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]

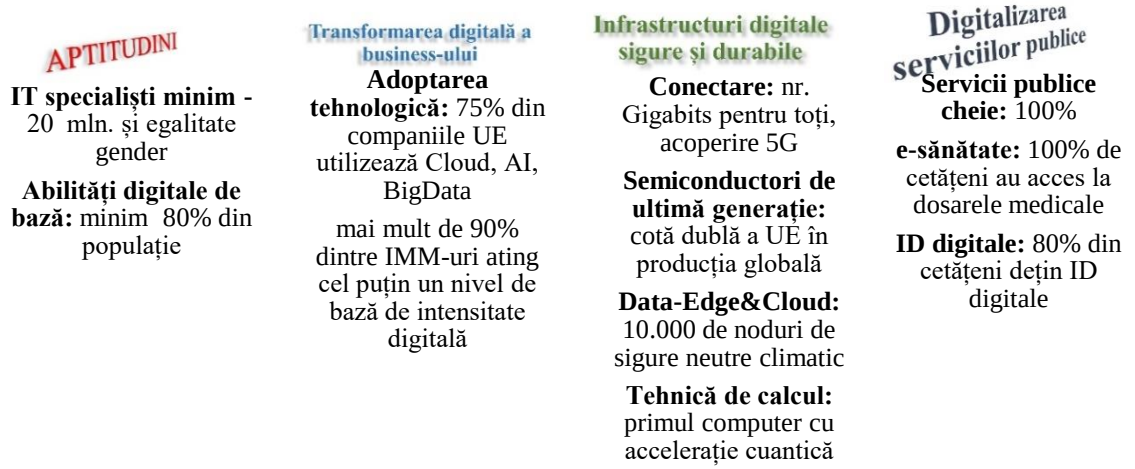

Figura 1. Țintele propuse de „Deceniul Digital"

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>