges from low to high

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chişinău, Moldova

importance, and the other from low to high influence. This can help inform strategies and priorities for engaging with various stakeholders **[7].**

In Table no. 1 presents an assessment of the interest and power of the Interest Groups involved in the process of reforming the most relevant international organizations. In order to remove the subjectivity of this evaluation, we also took into account the results of the situation analysis used in geopolitics (based on the data and information collected for the analysis of the geopolitical space – resources, the actors' perception of the geopolitical space, the approach and resolution of conflicts, etc.)

Table 1. Evaluation of the interest and power of interest groups in the process of reforming the most relevant international organizations

No. crt.	Interest Group	Interest in reform	The power (influence and importance) over the reform	Resources available for reform	The ability to mobilize resources for reform	The position of the group towards the reform	Impact/Effect of the reform on the group
(a)	(b)	(c)	(d)	(e)	(f)	(g)	(h)
A	US	**(+5)**	**(+5)**	-financial resources **(+5)** -coercion **(+5)**	**(+5)**	**(+5)**	**(+5)**
B	China	**(+4)**	**(+5)**	-financial resources **(+5)** -coerciţie **(+5)**	**(+5)**	**(+5)**	**(+5)**
C	European Union	**(+5)**	**(+5)**	-financial resources **(+5)** - coercion **(+5)**	**(+5)**	**(+5)**	**(+5)**
D	The Russian Federation	**(+2)**	**(+5)**	-financial resources **(+3)** - coercion **(+3)**	**(+2)**	**(+1)**	**(-1)**
E	Japan	**(+5)**	**(+5)**	-financial resources **(+5)** - coercion **(+5)**	**(+5)**	**(+5)**	**(+5)**
F	India	**(+5)**	**(+1)**	-financial resources **(-3)** -coerciţie **(+1)**	**(-3)**	**(+4)**	**(+4)**
G	Brazil	**(+5)**	**(+2)**	-financial resources **(+2)** - coercion **(+2)**	**(+2)**	**(+4)**	**(+3)**
H	Turkey	**(+5)**	**(+2)**	-financial resources **(+2)** - coercion **(+1)**	**(+1)**	**(+4)**	**(+4)**
I	Middle East	**(+5)**	**(+1)**	-financial resources **(+3)** - coercion **(+1)**	**(+3)**	**(+3)**	**(+4)**
J	Africa	**(+5)**	**(+1)**	-financial resources **(-3)** - coercion **(+1)**	**(-3)**	**(+1)**	**(+4)**
K	International Organizations (potential funders)	**(+5)**	**(+4)**	-financial resources **(+5)**	**(+1)**	**(+4)**	**(+4)**
L	Pressure groups (lobby)/Potenti al investors	**(+5)**	**(+2)**	-financial resources **(+4)**	**(+4)**	**(+3)**	**(+3)**
M	Consumers/ Labor Unions	**(+5)**	**(+2)**	-financial resources **(+2)**	**(+2)**	**(+1)**	**(+4)**

Note:(c) Estimation of the degree of interest the group has. This can be from Very High (+5), to Very Low (-5); It can also be: Uncertain or Unknown
(d) Powerful (+5), No Influence (0)
(e) Enumeration of the resources held by interest groups (eg: financial, status, legitimacy, coercion)
(f)Estimating how the group can mobilize resources. It can be from Very High (+5) to Very Low (-5); It can also be: Uncertain or Unknown
(g) Pro (+), with variation up to (+5); Against (-), with variation up to (-5).
(h) Positive (+5), Negative (-5)
Source: original

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chişinău, Moldova

Table 2. Classification matrix of interest groups
I=Interest, P=Power, H=High (>3), L=Low (≤ 3)

A: H.I. & L.P.:	**B: H.I. & H.P.:**
1. India 2. Brazil 3. Turkey 4. The Middle East 5. Africa 6.International Organizations (including potential funders) 7. Pressure groups (lobby)/Economic agents (Potential investors) 8. Consumers/ Labor Unions	1. The European Union 2. USA 3. China 4. Japan
C: L.I. & L.P.:	**D: L.I. & H.P.:**
	The Russian Federation

Source: original

Through the analysis of the Interest Groups, it was possible to identify those key groups that are important for the process of reforming the most relevant international organizations, that must be included in the process and that have sufficient strength to favorably influence this process. Thus, the groups listed on the right side of the stakeholder classification matrix at B and D and that hold "high power" are the key and most important groups for the success of the reformation process of the most relevant international organizations. So the Interest Groups important for the success of the Program are: the European Union; USA, China, Japan, Russian Federation. Note that in window D (L.I & H.P.) in the lower right is only the Russian Federation, indicating that it has an increased interest in the reform process (in the sense of keeping the current configuration), but its power to influence this process is (at least for now) quite reduced. On the other side of the matrix are the groups listed in window A (H.I & L.P.), for whom it is important, for the good progress of the reform process, to find the means by which to increase their interest in the reform process of the most relevant international organizations. They are: India, Brazil, Turkey, Middle East, Africa, International Organizations (including potential funders), Consumers/Labor Unions.

In fact, however, all interest groups related to the reform process must be involved and, for its success, those means will have to be identified by which high-powered, disinterested groups do not obstruct the reform process.

CONCLUSIONS

The new global geopolitical and geoeconomic context differs substantially from the developments recorded in the 19th and 20th centuries; we are witnessing in the 21st century a redefinition of power relations worldwide, a shift in the centers of power and a marked affirmation of multipolarity.

Few global issues have taken on more current importance than the future of the postwar, rule-based international order. Revisionist pressure against the order today is not as much opposed to the idea of multilateral rules and institutions *per se* as it is to US hegemony over key aspects of the order. The post-1945 order has come under

DOI: https://doi.org/10.53486/escst2023.28
International Conference, December 07-08, 2023, Chișinău, Moldova

unprecedented strain from the ambitions of increasingly revisionist powers, challenges to the underlying neoliberal ideology of the order.

The UN is a symbol of multilateralism and sustained global efforts for peace, security and sustainable development. Strategic autonomy, national security and other non-economic goals (environmental sustainability, worker protection and human rights) motivate calls for collaboration between countries with similar political-economic values and systems. In today's conditions, security considerations have already become more prominent in trade relations. Since the late 1990s, several scenarios have been proposed for the reform of the United Nations: the reform of the Security Council, the reform of the UN Secretariat, the financial reform, the reform of human rights, the reform of operational activities and, last but not least, the reform of the Economic and Social Council.

Although the reform should always generate a positive impact on society, experience has shown that the real interest in the reform of international institutions is still low, while the power and influence on the reform process is very high.

BIBLIOGRAPHY

1. MIRON, D. (coord.), COJANU, V.(coord.), BURNETE, S.,*Comerț internațional, vol.I, Specializarea țărilor și sistemul comercial multilateral*, Editura ASE, București, p. 369-389, 2013, ISBN: 978-606-505-775-3/ 978-606-505-776-0.
2. HOEKMAN B., MAVROIDIS, P.C. *WTO Reform: Back to the Past to Build for the Future*, Global Policy Volume 12 . Supplement 3, 2021, [viewed 03 december2023]. Available from: <https://olinelibrary.wiley.com/doi/full/10.1111/1758-5899.12924>
3. AKMAN, M.S., *The Need For WTO Reform: Where To Start In Governing World Trade*, T20 Saudi Arabia, 2020.
4. DUMITRESCU, A. L., OEHLER ȘINCAI, I. M.,*Reforma ONU: obiective, propuneri și priorităţi,* Revista de Economie Mondială, 11(2), 2019,[viewed 29 november2023]. Available from: <https://oaji.net/articles/2020/3365-1588087929.pdf>
5. ZAMFIR I., FARDEL T., *European Union involvement in the United Nations system*,Brussels, European Union. 2020, [viewed 02 december2023]. Available from: <https://www.europarl.europa.eu/RegData/etudes/IDAN/2020/652081/EPRS_IDA(2020)652081_FR.pdf>
6. PATRICK, S. (Ed),*UN Security Council Reform: What the World Thinks*. Carnegie Endowment for International Peace, Washington, DC, 74 pp., 2023, [viewed 01 december2023]. Available from: <https://carnegieendowment.org/files/Patrick_et_al_UNSC_Reform_v2_1.pdf>
7. DFID, *Tools for Development*. 2002, [viewed 28 november2023]. Available from: <http://www.protectedareas.info/upload/document/toolsfordevelopment-dfid.pdf>

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

ИСПОЛЬЗОВАНИЕ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БИЗНЕСЕ И ОБЩЕСТВЕ: УГРОЗЫ И РЕГУЛИРОВАНИЕ

USE OF ARTIFICIAL INTELLIGENCE IN BUSINESS AND SOCIETY: THREATS AND REGULATION

Olga PUGACHEVA

PhD,
Gomel State University 'Francisk Skorina', Republic of Belarus,
ORCID 0000-0003-4554-0038
E-mail: OPugacheva@gsu.by

Abstract: *The paper considers issues related to the relevance of research into the safe use of artificial intelligence, identifying vulnerabilities and potential threats to the use of neural networks in business, as well as ethical aspects of the use of neural networks in order to prevent possible abuse of this technology in society. Current data characterizing the development of the global market of artificial intelligence, related to reflecting the attraction of investments in this sphere, and various indicators reflecting the forecasts of its development are studied. The indicators characterizing the AI market, its users, solved problems, labor market, forecasts of its development and emerging risks are summarized. The indicators of AI market development in Russia, including the level of use of the main groups of AI technologies (in % of the number of organizations-users of AI), as well as in the Republic of Belarus are considered.*

On this basis, the main global trends in the AI sphere are identified: the desire of states for technological sovereignty in conditions of mutual restrictions, toughening competition for human resources, development of safe artificial intelligence, the desire of scientific researchers in various technological fields to use increasingly powerful large language models and generative AI, the growth of economic effect from the use of AI.

The paper analyzes the possibilities of using neural networks to solve various business and marketing tasks: analytics and forecasting, user service, personalized marketing, content generation, market research, and voice assistant.The paper explores the directions of solving business tasks using neural networks in various organizations and spheres of activity: large retailers, technology companies, hospitality companies, financial institutions, travel agencies. The threats and risks arising in this process are shown, related to hacker attacks, insufficient data verification, decision making without explanation, training failures, personal data security and others. The main dangers of using neural networks, directions of legislative regulation of artificial intelligence development are formulated.

Keywords: *artificial intelligence, neural networks, business, threats, security, regulation.*

UDC: *004.8:005.334*

JEL Classification: *O3, K24, F52, C8.*

ВВЕДЕНИЕ

Исследование безопасного использования искусственного интеллекта и нейросетей является актуальной темой в современном мире, где искусственный интеллект и машинное обучение все более внедряются в различные сферы деятельности и жизни. Нейросети используются в медицине, финансах, автомобильной промышленности, обороне, и многих других областях, что делает их безопасность критически важной.

Исследования в этой области помогают выявить уязвимости и потенциальные угрозы, связанные с использованием нейросетей. Это включает в себя анализ защиты от атак, проверку на проникновение, а также разработку методов обнаружения и предотвращения возможных угроз безопасности. Также важно

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

изучать этические аспекты использования нейросетей, чтобы предотвратить возможное злоупотребление этой технологии.

Безопасное использование нейросетей также имеет огромное значение для защиты личных данных и конфиденциальной информации. Исследования в этой области помогают разрабатывать методы шифрования и защиты данных, чтобы предотвратить утечку информации и несанкционированный доступ к ней.

ОСНОВНАЯ ЧАСТЬ

Рынок искусственного интеллекта (ИИ) становится процветающей отраслью, приносящей все больше преимуществ бизнесу.

По итогам 2023 года стартапы в области искусственного интеллекта в глобальном масштабе привлекли на развитие приблизительно $27 млрд, что является рекордным результатом. Предыдущий максимум на уровне $11 млрд был зафиксирован в 2021 году. Такие данные приводятся в исследовании компании PitchBook, результаты которого опубликованы в конце декабря 2023 года [1].

В отчете говорится, что из $27 млрд примерно две трети предоставлены корпорациями Microsoft, Google и Amazon. В частности, Microsoft вложила $10 млрд в компанию OpenAI — разработчика нейросети ChatGPT, а также участвовала в раунде финансирования ИИ-стартапа Inflection AI на сумму в $1,3 млрд. В свою очередь, Google и Amazon сообща выделили $6 млрд на поддержку молодой фирмы Anthropic, которая специализируется на разработке больших языковых моделей (рисунок 1) [1].

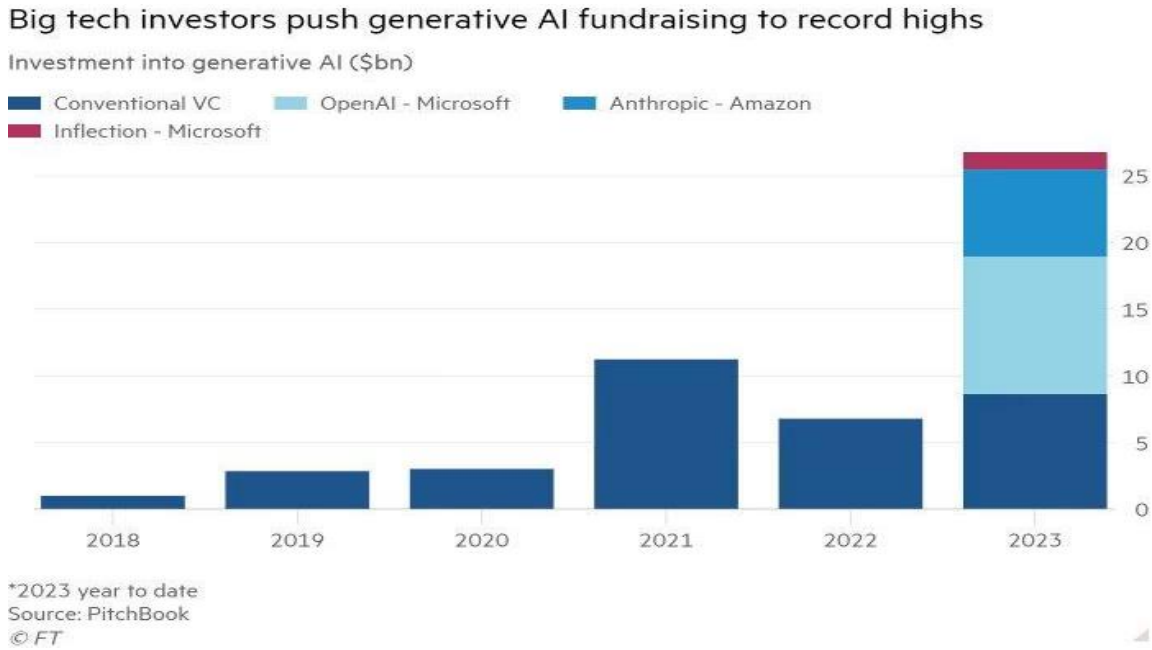


Рисунок 1. Инвестиции в развитие искусственного интеллекта в 2018-2023 гг.

Источник: https://www.tadviser.ru/index.php/

Обобщенные показатели, характеризующие рынок ИИ, его пользователей, решаемые проблемы, рынок труда, прогнозы его развития и возникающие риски, приводятся в таблице 1 [2].

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

Таблица 1. Обобщенные показатели, характеризующие развитие рынка ИИ

Показатели	Актуальные данные и прогнозы развития
1. Рынок ИИ	- $407 млрд достигнет объем рынка искусственного интеллекта к 2027 году; - 37,3% в год составят темпы роста ИИ с 2023 по 2030 год; - $1,8 трлн достигнет выручка глобального рынка ИИ в 2030 году; - более 1800 компаний в мире разрабатывают модели естественного языка для различных сфер; - на $15,7 трлн вырастет мировой ВВП благодаря ИИ в 2030 году; - 26% роста ВВП Китая придется на ИИ-отрасль в 2030 году, причем страна получит 26 % мирового рынка искусственного интеллекта; - минимум одна компания в сфере ИИ выйдет на IPO в 2024 году; - более $1 млрд будет тратиться на обучение одной большой языковой модели в 2024 году; - $180 млрд достигнет объем рынка носимых устройств с искусственным интеллектом к 2025 году; - 90% интернет-контента будет создаваться при помощи искусственного интеллекта к 2026 году.
2. Пользователи ИИ	- 314 млн человек будут использовать инструменты ИИ в 2024 году; - 54% пользователей считают, что ИИ может улучшить объемный текстовый контент, к примеру содержимое сайта; - 97% мобильных пользователей используют голосовых помощников на базе искусственного интеллекта; - 41% пользователей считают, что искусственный интеллект тем или иным образом улучшит их жизнь; - 65% потребителей не теряют доверие к бизнесу, который использует технологии ИИ; - 1,5 млрд человек в мире уже используют чат-ботов; - 8,4 млрд достигнет число устройств с голосовым помощником в мире к 2024 году — это больше, чем население Земли
3. Бизнес и ИИ	- 97% владельцев бизнеса считают, что ChatGPT поможет их компаниям; - 87% транснациональных корпораций уверены, что интеграция искусственного интеллекта будет способствовать росту их бизнеса на высококонкурентном рынке; - 80% руководителей считают, что ИИ-автоматизацию можно применить к любому бизнес-решению; - 35% мировых компаний уже активно используют ИИ; - 73% компаний используют или планируют внедрять чат-ботов для общения с клиентами; - более 80% предприятий будут использовать API и модели генеративного искусственного интеллекта, а также ИИ-приложения к 2026 году; - 92% предприятий уже добились измеримых результатов от использования ИИ в бизнес-операциях; - 40% организаций увеличат инвестиции в ИИ; - 64% предприятий ожидают, что ИИ улучшит их операции и взаимодействие с клиентами; - 95% взаимодействий бизнеса с клиентами будет осуществляться с

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

	помощью ИИ к 2025 году; - 92% разработчиков в США уже используют инструменты ИИ для задач программирования как на работе, так и вне ее; - на 50% к 2026 году вырастет эффективность моделей ИИ в компаниях, которые внедряют прозрачность, доверие и безопасность в системы на базе искусственного интеллекта; - $1 млрд ежегодно экономит стриминговый сервис Netflix, используя машинное обучение в целях создания индивидуальных рекомендаций для пользователей; - на 225% ускорила время выбора продуктов торговая площадка Amazon благодаря машинному обучению; - каждый десятый автомобиль будет беспилотным благодаря технологиям ИИ к 2030 году
4. ИИ и рынок труда	- 77% респондентов опасаются, что ИИ может привести к потере рабочих мест в ближайшем будущем; - 300 млн работников по всему миру может вытеснить искусственный интеллект по мере своего развития; - от 75 млн до 375 млн человек придется сменить профессию уже к 2030 году; - в 14 раз чаще будут увольнять работников низкооплачиваемых профессий в США к 2030 году из-за автоматизации их обязанностей; - 97 млн рабочих мест создаст ИИ к 2025 году; - до 40% к 2035 году повысится производительность труда в 16 отраслях, включая обрабатывающую промышленность, благодаря внедрению технологий ИИ; - 30% компаний внедряют технологии искусственного интеллекта из-за нехватки человеческих ресурсов и для автоматизации рутинных задач; - около $160 тыс. в год составляет средняя зарплата инженера в сфере ИИ; - 35% компаний обеспокоены тем, есть ли у их сотрудников необходимые технические навыки для эффективного использования ИИ; - 37% компаний инвестируют в обучение и внедряют другие стимулы для более быстрого осваивания сотрудниками навыков работы с ИИ; - 61% сотрудников планируют использовать ИИ в своей работе; - 3 дня в неделю будут работать люди, когда ИИ станет достаточно развитым, считает основатель Microsoft Билл Гейтс.
5. Опасения и риски использования ИИ	- 28 государств подписали Декларацию Блетчли — первое международное соглашение, направленное на устранение угроз, исходящих от ИИ; - более 75% потребителей контента обеспокоены опасностью распространения дезинформации с помощью ИИ; - 56% компаний называют неточность работы моделей главным риском при внедрении ИИ; - 75% руководителей опасаются, что неспособность внедрить ИИ может привести к закрытию их бизнеса уже в 2024 году; - только 52% респондентов смогли отличить сгенерированный ChatGPT-3 контент от созданного человеком; - к 2025 году может закончиться доступный запас открытых данных для обучения ИИ.

Источник: https://trends.rbc.ru/trends/industry/657963559a79474dd4bc9b88

Данные о развитии рынка ИИ в Российской Федерации показывают, что по количеству генеративных моделей ИИ Россия занимает 4-е место в мире, а по

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

совокупной мощности суперкомпьютеров — входит в топ-10. Объём российского рынка ИИ по итогам 2022 года превысил 650 млрд рублей, что на 18% больше, чем в 2021 году. Более 1000 российских компаний ведут разработки в этой сфере. Создано более 90 исследовательских центров для изучения ИИ и разработки новых решений. Во многих отраслях уже состоялся переход от стадии разработки технологий ИИ к их практическому применению. Правительство РФ одним из первых в мире начало работать на собственных платформенных решениях. В 2023 году стартовал переход всех государственных органов исполнительной власти и региональных органов власти на платформу «ГосТех», в которой содержится модуль ИИ [3].

Специально разработанный индекс интеллектуальной зрелости по внедрению ИИ достиг 31,5% в приоритетных отраслях экономики. Лидируют в этом финансовый сектор, сфера информационно-коммуникационных технологий и здравоохранение. По сравнению с 2021 годом в 2022 году средний уровень использования ИИ в РФ вырос в 1,5 раза. Уровень внедрения ИИ в федеральных органах исполнительной власти составляет более 60% [3].

Институт статистических исследований и экономики знаний (ИСИЭЗ) НИУ ВШЭ 26 сентября 2023 года поделился итогами проведенного исследования, в ходе которого эксперты оценили развитие и распространение искусственного интеллекта в России, изучили специфику использования решений на основе ИИ и связанные с этим направлением технологий тренды инновационной деятельности компаний [3].

По данным ИСИЭЗ НИУ ВШЭ, две трети (65%) обследованных организаций применяют ИИ пока в тестовом (экспериментальном) режиме, изучая и оценивая возможности новых решений для бизнеса. Примерно 3/4 респондентов используют ИИ совместно с другими цифровыми технологиями. В половине случаев речь идет о различных видах промышленного ПО, включая системы автоматизированного проектирования, управления процессами и др. Более четверти (27%) организаций применяют ИИ наряду с технологиями Интернета вещей, 38% — в связке с коммуникационными сервисами, обеспечивающими взаимодействие с клиентами и решение маркетинговых задач.

Наиболее востребованы продукты на основе технологий компьютерного зрения и распознавания и синтеза речи (78,7% и 62% ответов соответственно). Активно применяются и рекомендательные системы на основе и больших данных (40,7%), обеспечивающие функции прогнозирования развития ситуаций и поведения объектов, например, при обслуживании оборудования и транспортных средств. По оценкам экспертов ИСИЭЗ, чаще всего ИИ-решения оптимизируют управленческие задачи (продажи и маркетинг, финансовый и бухгалтерский учет), в меньшей степени — производственные процессы. Гораздо реже (около 10%) респонденты применяют интеллектуальные системы управления для автоматизации сложных процессов, которые трудно контролировать традиционными методами.

Уровень использования основных групп технологий ИИ (в % от числа организаций-пользователей ИИ) в РФ в 2023 г. приводится на рисунке 2 [3].

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

Рисунок 2. Уровень использования основных групп технологий ИИ (в % от числа организаций-пользователей ИИ) в 2023 г.
Источник: https://www.tadviser.ru/index.php/

Кроме того, проведенные аналитические исследования с августа 2022-го по февраль 2023 г. Показали, что количество пользователей нейросетей в России выросло в пять раз, а продолжительность взаимодействия с ИИ – в три раза [4].

Что касается Республики Беларусь, то по данным Белстата об использовании информационно-коммуникационных технологий населением и коммерческими организациями в 2022 году [5], технологии искусственного интеллекта составили только 3,6 % от общего количества используемых организациями ИКТ. Отмечается, что за последние пять лет в Республики Беларусь активно растет интереса к нейросетям у государственных структур, крупного бизнеса и населения. Так, в 2022 году показатель их востребованности в стране увеличился в десять раз, а за два последних года, – в двадцать раз [6].

Эксперты выделяют пять основных глобальных трендов в сфере ИИ [3]:

1. Стремление государств к технологическому суверенитету в условиях взаимных ограничений, когда отдельные страны закрывают доступ к своим разработкам.
2. Ужесточение борьбы за кадры. Поэтому правительство стремится обеспечить российским специалистам в области ИИ лучшие условия работы. Альянс в сфере ИИ совместно с Минобрнауки разработал рейтинг качества подготовки специалистов по искусственному интеллекту, который показывает, насколько образовательные программы различных вузов отвечают запросам рынка. Топ-10 российских университетов в этом рейтинге уже серьёзно конкурируют за звание лучших и готовят высококвалифицированных специалистов.
3. Развитие безопасного искусственного интеллекта. Имеется в виду переход от клиентоцентричной к человекоцентричной модели, когда приоритетами для государства и бизнеса становятся интересы конкретного человека. Поэтому важным является понимание, что при дальнейшем развитии ИИ всё большее значение приобретают вопросы этики искусственного интеллекта. За два года к Кодексу этики искусственного интеллекта присоединилось около 330 организаций, в

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

том числе 23 зарубежные и почти 60 российских органов исполнительной власти.

2. Стремление научных исследователей в различных технологических областях использовать всё более мощные большие языковые модели и генеративный ИИ. По экспертным оценкам, в ближайшие 10 лет такие технологии добавят около 7 трлн долларов к мировому ВВП.
3. Рост экономического эффекта от использования ИИ. По экспертным оценкам, к 2030 году в мировой экономике он превысит 15 трлн долларов.

В настоящее время широкое распространение для решения задач бизнеса и маркетинга получило использование модели искусственного интеллекта от OpenAI – ChatGPT. Основными преимуществами чат-ботов с искусственным интеллектом является круглосуточное обслуживание пользователей, оперативные отклики на запросы и ответы на простые вопросы.

ChatGPT может использоваться для решения различных задач в бизнесе и маркетинге (таблица 2) [7].

Таблица 2. Содержание результатов решения задач с использованием ChatGPT

Типы задач	Содержание результатов решения задач
1. Аналитика и прогнозирование	Обработка больших объемов данных в реальном времени с большой точностью и скоростью; обработка любого количества входящих запросов и генерация текстов ответов на вопросы.
2. Обслуживание пользователей	Автоматизация процесса обслуживания клиентов через онлайн-чаты или чат-боты; ответы на вопросы пользователей, предоставление информации о продуктах и услугах; помощь в решении проблем и разрешении конфликтов.
3. Персонализированный маркетинг	Помощь в создании персонализированных сообщений и рекомендаций для пользователей; анализ данных о предпочтениях и поведении пользователей с целью предложения им наиболее подходящих продуктов или услуг.
4. Генерация контента	Создание контента (статьи, блоги, рекламные тексты и описания продуктов); генерирование уникальных и привлекательных текстов в соответствии с заданными параметрами и требованиями.
5. Маркетинговые исследования	Помощь в проведении маркетинговых исследований на основе анализа текстовых данных (отзывов клиентов, комментариев в социальных сетях) и обратная связь с пользователями; выявление тенденций, предсказание потребительских предпочтений и помощь в разработке маркетинговых стратегий.
6. Голосовой помощник	Ответы на вопросы пользователей и предоставление информации о продуктах и услугах путем голосовых сообщений.

Источник: собственная разработка

ChatGPT может быть использован в различных организациях для решения их бизнес-задач (таблица 3) [7].

В контексте поиска финансовой выгоды от использования ИИ следует учитывать, что помимо экономических эффектов существуют ещё и социальные, институциональные и другие. Поэтому важно подобрать правильный подход к регулированию этой технологии. Существует несколько таких подходов:

– приоритет отдаётся саморегулированию со стороны бизнеса;
– гибридный, когда акты жёсткого нормативного регулирования комбинируются с саморегулированием;

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

– ограничительный подход, когда регулирование сосредоточено на рисках и ограничениях.

Таблица 2. Содержание бизнес-задач в различных организациях с использованием ChatGPT

Виды организаций	Содержание бизнес-задач
1. Крупные ритейлеры	Организации розничной торговли могут использовать ChatGPT для обслуживания клиентов через онлайн-чаты или чат-боты, для ответов на вопросы клиентов, их возражения и замечания; предоставление информации о продуктах и услугах; помощи с выбором продуктов и решением проблем покупателей.
2. Технологические компании	Компании, занимающиеся разработкой и реализацией научно-технической продукции и услуг, могут использовать ChatGPT для обслуживания пользователей и предоставления технической поддержки; для ответов на вопросы о функциональности продуктов; помощи в устранении неполадок и предоставлении рекомендаций по использованию.
3. Компании в сфере гостеприимства	Отельеры и другие организации в сфере гостеприимства могут использовать ChatGPT для обслуживания клиентов и предоставления информации о бронировании, услугах и местных достопримечательностях; для ответов на вопросы клиентов, помощи с бронированием мест проживания и предоставлении рекомендаций об объектах для посещения.
4. Финансовые учреждения	Банки и страховые компании могут использовать ChatGPT для обслуживания клиентов через онлайн-чаты или чат-боты, ответов на вопросы клиентов о продуктах и услугах, помощи в решении проблем с платежами, предоставлении финансовых консультаций.
5. Туристические агентства	Компании в сфере туризма и путешествий могут использовать ChatGPT для обслуживания клиентов и предоставления информации о турах, бронировании и визовых вопросах, для ответов на вопросы клиентов, предоставлении рекомендаций по выбору тура и помощи в бронировании мест проживания.

Источник: собственная разработка

Использование нейросетей в бизнесе имеет как проблемы, так и перспективы. Однако опасности, связанные с использованием нейронных сетей в бизнесе и в обществе, могут быть достаточно серьёзными. Основные из них следующие.

– **хакерские атаки.** Искусственные нейронные сети могут быть использованы хакерами для выпуска более сложных и адаптивных вирусов, создания фальшивых документов, а также для мошенничества при онлайн транзакциях;
– **недостаточность проверки данных.** Нейронные сети работают на основе обучения на данных в условиях, когда могут существовать недостатки в проверке и контроле этих данных, что может привести к неправильным выводам или к получению недостоверной информации;.
– **принятие решений без объяснения.** Нейронные сети могут принимать решения без объяснения своего решения, что может создать риски в отношении ответственности в бизнесе и в обществе в целом;
– **сбои в обучении.** Любые сбои или ошибки в процессе обучения могут вызвать серьезные проблемы в работе нейронной сети, что может привести к неверным выводам или даже риску для жизни (например, в случае с нейронными сетями, используемыми для управления автономными автомобилями);

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

- **личные данные.** Данные, используемые для обучения нейронных сетей, часто содержат чувствительную информацию, которая может быть использована для неправильных целей, если попадет к недобросовестным лицам;
- **использование искусственного интеллекта может привести к чрезмерной автоматизации производственных и бизнес-процессов**: В результате могут возникнуть угрозы потери рабочих мест и к созданию общества, в котором компьютеры замещают человеческие роли, что в свою очередь может вызвать социальные проблемы.

Поэтому важно обеспечить тщательное регулирование и качественную этику искусственного интеллекта для минимизации этих рисков и угроз. Безопасность данных, разработка объяснимого ИИ и надежного управления рисками - все это должно стать приоритетными областями в использовании нейронных сетей в обществе и бизнесе.

Законодательство, регулирующее использование искусственного интеллекта и нейросетей в бизнесе и обществе отличается в разных странах и регионах. Основные направления законодательного регулирования включают защиту личных данных, этику ИИ, безопасность и ответственность:

1. **защита личных данных.** В европейском союзе защита данных регулируется Общим регламентом по защите данных (GDPR), который устанавливает строгие требования к сбору, хранению и использованию персональных данных. В США также существуют различные законы на уровне штатов, такие как Калифорнийский закон о защите потребителей в интернете (CCPA).
2. **этика искусственного интеллекта.** Этот аспект законодательства еще находится в разработке в многих странах. В 2021 году Европейский Союз предложил первое в мире законодательство по искусственному интеллекту, которое регулирует использование ИИ и устанавливает стандарты для «высокорисковых» используемых систем.

Некоторые отраслевые группы и организации, в частности Китай, пытаются сформировать и ввести принципы этического регулирования использования нейросетей, которые призваны обеспечить этическое использование нейросетей и защитить права и интересы пользователей [8]. Эти принципы сформулированы следующим образом:

1 **принцип прозрачности**, который предполагает, что нейросети должны быть понятными и объяснимыми для пользователей;

2 **принцип ответственности**, который подразумевает, что создатели и владельцы нейросетей несут ответственность за их использование и возможные последствия;

3 **принцип справедливости**, который требует, чтобы нейросети не дискриминировали людей на основе расы, пола, возраста и других характеристик;

4 **принцип безопасности**, который подразумевает, что нейросети должны быть защищены от злоупотреблений и кибератак.

5 **безопасность и ответственность.** Вопросы безопасности и ответственности в области ИИ традиционно сложны из-за природы принятия решений с

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

использованием ИИ. Законодательство в этой области еще находится в разработке, но обычно центральной фигурой при обсуждении этих вопросов являются производители, которые могут привлекаться к ответственности в случае неправомерного использования нейросетей.

Так, YouTube разработал новые правила в отношении дипфейков. С 2024 года по требованиям платформы, контент, созданный нейросетями, обязательно должен быть отмечен специальной макировкой [9]. За несоблюдение правил будут наказывать отключением монетизации или удалением видео, но уровень вредности контента будет оценивать сам YouTube. Например, пародии или сатиру в отношении публичных людей удалять не будут. Новые правила также начнут работать для ИИ-музыки. Лейблы смогут удалять контент, исполненный в манере известных музыкантов.

ВЫВОДЫ

В результате исследования выявлено, что банковское дело, финансовые услуги, страхование и здравоохранение занимают наибольшую долю рынка искусственного интеллекта.

Ответы на сообщения, ответы на финансовые вопросы, планирование маршрутов путешествий и публикация контента в социальных сетях стали наиболее популярными вариантами применения ИИ в 2023 году.

Важно отметить, что нормативно правовое регулирование использования ИИ еще находится в стадии формирования, и необходимо больше усилий для того, чтобы обеспечить соответствующие и эффективные стратегии регулирования в этой быстро развивающейся сфере деятельности.

Таким образом, исследование безопасного использования нейросетей играет важную роль в обеспечении безопасности и защиты личных данных в условиях все более широкого применения искусственного интеллекта.

БИБЛИОГРАФИЯ

1. Искусственный интеллект (мировой рынок) [онлайн]. 2023 [Дата доступа: 3.11.2023]. Режим доступа: <https://www.tadviser.ru/index.php>
2. Искусственный интеллект в цифрах и фактах [онлайн]. 2023 [Дата доступа: 11.11.2023]. Режим доступа: <https://trends.rbc.ru/trends/industry/657963559a79474dd4bc9b88>
3. Искусственный интеллект (рынок России) [онлайн]. 2023 [Дата доступа: 13.11.2023]. Режим доступа: <https://www.tadviser.ru/index.php>
4. Число пользователей нейросетей в России выросло в пять раз за полгода [онлайн]. 2023 [Дата доступа: 13.11.2023]. Режим доступа: <https://www.vedomosti.ru/technology>
5. Информационное общество в Республике Беларусь, 2023. [онлайн]. 2023 [Дата доступа: 3.11.2023]. Режим доступа: <https://www.belstat.gov.by/ofitsialnaya-statistika/index_77679>
6. За год популярность нейросетей в Беларуси выросла в 10 раз. [онлайн]. 2023 [Дата доступа: 28.10.2023]. Режим доступа: <https://providers.by/2023/04/digest/ >
7. ПУГАЧЕВА О. В. Использование искусственного интеллекта в бизнесе. Актуальные вопросы современной экономической науки: теория и практика:

DOI: https://doi.org/10.53486/escst2023.29
International Conference, December 07-08, 2023, Chişinău, Moldova

сборник научных статей. Выпуск 2.– Гомель : ГГУ им. Ф. Скорины, 2023, С. 209-212.

8. YouTube адаптирует свою политику к предстоящему всплеску видео с искусственным интеллектом [онлайн]. 2023 [Дата доступа: 25.11.2023]. Режим доступа: <https://techcrunch.com/2023/11/14/youtube-adapts-its-policies-for-the-coming-surge-of-ai-videos>
9. Правовой фреймворк для использования нейросетей: как государства могут регулировать искусственный интеллект [онлайн]. 2023 [Дата доступа: 25.11.2023]. Режим доступа: <https://www.cossa.ru/news/322021>

Economic Security in the Context of Systemic Transformations

DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chişinău, Moldova

ПСИХОСОЦИАЛЬНАЯ АДАПТАЦИЯ ЛИЦ С ОСОБЫМИ ОТРЕБНОСТЯМИ КАК ОДИН ИЗ ФАКТОРОВ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ СТРАНЫ

PSYCHOSOCIAL ADAPTATION OF PERSONS WITH SPECIAL NEEDS AS ONE OF THE FACTORS OF NATIONAL SECURITY OF THE COUNTRY

Angela POLEVAIA-SERCĂREANU,

PhD, Associate Professor,
Comrat State University
State University of Physical Education and Sport, Moldova,
ORCID 0000-0002-7186-9462
E-mail:poleangela1975@mail.ru

Abstract: *The paper examines the features of the demographic situation that has developed in recent years in terms of an increase in the birth rate of children with special needs, personnel shortages and additional pressure on the social protection system, which have a direct relationship and impact on the security of the individual, society and the state. The main difficulties associated with the psychosocial adaptation of persons with special educational needs into society, which is associated with the fulfillment of a number of socio-economic conditions, the main of which is access to quality education and multilateral development, are analyzed. Organizational forms of health, physical education and sports activities were studied as the most effective opportunity for the socialization of children with special educational needs.*
Analytical and statistical research methods were used, including the method of constructing and analyzing time series. A sociological study was conducted to study the attitude of the adult population to the possibility of psychosocial adaptation of children with special needs in the process of physical education in general education and sports schools. The respondents were: teachers of secondary schools, specialists from various fields, including teachers of physical education, parents of children with special educational needs, sports coaches.

Keywords: *motor activity, autism, survey, national security.*

UDC: *[316.344.6:364.048.6+376.5:372.853](478)*

JEL Classification: *I38; J13; O15.*

ВВЕДЕНИЕ

Одна из основных задач решения общенациональной проблемы, имеющие прямое отношение к повышению или снижению экономической безопасности страны, является человеческий капитал, их возможный потенциал, физические и умственные способности, которые могут быть применены для того, чтобы увеличить производительность и социально-экономическую эффективность системы государства [1].

В многочисленных исследованиях в области экономических наук отмечаются факторы повышения эффективности социально-экономической системы, которые отражают основные пропорции развития и функционирования таких структур как: финансовой, инвестиционной, экономической, социальной и демографической [2].

Вопрос демографического состояния для любой страны весьма значительно, поскольку численность населения играет значимую роль в конкурентоспособности государства [3]. Понятие “демография” с греческого языка означает “описание народа”, и напрямую связано со всеми сферами жизнедеятельности человека. На

DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chişinău, Moldova

примере уровня рождаемости, можно наблюдать эволюцию изменений, отражающих на процентное соотношение поступающих в высшие учебные заведения, изменения структуры занятости населения в профессиональном плане, дефицита рынка труда, конкурентоспособности человеческого капитала, и т. д. [4]-[5].

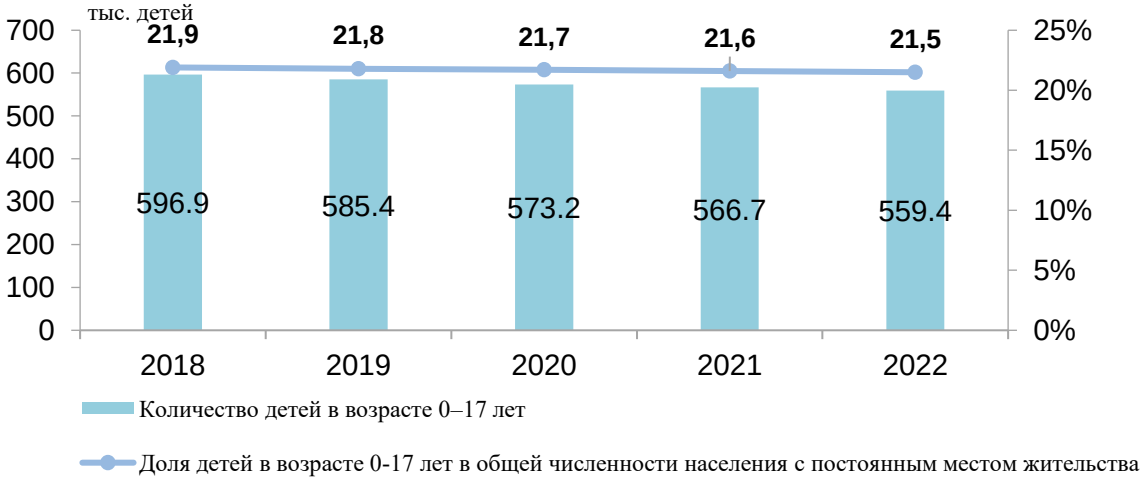
Национальная стратегическая программа в области демографической безопасности Республики Молдова (2011-2025г.г.) диктует новое видение политик развития способностей человеческого потенциала, направленная на согласование всех мер для решения проблем населения, как основного индикатора эффективности любого государства. Согласно последним демографическим теоретическим выводам, представленные в программе, демографический переходный период определяется не только спадом рождаемости и смертности, но к ним добавляются также и изменения в возрастной структуре населения, семьи, миграции, и т.д. Таким образом, явление «демографического спада» выражается в продолжающемся спаде численности населения из-за отрицательного естественного прироста населения и отрицательного сальдо миграции. В то же время сокращение рождаемости привело к дисбалансу возрастной структуры населения и ускорило процесс демографического старения [6].

МАТЕРИАЛЫ И МЕТОДЫ

Использовались аналитические и статистические методы исследования, в том числе метод построения и анализа динамических рядов. Было проведено социологическое исследование с целью изучения отношения взрослого населения к возможности психосоциальной адаптации детей с особыми потребностями в процессе физического воспитания в общеобразовательных и спортивных школах. В качестве респондентов выступили: педагоги общеобразовательных школ, специалисты из разных областей, родители детей с особыми образовательными потребностями, специалисты в области спортивной тренировки.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Бесспорно, ключевая проблема демографической политики состоит в росте уровня рождаемости, к сожалению, в последнее время наблюдается уменьшение количества детей (Рисунок 1).



DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chişinău, Moldova

Рисунок 1. Число рождаемости детей и увеличения численности населения за пять лет, период 2018-2022 гг.

Источник: [6] https://statistica.gov.md

По данным Национального бюро статистики на 1 января 2022 года количество детей в возрасте 0-17 лет в Республике Молдова составило 559,4 тыс., или 21,5% от общего количества населения с обычным местом жительства. Что вызывает настороженность за будущее [7].

Однако, по нашему мнению необходимо изучить и проблему рождаемости детей с ограниченными возможностями, и на примере рисунка 2 мы можем выделить стремительный рост рождаемости детей с ограниченными возможностями [8].

Более того, изучение проблемы исследования позволило отметить, что в последние годы в стране произошли значительные изменения и в показателях рождаемости детей с ограниченными возможностями. Таким образом, в период с 2019 г. по 2023 г. мы можем наблюдать рост показателей рождаемости количества детей с ограниченными возможностями в возрасте 0-17 лет в Республике Молдова (Рисунок 2).

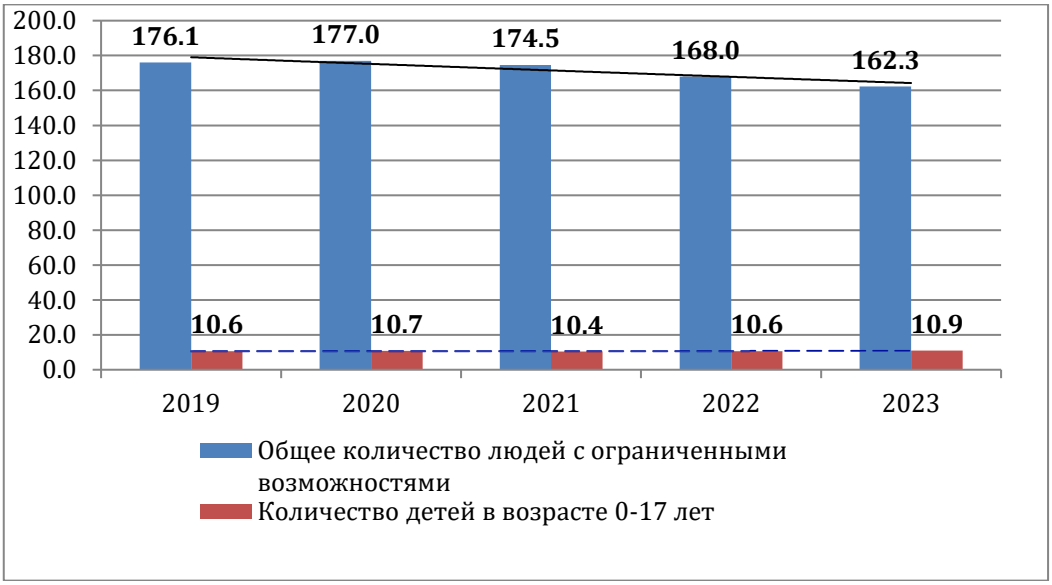


Рисунок 2. Число рождаемости детей и увеличения численности населения за пять лет, период 2018-2022 гг.

Источник:[6] https://statistica.gov.md

Из общей классификации людей с ограниченными возможностями, мы акцентировали внимание на детей с особыми потребностями, в особенности выделили рождаемость детей с аутистическими расстройствами, поскольку в последние годы все большее распространение получают аутистические расстройства различной этиологии [8]-[9].

Предоставленные данные международной компанией „Focus for Health", в начале 2019 года количественные показатели в некоторых странах выглядели следующим образом, рисунок 3: на первом месте оказался Гонконг, где 372 ребенка на 10 тысяч были диагностированы с аутизмом [10]. При этом каждому 27-му ребенку в Гонконге был поставлен диагноз "растущая инвалидность", на втором месте оказалась Южная Корея, в этой стране выявлен самый высокий уровень аутистических расстройств диагностирован у 263 детей из каждых 10 000, или у

DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chişinău, Moldova

одного из 38. Третье место занимают Соединенные Штаты Америки с показателем около 263 детей на каждые 10 тысяч, или соотношением 1 ребенок из 45.

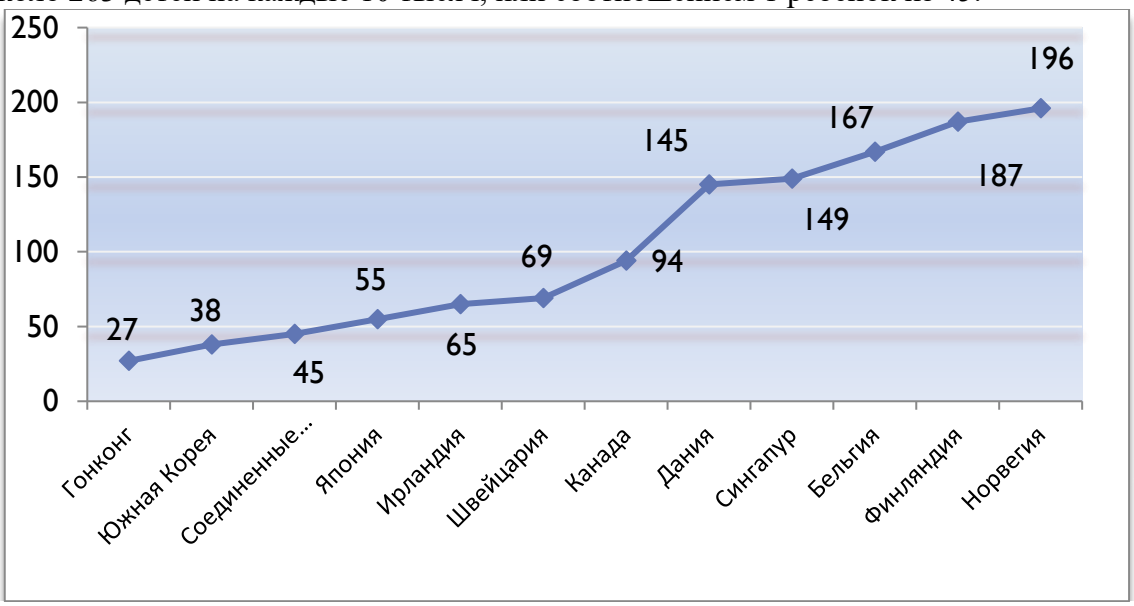


Рисунок 3. Данные представленные компанией „Focus for Health" о количестве детей, страдающих аутистическими расстройствами, в мире

Источник: [9] Draghici, E. (2016), pp. 58-60.

По мировой статистике, количество детей с аутизмом только за последние 10 лет увеличилось в десять раз (с 1 ребенка на 1500 новорожденных в 2000 году до 1 ребенка на 150 новорожденных в 2010 году) [3]. По официальным данным, представленные Всемирной организацией здравоохранения, в 2014 году в мире один ребенок из 160 страдал аутистическими расстройствами. Однако, было подчеркнуто, что соответствующая цифра была статистически средней и что в некоторых исследованиях, которые были тщательно проверены, реальные (эффективные) цифры были намного выше.

Программа развития инклюзивного образования в Республике Молдова на 2011-2020 годы, Стратегия развития образования на 2014-2020 годы, Кодекс об образовании, утвержденный в 2014 году, транслируют в сферу образования универсальные принципы из области основных прав и свобод человека и из области концепции инклюзии для обеспечения доступа к качественному образованию в общеобразовательной школе для всех детей.

За последние несколько лет в Республике Молдова были предприняты последовательные и одновременные действия во всех трех ключевых областях для внедрения инклюзивного образования*: политика, практика и инклюзивная культура.*

Однако когда мы обращаемся к теме детей с ограниченными возможностями в особенности детей с расстройствами аутистического спектра, одновременно возникает риторический вопрос: насколько общество в целом и школа в частности готовы принять таких детей?

Данные о проблеме распространенности расстройств аутистического спектра в странах с низким и средним уровнем дохода практически отсутствует. Что известно точно, так это то, что число аутистов имеет стабильную динамику роста во всем мире. К сожалению, статистики по аутизму в Республике Молдова, Украине и других странах СНГ фактически нет [11]. Именно поэтому невозможно точно

DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chişinău, Moldova

сказать, сколько людей с аутизмом проживает в Республике Молдова. По данным Минздрава [10], в 2012 г. аутизм был диагностирован примерно у 157 человек, из них –144 детей; в 2013 году – 220 человек, 191 ребенок, в 2016 году – под медицинским наблюдением находились 366 человек с диагнозом аутизм, из них 349 детей; В 2019 году выявлено около 633 человек с расстройствами аутистического спектра, из них 603 - дети. И данное число постоянно увеличивается, на данный момент считается, что людей с аутизмом более 1000 (Рисунок 4).

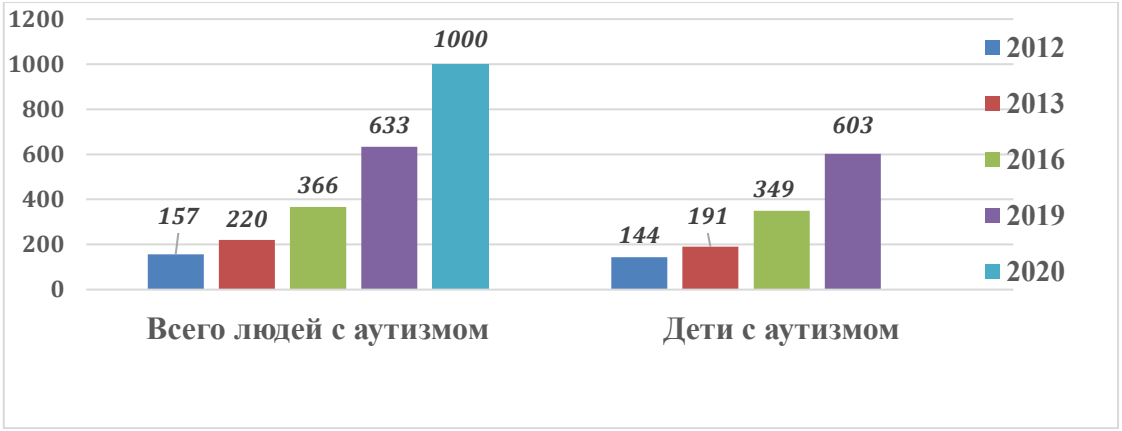


Рисунок 4. Количество людей с аутизмом в Республике Молдова за 2012-2020 гг.
Источник: [10], Draghici, E. pp. 58-60.

Эта тенденция внушает большие опасения, связанные с полностью неизученной природой аутизма, невозможностью профилактики, проблемами его коррекции, неоднозначным воздействием лекарств и другими факторами. В мире, где число людей с аутизмом, у которых возникают сложные проблемы с социализацией и общением, увеличивается с каждым годом, темпы социального развития снижаются, и в будущем это может стимулировать негативные социальные явления, которые трудно предсказать [9].

Можно отметить неоспоримую истину, что важнейшими факторами развития мозга являются движение и физическое благополучие. Многочисленные исследования показывают, что развитие двигательных навыков тесно связано с развитием речи, психических процессов, социальных и эмоциональных навыков, позволяющих личности адаптироваться к окружающему миру. В данном контексте можно отметить, что тренировка двигательных навыков логично включена в воспитание обычного ребенка, у которого прямо или косвенно, через общение с близкими людьми, в том числе посредством двигательной деятельности, игр, строится собственное представление о том, как он сам устроен, начинает понимать, почему ему приходится самому собирать игрушки, четко выражать свои пожелания, здороваться с другими людьми и многое другое.

Методологический модуль педагогической системы составляют современные концепции теории и методики физической культуры и спорта. В качестве результата реализации педагогической системы в образовательных учреждениях выступают две цели: гармонизация моторного потенциала детей и повышение профессионального мастерства педагога [12]. Поэтому, потребность развития системы инклюзивного образования в области физической культуры и спорта – учащихся общеобразовательных школ и специальных учебных заведений несет в себе достаточно актуальную проблему. Тому свидетельствует Положение об организации и деятельности спортивных школ,

DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chişinău, Moldova

утвержденное в 2019 Постановлением Правительства Республики Молдова № 31, п.22 предусматривающая регистрацию людей с особыми потребностями в спортивные секции [13].

Для оценки состояние данной проблемы мы обратились к мнению респондентов, специалистов различных областей. В опросе приняли участие 113 респондентов. Нас заинтересовало, на сколько, данная проблема известна респондентам в особенности специалистам по физическому воспитанию и спорта (Рисунок 5). Анализ результатов опроса показал, что уровень знаний об аутизме является средним.

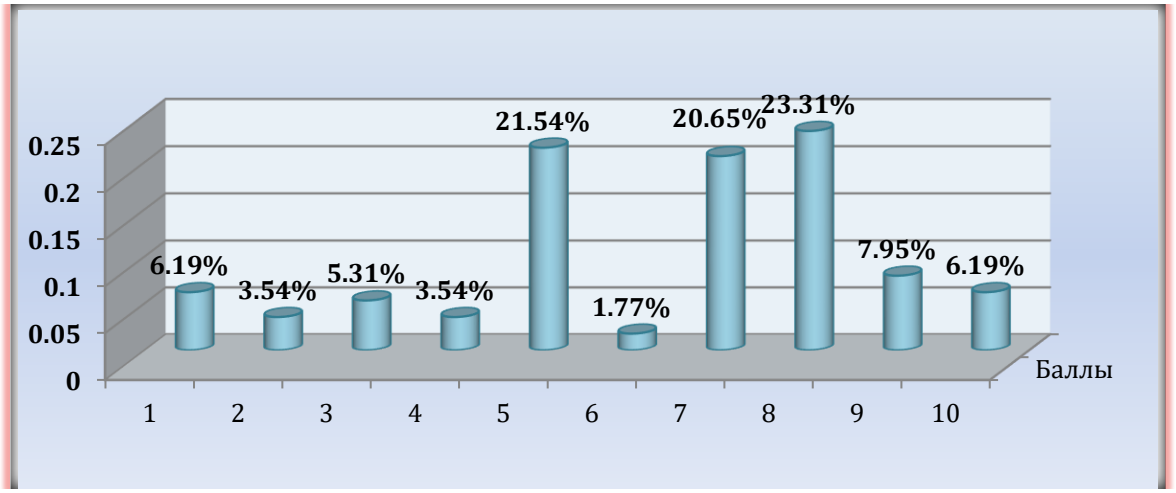


Рисунок 5. Насколько известна проблема аутизма среди специалистов из различных областей

Источник: [13] Polevaia-Secareanu, A., pp. 183-192.

По многочисленным исследованиям в целом у детей с аутизмом плохая моторика. Следовательно, адаптационные терапевтические программы должны быть сосредоточены на формирование основных двигательных навыков, моделей движений, а также на двигательной активности, повышающих физическую компетентность, в обычной жизни используя при этом различные виды спорта [8].

Данное положение позволило нам продолжить социологический опрос, выяснить и провести исчерпывающий анализ мнений респондентов по приоритетному использованию спортивной деятельности в психосоциальную адаптацию лиц с особыми потребностями. На рисунке 6, наглядно можно видеть, что на первое место респонденты отобрали плавание "плавание" - 46,02%, на второе место выставили игры - 40,78%, на третье место отобрались "Гимнастика" и „Единоборства". Не остались без внимания такие виды спорта как, „Конный спорт”- 21,24%,, Легкая атлетика” - 17,70%, „Настольный теннис”- 0,88% и другие.

По результатам данного опроса можно, отметить, то, что респонденты достаточно осознано, относятся к физическому развитию детей с особыми потребностями.

DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chişinău, Moldova

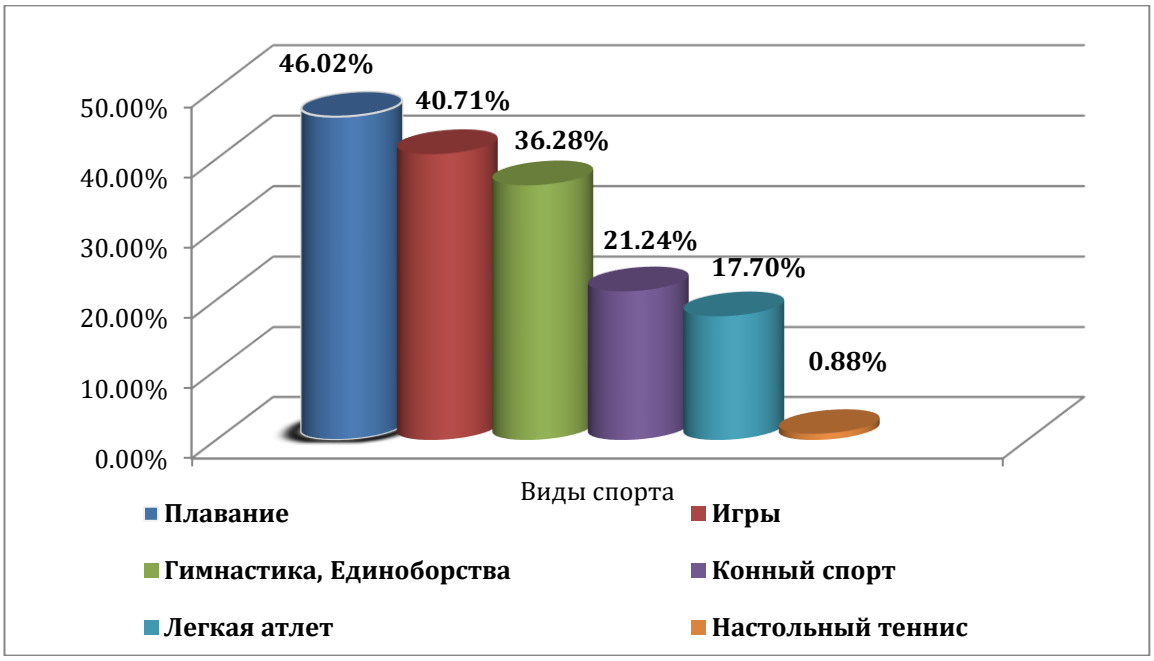


Рисунок 6. Какие виды спорта можно использовать для развития и психосоциальную адаптацию лиц с особыми потребностями

Источник: [13], pp. 183-192.

Поэтому следующий заданный вопрос, отражал понимание состояния готовности педагогических кадров в области физического воспитания и спорта работать с такой категорией детей. Мнения респондентов распределились следующим образом. 70% респондентов ответили “НЕТ”, 26% респондентов отметили “Можно попробовать” и всего лишь 4% отметили “ДА”. Задается вопрос, в чем проблема отказа специалистов по физическому воспитанию и спорта работать с детьми с особыми потребностями. Выявлено, что первая причина это “Нет опыта”, вторая причина это “Нет методических пособий”.

ВЫВОДЫ

Проведенное исследование позволяет утверждать, что один из основных принципов обеспечения безопасности государства является соблюдение баланса жизненно важных интересов личности потребности общества. Образование и обучение могут способствовать экономическому росту и созданию рабочих мест только в том случае, если обучение сосредоточено на знаниях, навыках и компетенциях, которые необходимо приобрести в процессе обучения, включающие образовательный научно-методический ресурс для формирования и выявления человеческого потенциала.

Поэтому стратегия развития научно-методологического обеспечение качества процесса психосоциальной адаптации людей с особыми потребностями, его соответствия современным требованиям, позволит повысить эффективность социально-экономической системы, отражающую основные пропорции развития и функционирования таких структур как: финансовой, инвестиционной, экономической, социальной и демографической.

DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chişinău, Moldova

БИБЛИОГРАФИЯ

1. ДЕМЧЕНКО, С.А. МЕЛНИКОВ Т.А. Социально-экономическая система страны и проблемы ее эффективности. *Проблемы современной экономики.* 2013, с. 136-139
2. ГАРТВИГ, К.Е. Реализация государственной политики в области развития человеческого потенциала. *Вестник ХГУ им. Н..Ф. Катанова,* [online]. Экономические науки, Institute. 2022. [viewed 3 November 2023] Available from: <https://cyberleninka.ru/article/n/realizatsiya-gosudarstvennoy-politiki-v-oblasti-razvitiya-chelovecheskogo-potentsiala
3. БУШКОВА, А.Ю. Деструктивные факторы, влияющие на демографический потенциал России: пути противодействия [online]. *Гуманитарный вестник.* 4.·2018 [viewed 10 November 2023] Available from: <https://cyberleninka.ru/article/n/destruktivnye-faktory-vliyayuschie-na-demograficheskiy-potentsial-rossii-puti-protivodeystviya/viewer>
4. БОРИСОВ, В.А. *Демография.* Москва, NotaBene, 2001. 272 с.
5. КАУФМАН, Н.Ю. Генезис конфликтов развития рынка труда в условиях цифровой экономики. *Вестник университета* № 5, 2019, с.16-22.
6. *HOTĂRÂRE Nr.* 768 din 12-10-2011cu privire la aprobarea Programului naţional strategic în domeniul securităţii demografice a Republicii Moldova (2011-2025) [online] Avalabel from: < https://www.legis.md/cautare/getResults?doc_id=131216&lang=ru#
7. *PERSOANELE CU DIZABILITĂȚI în Republica Moldova în anul 2022* [online] Institute. [viewed 28 November .2023] Available from: <https://statistica.gov.md/ru/print/polozenie-lic-s-ogranicennymi-vozmoznostyami-v-respublike-moldova-v-2022-godu--9460_60822.html >
8. *Diagnostic and Statistical Manual of Mental Disorders.* [online] Fifth Edition. *American Psychiatric Association.* 2013. [viewed 02 September 2023] Available from: <https://www.psychiatry.org/psychiatrists/practice/dsm >
9. BĂNĂRESCU, M., DRAGHICI, E. *Incluziunea socială a copiilor cu tulburări din spectru autist în Republica Moldova*.[online] Raportul tematic prezentat de avocat al poporului pentru protecția drepturilor copilului. Chișinău, 2016. 24 c. [viewed 02 September 2023] Available from: http://ombudsman.md/wp-content/uploads/2018/10/raport_tematic_autismul_0.pdf
10. DRAGHICI, E. *Incluziunea socială a copiilor cu tulburări din spectrul autist în Republica Moldova*. [online] Raport tematic Chișinău, 2016. pp. 58-60. [viewed 03 October 2023] Available from: <http://ombudsman.md/wp-content/uploads/2018/10/raport_tematic_autismul_0.pdf>
11. *SCRISOAREA* Ministerului Sănătății nr.01-9/1308 din 21.07.2016
12. МУХИНА, М. П. *О преемственности физического воспитания детей дошкольного и младшего школьного возраста в условиях применения педагогической технологии.* Ученые записки университета им. П. Ф. Лесгафта. № 7 (41). 2008, pp. 61-65.
13. *HOTĂRÂRE Nr. 31din 30-01-2019* cu privire la aprobarea Regulamentului de organizare şi funcţionare a școlilor sportive [online] [viewed 20 May .2023] Available from: <https://www.legis.md/cautare/getResults?doc_id=137431&lang=ro

DOI: https://doi.org/10.53486/escst2023.30
International Conference, December 07-08, 2023, Chișinău, Moldova

14. POLEVAIA-SECAREANU**,** A. The use of martial arts means in the development and socialization of children with autistic spectrum disorder. *Bulletin of the Transilvania* University of Braşov Series IX: Sciences of Human Kinetics • Vol. 16(65) No. 2 2023, pp.183-192.
15. ABRAMIHIN, C. *Dezvoltarea competențelor pentru secolul XXI prin sisteme de învățământ pe tot parcursul vieții* [online] international scientific-practical conference 2nd ed., December 17, Chișinău, Academy of Economic Studies of Moldova. 2021 .ISBN 978-9975-155-73-1
16. GAGAUZ, O. Provocări demografice şi politici necesare. Tendinţe în Economia Moldovei. 2013, nr. 12(trim. 4), pp. 106-114. ISSN 1857-3126.
17. ДАДАШЕВ, А.М. Оценка качества жизни населения российской федерации на основе критериев экономической безопасности. *Здоровье - основа человеческого потенциала: проблемы и пути их решения*. 2020, 1373-1384.

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chișinău, Moldova

The collection of articles is the result of the International Scientific Conference "Economic Security in the Context of Systemic Transformations", organized on **December 7-8, 2023** at the **Academy of Economic Studies of Moldova** and simultaneously online via the Zoom platform.
https://ase.md/econsec

Conference organizer:

Department "Economic Theory and Policy", Academy of Economic Studies of Moldova
https://tpe.ase.md

Co-organizers:

Stefan cel Mare University of Suceava (USV, Suceava, Romania)
http://www.usv.ro

D.A. Tsenov Academy of Economics, (Svishtov, Bulgaria)
http://www.uni-svishtov.bg

Bucharest University of Economic Studies (Bucharest, Romania)
http://www.ase.ro

Valahia University of Târgoviște (Bucharest, Romania)
https://www.valahia.ro

Armenian State University of Economics (Yerevan, Armenia)
https://asue.am

V.I. Vernadsky Taurida National University (Kiev, Ukraine)
https://tnu.edu.ua

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chișinău, Moldova

Conference International Scientific Committee:

Moldova

Stratan Alexandru, Coressponding member of AȘM, PhD Habilitat, Professor, Rector of the Academy of Economic Studies of Moldova, ORCID 0000-0001-7086-8604

Belostecinic Grigore, Academician, PhD Habilitat, Professor, Academy of Economic Studies of Moldova , ORCID 0000-0002-6913-2437

Cociug Victoria, PhD, Associate Professor, Vice-Rector for Research and Partnerships, Academy of Economic Studies of Moldova , ORCID 0000-0001-8114-4644

Ignatiuc Diana, PhD, Associate Professor, Head of the Economic Theory and Policy Department, Academy of Economic Studies of Moldova , ORCID 0000-0002-8229-8941

Barbăneagră Oxana, PhD, Associate Professor, Economic Theory and Policy Department, Academy of Economic Studies of Moldova, ORCID 0009-0008-2567-0170

Bucos Tatiana, PhD, Associate Professor, Economic Theory and Policy Department, Academy of Economic Studies of Moldova**,** ORCID 0000-0001-6448-6001

Ohrimenco Serghei, PhD habilitat, Professor, Laboratory of Information Security, Academy of Economic Studies of Moldova, ORCID 0000-0002-6734-4321

Tomșa Aurelia, PhD, Associate Professor, Economic Theory and Policy Department, Academy of Economic Studies of Moldova, ORCID 0000-0002-5272-0208

Bejan Ghenadie, PhD, Associate Professor, Economic Theory and Policy Department, Academy of Economic Studies of Moldova, ORCID 0000-0003-3741-1949

Coban Marina, PhD, Associate Professor, Economic Theory and Policy Department, Academy of Economic Studies of Moldova, ORCID 0009-0005-1984-9682

Munteanu Corneliu, PhD, Economic Theory and Policy Department, Academy of Economic Studies of Moldova

Crudu Rodica, PhD, Associate Professor, International Business Department, Academy of Economic Studies of Moldova , ORCID 0000-0002-6470-8601

Șavga Larisa, PhD Habilitat, Professor, Rector of Trade Co-operative University of Moldova , ORCID 0000-0002-9691-7475

Prițcan Valentina, PhD, Associate Professor, Vice-Rector for Research and International relationship, Balti State University ,,Alecu Russo, ORCID 0000-0003-0743-8577

Romania

Prelipcean Gabriela, PhD, Professor, Vice-Rector, Ștefan cel Mare University of Suceava, ORCID 0000-0002-2584-1733

Carmen Nastase, PhD, Professor, Dean of the Faculty of Economics, Administration and Business, Ștefan cel Mare University of Suceava, ORCID 0000-0002-1660-2087

Lupan Mariana, PhD, Associate Professor, Vice Dean, Faculty of Economics, Administration and Business, Ștefan cel Mare University in Suceava, ORCID 0000-0002-2256-8276

Albu Angela, PhD, Associate Professor, Department Director, Faculty of Economics, Administration and Business, Ștefan cel Mare University of Suceava, ORCID 0000-0002-6580-8209

Piroșcă Grigore Ioan, PhD, Associate Professor, Dean of the Faculty of Theoretical and Applied Economics, Bucharest University of Economic Studies, ORCID 0000-0001-8148-4163

Duica Mircea-Constantin, PhD, Valahia University of Targoviste, ORCID 0000-0002-5106-638X

Croitoru Gabriel, PhD, Valahia University of Targoviste, ORCID 0000-0002-8327-3455

DOI: https://doi.org/10.53486/escst2023
International Conference, December 07-08, 2023, Chișinău, Moldova

Bulgaria

Velev Dimiter, PhD, Professor, Department of Computer Science, University of National and World Economy, Sofia, ORCID 0000-0003-3030-1819

Krasimir Shishmanov, PhD, Professor, Department of Business Informatics of the D. A. Tsenov Academy of Economics, Svishtov, ORCID 0000-0001-9874-2149

Ukraine

Hornyk Volodymyr, PhD, University Professor, V.I. Vernadsky Taurida National University, ORCID 0000-0002-9723-3956

Hrosul Victoria, PhD, Professor, Head of the Department Economics and Business State Biotechnological University, Kharkiv, ORCID 0000-0002-2019-3853

Portnaia Oksana, PhD, Professor, V. N. Karazin Kharkiv National University, Kharkiv

Rybalchenko Lyudmyla, PhD, Associate Professor Department of Economic and Information Security Dnipropetrovsk State University of Internal Affairs, Dnipropetrovsk, ORCID 0000-0003-0413-8296

Armenia

Mkrtchyan Tatul, PhD, Vice-Rector for Science, Armenian State University of Economy, ORCID 0000-0003-2057-8590

Gevorgyan Nerses, PhD, Armenian State University of Economy

Belarus

Lebedeva Svetlana, PhD, Professor, Rector, Belarusian Trade and Economic University of Consumer Cooperatives, Gomel, ORCID 0000-0003-1546-3238

Latvia

Kreituss Ilmars, PhD, Professor, RISEBA University, ORCID 0000-0001-8510-376X

Turkey

Özen Ercan, PhD, Associate Professor, School of Applied Sciences, University of Uşak, Department of Banking and Finance, ORCID 0000-0002-7774-5153

Tufan Ekrem, PhD, Professor, Canakkale Onsekiz Mart University, Faculty of Applied Sciences, ORCID 0000-0002-1966-0709

Approved for publication: 23.02.2024

Editorial and Publishing Service of the Academy of Economic Studies of Moldova
Chișinău, MD-2005, 59 Bănulescu-Bodoni Street, Phone: +373 22 402 910