DOI: https://doi.org/10.53486/sstc2026.v1.111

CZU: 004.056:339.92(478+4EU)

INFORMATION SECURITY IN THE REPUBLIC OF MOLDOVA IN THE CONTEXT OF EUROPEAN INTEGRATION: CYBER CHALLENGES AND PROSPECTS IN THE ERA OF ARTIFICIAL INTELLIGENCE

SECURITATEA INFORMAȚIONALĂ A REPUBLICII MOLDOVA ÎN CONTEXTUL INTEGRĂRII EUROPENE: PROVOCĂRI CIBERNETICE ȘI PERSPECTIVE ÎN ERA INTELIGENȚEI ARTIFICIALE

COJOCARI Vladislav, student, specialitatea: TISE
Academia de Studii Economice din Moldova,
str. Banulescu-Bodoni 61, Republica Moldova, Chișinău
Email autor: vlad.le1120@ase.md

Abstract: *In the last couple of years Republic of Moldova has prioritized EU integration, requiring improved information security against cyber and hybrid threats. In June 2024 Moldova became an EU candidate country, necessitating alignment with EU cybersecurity standards. This paper describes the main cybersecurity challenges Moldova will face and the role of AI in improving information security. The findings show that Moldova must develop capabilities to address deepfakes and automated disinformation, and establish strong mechanisms for early detection and prevention of cyber incidents. Artificial intelligence presents significant opportunities to enhance these protective measures. The paper concludes that Moldova requires a comprehensive approach encompassing technological advancement, legislative modernization, institutional capacity building, and international cooperation.*
Key words: *information security, cybersecurity, Republic of Moldova, European integration, artificial intelligence.*
JEL CLASSIFICATION: O33, K24, H56

INTRODUCERE:În secolul 21 securitatea informațională reprezintă un factor important al securității naționale. Pentru Republica Moldova această temă este deosebit de importantă, deoarece este stat candidat la UE – statut obținut în iunie 2022 – iar negocierile de aderare au fost deschise oficial la 25 iunie 2024. Securitatea informațională nu presupune doar reforme politice, ci și consolidarea cadrului normativ și instituțional în domeniul securității cibernetice. Creșterea frecvenței atacurilor cibernetice și hibride (atacuri informatice, manipulare informațională, dezinformare) și dezvoltarea inteligenței artificiale amplifică atât riscurile (deepfake-uri, phishing automatizat), cât și oportunitățile de prevenire. Scopul lucrării constă în analiza securității informaționale a Republicii Moldova în contextul integrării europene, identificând principalele riscuri și direcțiile de consolidare conform standardelor europene.

CONȚINUTUL DE BAZĂ:

Analiza bibliografiei

Literatura de specialitate și documentele oficiale arată că integrarea europeană a Republicii Moldova este strâns legată de adaptarea cibernetică. Deschiderea negocierilor de aderare la 25 iunie 2024 confirmă că alinierea la standardele UE privind securitatea cibernetică și guvernanța digitală este esențială. Consiliul UE, EEAS, ENISA și Comisia Europeană furnizează contextul politic și analitic al lucrării, demonstrând că securitatea informațională nu este doar o problemă tehnică, ci una de securitate strategică și stabilitate democratică. Legea nr. 48/2023 privind securitatea cibernetică a Republicii Moldova, elaborată cu sprijinul UE și intrată în vigoare la 1 ianuarie 2025, reprezintă baza normativă pentru analiză. Principalele surse sunt sintetizate în Tabelul 1.

Tabelul 1. Principalele surse utilizate în cercetare și relevanța lor

Sursa	**Tipul sursei**	**Ideea principală**	**Relevanța pentru cercetare**
Consiliul UE	document oficial	Negocierile de aderare deschise la 25 iunie 2024	Contextul integrării europene
EEAS / Delegația UE	document instituțional	Legea cibernetică susținută de UE, vigoare 1 ian. 2025	Legătura reformă națională – sprijin european
Comisia Europeană	document oficial	AI Act intrat în vigoare la 1 august 2024	Baza pentru analiza dimensiunii AI
ENISA	raport de specialitate	Amenințări: phishing, deepfake-uri, manipulare	Susține analiza provocărilor cyber
Gov.md / doc. strategice	document strategic	Capacități operaționale și cooperare cyber	Sprijină perspectivele de dezvoltare

Sursa: elaborat de autor în baza Consiliului Uniunii Europene (2024), Serviciului European de Acțiune Externă (2023) și Comisiei Europene (2024).

Descrierea metodelor de cercetare utilizate:

Analiza documentară – metoda principală, aplicată actelor normative, strategiilor și materialelor oficiale naționale și europene, pentru identificarea direcțiilor de reformă și vulnerabilităților existente;

Analiza comparativă – confruntarea abordărilor naționale cu cerințele UE, evidențiind gradul de armonizare și diferențele legislative;

Sinteza – combinarea informațiilor despre amenințările cibernetice, riscurile hibride, integrarea europeană și impactul AI pentru o imagine de ansamblu;

Metoda descriptivă – caracterizarea fenomenelor precum securitatea informațională, atacurile cibernetice, dezinformarea și deepfake-urile;

Metoda deductivă – pornind de la cadrul european general pentru a formula concluzii specifice Republicii Moldova. Combinarea acestor metode a permis o analiză atât teoretică cât și practică, evidențiind provocările cibernetice principale și influența AI asupra securității informaționale.

Rezultatele obținute:

Contextul european și instituțional: Securitatea informațională a Republicii Moldova trebuie analizată din perspectiva integrării europene. Obținerea statutului de candidat la UE și deschiderea negocierilor de aderare au creat un cadru politic unde securitatea cibernetică a devenit o componentă crucială a modernizării statului conform standardelor europene.

Principalele provocări cibernetice și hibride: Pe lângă riscurile cibernetice clasice, Republica Moldova se confruntă cu atacuri hibride – manipulare informațională și presiuni politice – care subminează integritatea statului și procesele democratice. Principalele provocări vizibile sunt dezinformarea și protecția infrastructurii digitale a instituțiilor publice și private. Mecanismele de prevenire și raportare a atacurilor cibernetice au devenit esențiale.

Riscurile emergente ale AI: Dezvoltarea rapidă a inteligenței artificiale a schimbat peisajul securității informaționale, generând riscuri noi, mai greu de identificat și controlat (deepfake-uri, phishing automatizat, campanii de dezinformare automatizate). AI trebuie privită atât ca risc cât și ca instrument de apărare.

Inteligența artificială și adaptabilitatea cibernetică: AI poate sprijini instituțiile în detectarea mai rapidă a amenințărilor, analiza volumelor mari de date și automatizarea răspunsului la incidente cibernetice, contribuind la clasificarea alertelor și prioritizarea riscurilor. Riscurile și oportunitățile utilizării AI sunt sintetizate în Tabelul 2.

Tabelul 2. Riscurile și oportunitățile utilizării inteligenței artificiale în domeniul securității informaționale

Riscuri generate de AI	Oportunități oferite de AI
Deepfake-uri și falsificarea conținutului	Detectarea mai rapidă a anomaliilor
Phishing automatizat	Analiza volumelor mari de date
Amplificarea dezinformării	Identificarea timpurie a amenințărilor
Atacuri cibernetice mai sofisticate	Automatizarea răspunsului la incidente
Imitarea stilului de comunicare al persoanelor reale	Sprijin pentru monitorizare și evaluare a riscurilor
Utilizarea AI în campanii de influență online	Îmbunătățirea conștientizării situaționale

Sursa: elaborat de autor în baza Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA) (f.a.), accesat la 29 martie 2026.

CONCLUZII:

Securitatea informațională a Republicii Moldova a devenit un domeniu esențial, în special în contextul integrării europene și al intensificării amenințărilor hibride concomitent cu dezvoltarea rapidă a inteligenței artificiale. Pentru a adera la UE, Moldova trebuie să implementeze reforme politice și juridice noi și să îmbunătățească protecția infrastructurii digitale. Cercetarea a arătat că Republica Moldova se confruntă cu atacuri cibernetice, dezinformare, manipulare informațională și presiuni hibride care afectează integritatea statului și încrederea populației. Inteligența artificială este simultan un pericol și un instrument eficient împotriva atacurilor cibernetice, impunând o abordare echilibrată și responsabilă.

RECOMANDĂRI:

1) Dezvoltarea structurilor competente pentru consolidarea capacităților instituționale;
2) Continuarea armonizării legislative cu standardele Uniunii Europene;
3) Utilizarea responsabilă a inteligenței artificiale în instituțiile publice;
4) Dezvoltarea mecanismelor de prevenire și răspuns la dezinformare și manipulare informațională;
5) Creșterea nivelului de educație digitală și a culturii de securitate cibernetică.

REFERINȚE:

1. Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA). (f.a.). *Threat landscape*. https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape (accesat la 15 aprilie 2026)
2. Banca Mondială. (f.a.). *Individuals using the Internet (% of population) – Moldova*. https://data.worldbank.org/indicator (accesat la 28 martie 2026)
3. Comisia Europeană. (2024, 1 august). *AI Act enters into force*. https://commission.europa.eu/news-and-media/news/ai-act-enters-force-2024-08-01_en
4. Consiliul Uniunii Europene. (2024, 25 iunie). *EU opens accession negotiations with Moldova*. https://www.consilium.europa.eu/en/press/press-releases/2024/06/25/eu-opens-accession-negotiations-with-moldova/
5. Serviciul European de Acțiune Externă. (2023, 11 mai). *Moldova adopted the EU-backed cybersecurity law*. https://www.eeas.europa.eu/delegations/moldova/moldova-adopted-eu-backed-cybersecurity-law_en
6. Serviciul European de Acțiune Externă. (2025, 22 mai). *EUPM Moldova: Moving forward towards sustainable security resilience in Moldova*. https://www.eeas.europa.eu/eupm-moldova/eupm-moldova-moving-forward-towards-sustainable-security-resilience-moldova_en

Coordonator științific: ȚURCAN Aurelia, dr.,conf.univ.
Academia de Studii Economice din Republica Moldova,
Chișinău, str. Bănulescu-Bodoni 61
e-mail: turcan.aurelia.4u8h@ase.md