Academia de Studii Economice din Moldova

THE COLLECTION

of the Online International Scientific-Practical Conference

"Economic security in the context of sustenable development"

Chișinău, 2021

THE COLLECTION

of the Online International Scientific-Practical Conference,
December 11, 2020, ASEM, Chișinău, Moldova:

”ECONOMIC SECURITY IN THE CONTEXT OF SUSTENABLE DEVELOPMENT”

Chișinău, 2021

CZU : 33(082)=135.1=111=161.1
E 15

Collection of scientific articles presented at the Online International Scientific-Practical Conference "Economic Security in the Context of Sustainable Development" (December 11, 2020)

Descrierea CIP a Camerei Naţionale a Cărţii

"Economic security in the context of sustenable development", online international scientific-practical conference (2020 ; Chişinău). The Collection of the Online International Scientific-Practical Conference "Economic security in the context of sustenable development", December 11, 2020, ASEM, Chișinău, Moldova / scientific committee: Tomșa Aurelia [et al.] ; drafting committee: Tomșa Aurelia [et al.]. – Chișinău: ASEM, 2021. – 341 p. : fig., tab.

Cerinţe de sistem : PDF Reader.

Antetit.: Acad. de Studii Econ. din Moldova. – Texte : lb. rom., engl., rusă. – Rez.: lb. rom., engl. – Referinţe bibliogr. la sfârşitul art.

ISBN 978-9975-155-01-4

**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.*

Contents:

National Economic Security

Economic Security at the Individual Level

Information Security

National Economic Security

THEORETICAL AND PRACTICAL ASPECTS OF ENERGY SECURITY OF THE ROMANIAN ECONOMY IN THE CONTEXT OF SUSTAINABLE DEVELOPMENT

ASPECTE TEORETICE ȘI PRACTICE ALE SECURITĂȚII ENERGETICE A ECONOMIEI ROMÂNIEI ÎN CONTEXTUL UNEI DEZVOLTĂRI DURABILE

Gribincea Alexandru
Doctor habilitat în economie, profesor universitar
Universitatea Liberă Internațională din Moldova
e-mail: agribincea@mail.ru

Popescu Maria
Doctorandă, Universitatea Liberă Internațională din Moldova
e-mail: blondin42003@yahoo.com

Abstract
The energy policy of the E.U. has constantly adapted to the macroeconomic and geo-strategic realities of the member states policies, in order to provide and ensure security of energy supply, constancy, sustainability and also to guarantee affordable and competitive prices for all the consumers,where as a major beneficiary of energy, still has a vulnerable and unstable position on the global market. The challenges of climate change, supporting development in energy efficiency as a contribution to tempering energy transfer demands, reducing gas emissions, all lead to the development of research, innovation and increasing competitiveness. Energy security is, along with competitiveness and sustainable development, one of the pillars of the energy strategy. Romania must start from a rigorous analysis of what it has, to propose a strategy by 2030, which will correlate national investments with European and global ones, to find the right model in terms of market configuration and internal energy system, to benefit from the development of the interconnection of the gas-energy networks north-south and to build an energy community, which will support the national energy regulators and operators and of transmission systems.

Keywords: *energy, energy security, alternative sources, hydrocarbon imports, energy policy*

JEL Classification: *F5, K32, L71, Q43*

INTRODUCERE

În contextul permanentelor transformări economice care se desfășoară la nivel global, noua strategie de securitate europeană este solicitată să se modifice permanent faţă de principalele riscuri globale, să identifice apariţia unor ameninţări ori vulnerabilităţi, pentru a pune la dispoziţia actorilor din sistemul energetic soluţii detaliate pentru orice situaţie. Vulnerabilităţi ca încălzirea globală, dependenţa energetică, crizele economice europene și mondiale și, mai nou, medicale, dar și alte elemente identificate ca pericole, precum sărăcia, foametea, corupţia, eşecul creșterii economice, pot deveni ameninţări reale. Creșterea substanțială a economiei statelor mai puţin dezvoltate și recenta criză financiară provocata de criza medicală, au destabilizat statele puternic industrializate și pe cele unde ritmul creșterii economice este mai scăzut. Varietatea furnizorilor de resurse angrenați într-o aprovizionare flexibilă, adaptarea infrastructurilor la cerințele actuale, încheierea procesului de realizare a unei piețe integrate și dinamice, reducerea modalităţilor dependenţei energetice, evaluarea progreselor, reducerea cheltuielilor în

cadrul sistemului energetic și combaterea încălzirii globale, sunt printre principalele obiective ale UE. Constituirea uniunii energetice va duce la creștere economică și la modernizarea sistemului energetic european. Securitatea energetică constituie, alături de competitivitate și dezvoltare durabilă, unul dintre pilonii strategiei energetice. România trebuie să pornească de la o analiză riguroasă a situației actuale, să propună o strategie nouă până în anul 2030, care să coreleze investițiile naționale cu cele europene și mondiale, să găsească modelul potrivit privind configurarea pieței și a sistemului energetic intern, să beneficieze de dezvoltarea interconectării rețelelor de gaz și energie nord-sud și să construiască o comunitate energetică care să susțină reglementatorii și operatorii naționali de energie și ai sistemelor de transport.

Gradul de investigare. Printre cercetătorii străini ai cooperării internaționale pe probleme de analiza securității energetice, trebuie remarcate lucrări care prezintă o gamă largă de abordări în studiul securității energetice. Această diversitate contribuie la o înțelegere cuprinzătoare a securității energetice. De exemplu, lucrările lui D. Yergin ne permit să studiem SEG în contextul istoriei rolului sistemelor energetice în cadrul relațiilor externe. E. Downs, care are experiență în cercetarea structurilor analitice ale experților legate de organele guvernamentale, explorează caracteristicile formării politicii de stat dependentei energetice, cu precădere China. M. Clar examinează locul problemelor globale de securitate energetică, analizând potențialul de criză al dezacordurilor, în general, pentru alte domenii ale relațiilor internaționale. Între toate aceste curente de gândire se remarcă Școala de la Copenhaga, ai cărei reprezentanți – Barry Buzan, Ole Waever și Jaap de Wilde – sunt „adepții distincției în funcție de nivelul de coeziune socio-economică”și susțineau că „securitatea colectivităților umane este afectată de factori din cinci sectoare principale: militar, politic, economic, social și de mediu. Aceste dimensiuni „operează în interdependență, fiecare dintre ele fiind un punct central în ordonarea priorităților din cadrul problematicii securității” Criza din lumea financiară descoperă posibilități noi de acțiune în lumea energiei cu impact asupra țărilor și companiilor din sectorul energiei și modul în care criza le-ar putea forța pe acestea să se transforme, susțin Dr. Heiko Borchert și Karina Forster [1].

Obiectivul pachetului privind securitatea energetică din cadrul UE este de a asigura o eficiență energetică sporită la prețuri competitive, garantată și durabilă care sa conducă la temperarea cheltuielilor, scăderea emisiilor poluante, sprijinirii cercetării, inovării și creșterii competitivității, accelerarea dezvoltării tehnologiilor de rețele cu aplicații inteligente în urbanism, transporturi curate, combustibili alternativi și utilizarea în continuare a energiei nucleare.

Scopul cercetării constă în investigarea impactului amplificării proceselor de globalizare, tehnologizare și digitalizare asupra strategiei energetice, importanța și modalitatea de a utiliza cea mai bună metodă de studiere și tratare a viitoarei strategii energetice pentru România, în contextul în care energia a devenit un factor strategic în politica globală, o cheltuială costisitoare, o componentă vitală în creșterea economică și evoluția societății, în identificarea potențialului unor surse de energie de adaptare la provocările globalizării în condiții de vulnerabilitate și instabilitate economică mondială, consolidarea unor pachete de politici optime, care să asigure o energie la prețuri accesibile, sigură și durabilă, la adoptarea unor obiective referitoare la dezvoltarea surselor regenerabile; o eficiență energetică cu realizarea de economii, diminuarea efectului de seră; dezvoltarea infrastructurii energetice și finalizarea pieței interne de energie, implicarea mediului academic, a reprezentanților din economia reală și a instituțiilor publice pentru a scoate în evidență pericolele existente pentru securitatea energetică și a căilor de depășire a acestora.

CERCETARE ȘI ANALIZĂ

Dezvoltarea durabilă reprezintă îmbunătățirea standardului de viață**,** opțiunea concretă a cetățenilor de a face alegeri, crearea unui mediu propice de răspândire a cunoștințelor pentru o mai bună informare. Astfel, ar trebui să ajungem la o situație în care să avem „o viață bună, în interiorul planetei noastre"[2] prin utilizarea mai inteligentă și eficientă a resurselor, cu o economie modernă care să servească sănătății și bunăstării, tranziția către realizarea unui sistem decarbonizat în paralel cu asumarea de soluții eficiente la costuri competitive şi a trecerii la o creştere economică bazată pe investiții fără influenţe asupra climei, bogată în biodiversitate care să se conformeze pe deplin Agendei 2030 a ONU, cu respectarea țintelor stabilite pentru o dezvoltare durabilă. Această tranziție trebuie să aducă beneficii, fără discriminare, tuturor, asigurând egalitate și incluziune.

Importanţa problemei abordate este evidentă, întrucât analizează necesitatea şi oportunitatea implicării mai accentuate a rolului energiei în procesul asigurării securităţii, atât la nivel național, cât şi la nivelul UE. Este nevoie de o atentă cercetare, o evaluare a previziunilor şi performanţelor în domeniul securităţii energetice în cadrul UE pentru identificarea relaţiei energie-societate, care sunt factorii care determină necesitatea unei eventuale reconfigurări şi care este mecanismul de răspuns la provocările globalizării în condiţii de vulnerabilitate şi instabilitate economică mondială.

Politica energetică a UE are nevoie de o viziune integrată, bazată pe interacţiunea dintre decidenţi, obiective şi sectoare implicate, să regrupeze diferite obiective -surse regenerabile, emisii de carbon, consum de energie, eficienţă energetică, securitatea aprovizionării, preţ stabil, domenii ca securitate, economie, mediu, transport, social, politic şi actori (instituţii europene, ONG-uri, industrii, organizaţii umbrelă, actori politici locali, media europeană). Eficiența energetică trebuie să devină avangarda tehnologiilor pentru rețele și locuințe inteligente, a transporturilor curate, a combustibililor nepoluanți și a celei mai sigure producții de energie nucleară din lume.

După cum se susţine şi în proiectul noii Strategii de Securitate Naţională a României, "globalizarea reprezintă cauza esenţială în producerea unor pericole şi ameninţări necunoscute, cu influenţe asupra securităţii economice şi energetice actuale, apar oportunităţi şi riscuri noi, avantajează rivalitatea şi conlucrarea pentru putere, lupta pentru resurse, rute de transport şi pieţe de desfacere". Prin urmare, "securitatea energetică trebuie să ţină cont de vulnerabilităţile generate de influenţele produse de globalizare, orice disfuncţionalitate sau instabilitate dintr-o parte a sursei energetice afectând consumatorii din întreaga lume" [3]. Securitatea energetică este "strâns legată de vulnerabilitatea faţă de întreruperile în aprovizionarea cu resurse energetice, care se poate reflecta în distrugerea infrastructurii energetice, evenimente naturale, terorism sau război, instabilitatea politică şi economică datorată războiului sau altor factori, precum acţiunile greviste, poate duce de asemenea la sincope în industria energetică a unei ţări furnizoare. Una din ameninţările majore în domeniul securităţii energetice este reprezentată de creşterea preţului energiei pe piaţa mondială, impunerea unor creşteri a cheltuielilor de către furnizorii intermediari, ameninţarea din partea unor superputeri energetice capabile să influenţeze semnificativ piaţa mondială prin acţiunile lor, prin suspendarea sau anularea livrărilor" [3]. Securitatea aprovizionării cu energie, o utilizare eficientă a resurselor, îmbunătăţirea eficienţei energetice, preţuri accesibile şi soluţii inovatoare sunt cruciale pentru o creştere durabilă, care să conducă la diminuarea efectelor rezultate din vulnerabilitatea şi instabilitatea energiei [4].

Este analizată importanţa energiei, care a devenit un factor principal în politica mondială, o cheltuială importantă pentru dezvoltarea economică, primordială pentru progresul societăţii, reprezintă un element de bază în domeniul energetic naţional, fiecare

țară, inclusiv Romania, acționând astfel încât să fie îndeplinite țintele de politică energetică globală și durabilă, este o parte a strategiei de apărare, militează pentru păstrarea identității energetice naționale, obiectiv care corelează politica internă cu obligațiile care îi revin la nivelul UE. "Strategia energetică trebuie să fie cunoscută, pe înțelesul și la îndemâna tuturor, un îndrumar eficace și eficient pentru organele decizionale din domeniul public, privat, întreprinzători și abonați" [5].

Principiile Strategiei pun în plan central drepturile consumatorilor de energie, cu nevoi și interese diverse în permanentă evoluție, transparență și dialog de substanță cu părțile interesate, modernizarea sistemului de guvernanță energetică, în utilizarea mecanismelor unei piețe competitive cu urmărirea țelurilor asumate, o modelare cantitativă care oferă soluții referitoare la competitivitatea relativă a tehnologiilor și în care mixul acestora poate susține eficace realizarea obiectivelor strategice (fig.1). Securitatea energetică a României nu mai este posibil să fie definită printr-o singură variantă, ci prin mai multe soluții pe perioade diferite. În primul rând, analiza calitativă a evidențiat deschiderea și transparența activităților de redactare a strategiei, urmată de modelarea cantitativă a informațiilor din domeniul energetic românesc.

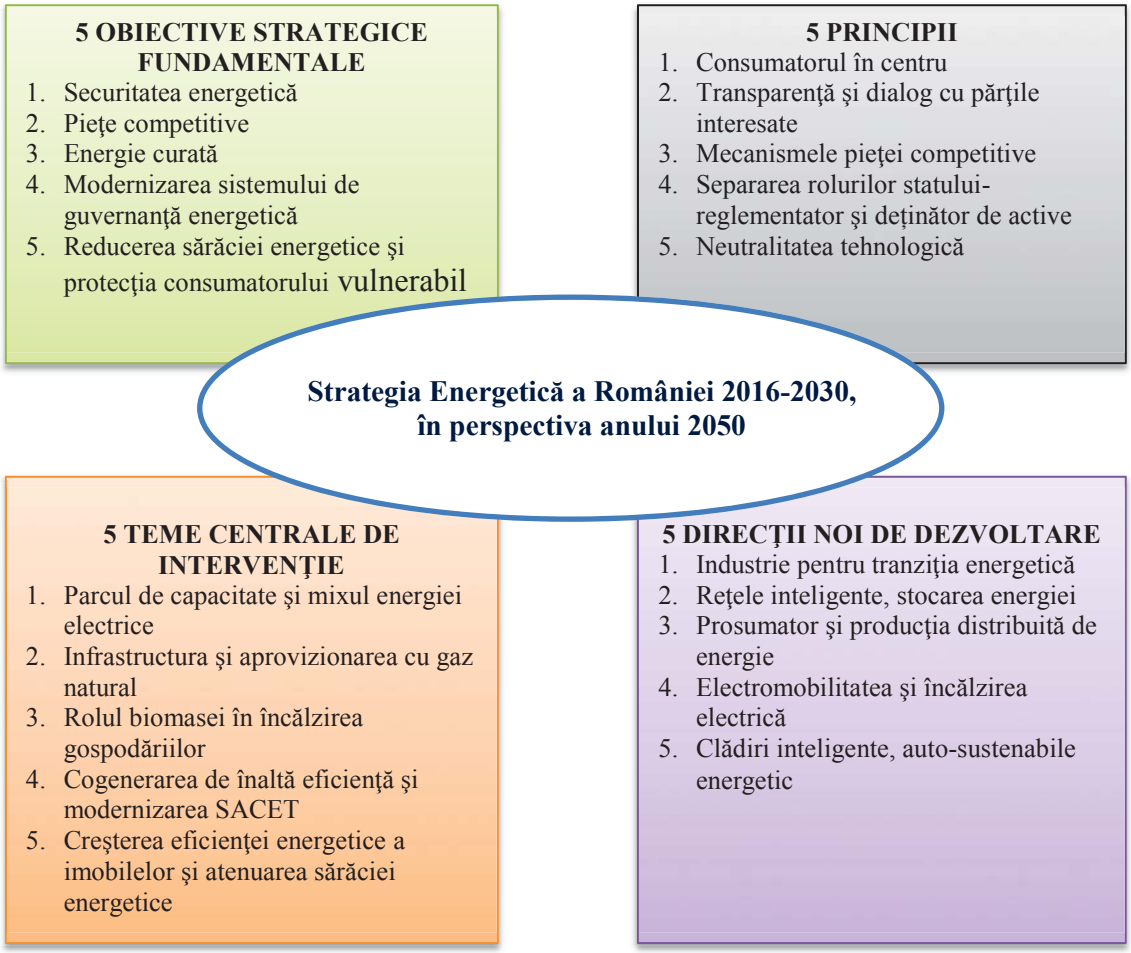


Figura 1. Elementele ce definesc Strategia Energetică a României 2016-2030, în perspectiva anului 2050

Sursa: elaborat de autor în baza [energie.gov.ro//Strategia-Energetica-a-Romaniei-2016-2030]

Strategia cuprinde cinci obiective strategice fundamentale: necesitățile de securitate energetică, de garantare a competitivității economiei, tranziția sectorului energetic către un sistem de evoluție sustenabil bazat pe o bună guvernanță a sectorului

energetic, asigurarea energiei pentru toți consumatorii, reducerea sărăciei energetice și protecția consumatorilor vulnerabili [6] (fig.2).

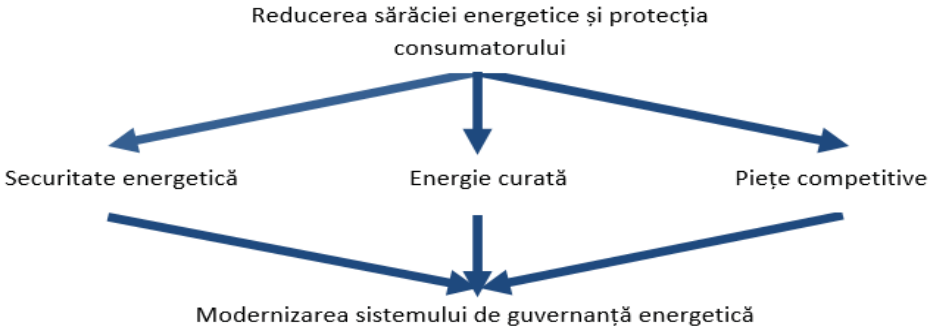


Figura 2. Cinci obiective strategice fundamentale. Strategia Energetică a României 2016-2030

Sursa: elaborat de autor în baza:[energie.gov.ro/.../Strategia-Energetica-a-Romaniei-2016-2030]

În cadrul Strategiei sunt menționate: ponderea combustibililor tradiționali în mixul energetic din viitor, hidroenergia care va rămâne o prioritate a sistemului energetic național urmată de importanța aparte a componentei nucleare și a energiei verzi; gazul natural extras care poate asigura cererea internă, producția de cărbune va fi limitată de costul *emisiilor* naţionale de gaze cu efect de seră; biomasa și cogenerarea de înaltă eficiență energetică a locuințelor își păstrează rolul central în încălzirea gospodăriilor din mediul rural. Sunt necesare investiții programate împreună cu înoirea și abordarea dintr-o altă perspectivă a sistemelor de alimentare centralizată cu agent termic (fig.3).

Figura 3. Cinci arii centrale de intervenție strategică. Strategia Energetică a României 2016-2030

Sursa: elaborat de autor în baza [energie.gov.ro/.../Strategia-Energetica-a-Romaniei-2016-2030]

Obiectivele strategice fundamentale sunt asumate cu ținte concrete, acțiuni și procese de funcționare precise, preluate ulterior de politicile din domeniu, în concordanță cu interesele părților participante și culminând cu transpunerea lor în viitor prin dispoziții legale și obligatorii" [7]. Acestea pot fi îndeplinite în diferite configurații ale țintelor operaționale, căile corespunzătoare de acțiune sunt redate prin mijloace adecvate, conținutul acestora fiind explicat și lămurit de părțile interesate, exprimarea lor trebuie să fie o formă de exercițiu democratic, cu eventuale obligații concrete de ordin economic, tehnologic, ecologic și geopolitic" [8]. Etapa finală constă în modelarea cantitativă a cifrelor din domeniul energetic românesc, prin "completarea a trei ipoteze de strategii energetice cu viziuni în perspectiva Strategiei în toate aspectele privind producția de energie, import, consum, producția totală de electricitate, evoluția intensității energetice,

nevoia de investiții, energia nepoluantă, prețurile de cost pentru producerea acesteia" [9]. Aceasta va include, după integrarea rezultatelor modelării, "proiecții optimizate ale mixului energetic, opțiuni tehnologice de dezvoltare către realizarea obiectivelor strategice fundamentale, definirea rolului statului în acest domeniu, țintele naționale privind măsurile de protecție a mediul înconjurător și a biodiversității. Vor fi enunțate țintele prioritare cu privire la cercetarea științifică, la educație și la formarea profesională, vor fi specificate acțiunile de consolidare a poziției României în piețele energetice regionale și de creștere a securității energetice interne și externe" [9].

La Bucureşti, experţi şi decidenţi din energetica românească au participat la Energy Strategy Summit 2016, al cărui obiectiv principal a fost „să contribue prin realizarea unui raport, care a fost promovat Guvernului cu propuneri pentru a fi cuprinse în strategie. Drept urmare, mai mulţi invitaţi din zona afacerilor, economişti cu o îndelungată experienţă şi autorităţi cu responsabilităţi în industria energetică au asistat la dezbaterea organizată pe subiectul strategiei energetice naţionale" [10]. Din acest raport am selectat următoarele idei esențiale: interconectivitate și avans tehnologic, costurile securității naţionale investiţia în securitatea energetică, contribuie la întărirea securităţii naţionale, independență, atingerea unui grad ridicat de asigurare a necesarului energetic, în totalitate din resurse interne, accesul la traseele gazoductelor din zona sud-est europeană, dezvoltarea portofoliului de resurse energetice, siguranţa resurselor, conlucrare la nivel regional; identificarea "intereselor specifice ale României, prin cunoaşterea situaţiei de facto din domeniul energetic, în scopul prevederii în acţiunile viitoare, și a modalității prin care putem să ne promovăm interesele la nivel regional"; - energia nucleară are o mare şansă în contextul actual, poate "să dovedească performanțele economice" ale acestei resurse, deoarece "produce o energie ieftină, sustenabilă, predictibilă, nepoluantă, cu un rol important în strategia viitoare a României"; - transportul de energie lichidă, gazoasă şi de electricitate trebuie sa fie permanent în atentie; - interconectare cu vecinii – subtraversare Dunării pe relaţia cu Bulgaria prin proiectul BRUA 2 (coridorul de gaze Bulgaria-România-Ungaria-Austria); - se impune "o cooperare între instituții, de intensificare chiar formalizată a dialogului între legislativ, executiv și reglementatorul energetic, pentru identificarea și îndeplinirea strategiei naționale" - să fim cunoscuți și recunoscuți în zona energetică europeană ca "garant în apărarea și cunoașterea clienților și al producătorilor. Cu un mix energetic diversificat are posibilitatea să solicite și beneficia poziții avantajoase în ansamblul Uniunii Energetice"; - Uniunea Energetică și "noua conjunctură din piața de energie reprezintă o mare oportunitate, iar companiile din România pot să se angajeze în mod activ și coordonat în derularea afacerilor în apărarea intereselor lor"; - României îi revine obligația ca pentru următoarea perioadă până în anul 2030 "să definească cea mai redusă generare de energie pe bază de lignit pentru a putea garanta satisfacerea permanentă a consumatorilor "după negocieri cu UE; - strategia energetică națională trebuie "să funcționeze ca îndrumar investițional, nu ca obligație sau interdicție, să indice primordial opțiuni"; - România are șansa de a ajunge un important producător și exportator de petrol și gaze prin "activități specifice acestui domeniu "; - pentru a beneficia de securitate energetică, "trebuie să fim producator"; - investițiile în domeniul mediului din proiectele energetice trebuie analizate "ca o șansă și nu ca .o cheltuială", prin creşterea eficienţei pieţelor de energie şi integrarea acestora în piaţa europeană; - includerea în practică și exploatarea rezultatului revoluțiilor tehnologice.

Revoluţia energetică pe care o traversăm a schimbat în profunzime politica, economia, mediul şi relaţiile sociale, a influențat impresionant cererea de energie, decuplând-o de creșterea economică. Au apărut în piață "resurse noi (șisturi, offshore de mare adâncime), a determinat apariţia pe piaţă pentru prima dată de tehnologii de foraj la

adâncime și a influențat continuu producția cu rezultat direct asupra abundenței de energie"; dezvoltarea infrastructurii și a competitivității constituie substanța unui nou proiect economic național, piața "funcționează prin competiție și prin creșterea concurenței, ceea ce este în beneficiul clientului"; - indiferent "că vorbim de clienții rezidențiali sau industriali, ANRE trebuie să acorde atenție drepturilor pe care aceștia le au în prezent și în viitor, indiferent de furnizor"; "sărăcia" energetică este o temă actuală care trebuie să fie abordată. Clienții vulnerabili, clienții protejați și clienții casnici sunt noțiuni care trebuie prevăzute distinct în actele normative viitoare, inclusiv acordarea de sprijin consumatorilor aflați în nevoie; creșterea eficienței piețelor de energie și integrarea acestora în piața europeană, deoarece pe cont propriu încă au o productivitate necorespunzătare, încurajarea cu sprijinul tehnologiilor inovatoare care pot verifica producția și consumul; conectivitatea și partajarea infrastructurii – un management mai inteligent al sistemelor complexe, o analiză mai sofisticată a datelor precum și a impactului tehnologic, "obligă companiile să facă mai mult decât ce le permite modelul tradițional de business"; ideea independenței energetice, înțeleasă ca "posibilitatea de a ne baza pe propriile puteri și de a avea inițiativă de stat în promovarea propriilor politici și interese; producerea energiei pe care o consumăm nu este pusă în practică din cauza legislației actuale"; "consumul biomasei aduce beneficii la realizarea de energie electrică și termică, reprezintă un avantaj de țară pentru România și trebuie susținută producția utilizând această resursă" care aduce sustenabilitate economică și independență energetică ; scăderea nivelului de carbon este o țintă importantă pentru România.

Accesarea continuă a fondurilor și mecanismelor de finanțare UE sub egida schimbărilor climatice va permite României să realizeze o economie nepoluantă și va promova adaptarea acestora. "Energia solară, eoliană și hidro, a fost cu peste 10% mai ridicată în primele șapte luni ale anului 2016. Consumul a crescut cu peste 9%, iar energiile-regină au fost cea solară (aproape 15% creștere), eoliană și hidro, care au înregistrat majorări-record în această perioadă, potrivit Institutului Național de Statistică (INS)" [11].

Politica energetică externă a României are nevoie de asocieri și discuții strategice, accorduri reciproce cu celelalte țări, "promovarea de fundamente și reguli de guvernanță globală fondate pe receptivitate, competitivitate a piețelor internaționale și pe promovarea tehnologiilor eficiente și curate" [12]. Diplomația României trebuie orientată "în funcție de scopurile urmărite privind interconectările cu rețelele de transport de gaz natural și energie electrică, structura sistemului său energetic, caracteristica zăcămintelor naturale, așezarea geografică și de creșterea economică". Interconectările, capacitățile noi de depozitare a gazului și calitatea infrastructurii sunt deficitare în România. Concomitent să se soluționeze problema stabilității politice și energetice a regiunii: interconectarea Moldovei este de primă importanță în paralel cu conectarea Ucrainei la traseele de aprovizionare existente.

Pe plan intern**,** într-o epocă a piețelor globalizate de energie și a interconectărilor, o politică de autosuficiență energetică, neimplicarea în dezvoltarea capacității de export de gaz natural din rațiuni de protecție prin prețuri legiferate, sub media europeană, și a unei accesibilități reduse la beneficiarii finali, a reprezentat o decizie contraproductivă politic și ineficientă economic. Diplomația României privind securitatea economică este legată de calitatea infrastructurii, a guvernanței și a politicilor energetice, domenii la care România înregistrează restanțe importante. Vulnerabilitatea cea mai pregnantă ține de "problematica guvernanței energetice, de precizia și constanța legilor și a reglementărilor, de compatibilitatea și valoarea instituțiilor, și de autoritatea actului birocratic și administrativ în sectorul energetic". Alte vulnerabilități interne de securitate energetică pe care le are în

față România în prezent "sunt legate de o stare tehnică precară a capacităților convenționale de producție a energiei electrice, care necesită investiții majore pentru a spori eficiența, pentru a reduce pierderile și pentru a realiza tranziția către conceptul de rețele inteligente prin modernizări și retehnologizări".

În context actual al uniunii energetice și al liberalizarii pieței, România are oportunitatea mai multor căi de acțiune, care să ducă, *în primul rând,* la o mai bună guvernare a sectorului energetic, având interese în concordanță cu cele ale UE, inclusiv de aplicare integrală a celui de-al treilea pachet energetic. *În al doilea rând,* România poate ajunge un jucător regional important și poate primi resurse financiare suplimentare din folosirea situației create ca țară de tranzit pentru rețelele de gaze naturale. *În al treilea rând*, România poate participa esențial la securitatea energetică a Ucrainei și a Republicii Moldova, prin proiecte finanțabile din fonduri europene, inclusiv interconectări cu Republica Moldova și Ucraina, ceea ce ar conduce la creșterea securității energetice a acestora și o mai bună funcționare a piețelor de energie în statele din estul Europei.

România trebuie să pregătească "o viziune cu acțiuni curajoase și ambițioase, de conservare a capacităților de producție, sprijinirea investițiilor în producători noi de energie electrică, măsuri concrete care să asigure dezvoltarea corectă a pieței. Este nevoie de un cadru juridic și de reglementare stabil pentru investitori, reguli de joc egale pentru toți actorii din piață, privind în ansamblu competitivitatea sectoarelor românești, realizarea unui consens cu părțile interesate după o estimare corectă a costurilor, a beneficiilor fiecărei alternative, examinării angajamentelor anterioare prin susținerea și avansarea obiectivelor uniunii energetice" [13]. România trebuie să aibă în vedere condițiile rămase neîndeplinite, *în primul rând*, cele de profesionalizare în continuare a instituțiilor-cheie, a reglementatorului ANRE, a companiilor de stat Transelectrica și Transgaz, Hidroelectrica, Nuclearelectrica și Romgaz, dezvoltarea abilităților de negociere, pentru ca aceștia să fie pregătiți să reacționeze la evoluțiile în contextul international. *În al doilea rând,* România ar trebui să sprijine mai mult integrarea pieței de energie prin crearea unui viitor reglementator european în domeniul energiei și "europenizarea rețelelor de transport al energiei electrice și a gazelor". Dezvoltarea "unor operatori europeni și a unui reglementator cu o viziune paneuropeană, dacă este inteligent susținută de negociatorii români, ar putea constitui cel mai bun lucru pentru propriul interes național al României" [13]. Este necesar ca diplomația energetică românească să descifreze permanent potențialele vulnerabilități, să riposteze fără întârziere la mișcările de pe piețele internaționale de energie, luând în considerare realitățile geopolitice, să demareze proiecte majore de infrastructură, să încheie parteneriate strategice "ce implică aspecte de securitate, mediu, economice, cercetare și tehnologie, parteneriate ce se construiesc pe eforturi considerabile, pentru obținerea unui consens" [13]. Un aspect important în demararea unor proiecte de succes la nivelul diplomației energetice este reprezentat de calitatea corpului diplomatic, demersurile acestuia în demararea, implementarea sau susținerea unor proiecte transfrontaliere, în reprezentarea intereselor României pentru atingerea obiectivului final de a face eforturile din sectorul energiei mai vizibile și mai de succes în derularea proiectelor.

CONCLUZII

Noutatea dezbaterii din cadrul conferinței scoate în evidență pericolele existente privind securitatea economică și energetică, identificarea căilor de depășire ale acestora. Cercetarea, inovarea și competitivitatea, necorelarea între procesele și fenomenele care privesc factorii de risc la adresa dezvoltării durabile a securității economice, în condiții de vulnerabilitate și instabilitate a economiei europene și mondiale, aflate într-o conjunctură

internațională schimbătoare, pot genera instabilitate în planul procesului de reformare. Nu se poate neglija nici modul în care statele membre își propun să se raporteze la politica energetică a UE, manifestând o sensibilitate ridicată în fața șocurilor care se reflectă ca vulnerabilitate economică. Efectele instabilităţilor de pe pieţele globale sunt în mare măsură atenuate, în ultimii ani, datorită liberalizării şi posibilităţii de a se aproviziona din import cu produsele necesare. Preţurile energiei vor fi afectate de vulnerabilităţile privind investiţiile din domeniul energiei, precum şi de stabilitatea preţului carbonului şi a preţurilor internaţionale, datorită creşterii cererii în ţările emergente. Competitivitatea, securitatea aprovizionării şi obiectivele legate de atenuarea schimbărilor climatice vor fi compromise, dacă reţelele electrice nu vor fi modernizate cu reţele alternative competitive şi mai curate, prin folosirea eficientă a energiei pe tot parcursul lanţului energetic. Securitatea aprovizionării cu energie, utilizarea eficientă a resurselor, îmbunătăţirea eficienţei energetice, preţuri accesibile şi soluţii inovatoare sunt cruciale pentru o creştere durabilă, care să conducă la diminuarea efectelor rezultate din vulnerabilitatea şi instabilitatea energiei în Uniunea Europeană.

Mediul actual în evoluţia securitataţii energetice este influenţat de modificările profunde existente pe scena internaţională prin apariția de noi concurenți în piața energetică, unde vechii actori își reduc ponderea, sau dispar, iar alți actori de tip statal, sisteme integrate economico-politice, continentale și globale își dispută cucerirea scenei energiei.

Politica energetică trebuie orientată spre accesibilitatea și interoperabilitatea tuturor conductelor şi terminalelor, identificarea unor trasee alternative și a unor metode eficiente de utilizare a energiei, prin găsirea unor alternative de substituire a resurselor limitate și atenuarea dezechilibrelor de mediu ale resurselor energetice care în prezent devin tot mai limitate pe plan naţional si european. Teama epuizării acestor resurse în viitorul apropiat, obiectivele climatice și integrarea resurselor rezultate din energia verde, au determinat o reorientare a obiectivelor în materie de energie și climă a membrilor UE.

Credem, însă, că este nevoie de o strategie energetică comprehensivă, care să identifice clar vulnerabilităţile şi riscurile majore, să stabilească în mod concret obiectivele strategice realizabile, modalităţile de îndeplinire a lor şi, mai ales, direcţiile de acţiune care să asigure un grad înalt de securitate economică, concomitent cu o dezvoltare durabilă, prin cresterea competitivităţii, funcţionării eficiente a unei pieţei concurențiale interne de energie, integrate, interconectate și care să contribuie la dezvoltarea tehnologiilor energetice.

BIBLIOGRAFIE

1. *Financial Crisis Energy-Security-Cooperation; Energia şi criza – mai mult sau mai puţin în siguranţă?* Disponibil: www.nato.int review
2. *Către o Europă durabilă până în 2030 Bruxelles*, 30.1.2019, COM(2019) 22 final
3. Stănișteanu, A.I. *Securitatea energetică şi coridoarele energetice din Balcani.* București, În: Buletinul Universităţii Naţionale de Apărare "Carol I", 2015. Disponibil: https://revista.unap.ro/index.php/revista/article/download/156/155 [citat 12.06.2016]
4. Al patrulea raport privind starea uniunii energetice. Bruxelles, 9.4.2019 COM(2019) 175 final
5. Popescu M. *Politica actuală privind finalizarea viitoarei strategii energetice naționale a României.* Disponibil: www.ecoforumjurnal.article
6. *Strategia de Securitate Naţională a României.* Bucureşti, 2006. 7 p. Disponibil: www.presidency.ro.

7. *Raport al Comisiei privind punerea în aplicare a Comunicării privind securitatea aprovizionării cu energie şi cooperarea internaţională şi a concluziilor Consiliului pentru energie din noiembrie 2011*. Disponibil: http://eur-lex.europa.eu/procedure/EN/1041210
8. *Despre strategia energetică a României*. 25 iul. 2016. Disponibil: www.hotnews.ro. Actualitate Home - HotNews.ro
9. Popescu M. *Securitatea aprovizionării cu energie a UE şi cooperarea internaţională*. În: Conferinţa internaţională Global Economy under crisis. Constanţa, 4-5 decembrie 2014. Disponibil: http://stec.univ-ovidius.ro/conferinte/the-international-conference-present-issues-of-global
10. Parlamentul European. *Fişe tehnice privind Uniunea Europeană. Rezoluţia Parlamentului European din 21 mai 2013*. Disponibil: www.europarl.europa.eu.
11. *Statistici privind energia din surse regenerabile* - Statistics ; ec.europa.eu › eurostat › statistics-explained .
12. *Energie curată pentru toți europenii*. Bruxelles, 30.11.2016 COM(2016) 860 final
13. Ministerul Energiei. *Securitate și diplomație energetică*. 2016. Disponibil: http://cursdeguvernare.ro/Raport-Sesiune-Lucru

EUROPE IN THE CONDITIONS OF GLOBAL TURBULENCE – THEORETICAL AND APPLIED ASPECTS

Lichev Tihomir
PhD, associate professor
The "D.A.Tsenov" Academy of Economics, Svishtov, Bulgaria
e-mail: t.lichev@uni-svishtov.bg

Abstract
In recent decades, changes in world development have brought global security to the forefront, as well as that of individual countries and regions. Security, whether global, national or regional, is linking to the geopolitics and geoeconomics that lead major countries and political blocs. The world that has being forming because of globalization is interdependent on economic and integration processes. The modern free movement of goods and services, as well as the unrestricted distribution of information, pose serious threats to society. There are also negative consequences of globalization such as the destruction of national societies and social ties. That is why the problem of security in all its aspects is a particularly important and topical issue for modern science. The present study analyzes the theoretical and applied aspects of national security – demographic, military, economic, political, information and others. In recent months, medical and infectious aspects of security have become important in connection with the COVID-19 pandemic. The main alternatives for the development of the world are indicated, incl. and Europe, internal and external problems and threats to the EU.

Keywords: *Globalization, Global security, EU, Economic security; pandemic, COVID-19*

JEL Classification: *F5, F6, R5*

INTRODUCTION

In recent decades, changes in world development have brought global security to the forefront, as well as that of individual countries and regions. Security, whether global, national or regional, is linking to the geopolitics and geoeconomics that lead major countries and political blocs.

The changes in world development after the Cold War put on foreground global security as well as that of individual countries and regions. Security - be it global, national or regional connects directly with geopolitics and geoeconomics. There are links between the world economy (geoeconomics) and global security. The same dependence exists in any national economy and national security, and within individual regions. In modern conditions there are national conflicts that threaten security not only in individual countries but also in regions where [1, pp.200-208] it`s found. In modern conflicts, there is a real danger that they will grow into continental ones and even acquire a global character.

Globalization today is a phenomenon that is rapidly entering all aspects of real life and, along with the benefits it brings, creates problems for the individual. Until recently, unimaginable processes such as the practical merging of borders, cultural unification and loss of identity are emerging. Instead of the beautiful world of dreams for the future, there are struggles for military, political and economic supremacy.

THE ESSENCE OF THE CONCEPT OF "SECURITY" – THEORETICAL ASPECTS

The changes in world development after the Cold War put on foreground global security as well as that of individual countries and regions. Security - be it global, national or regional connects directly with geopolitics and geoeconomics. There are links between

the world economy (geoeconomics) and global security. The same dependence exists in any national economy and national security, and within individual regions. In modern conditions there are national conflicts that threaten security not only in individual countries but also in regions where [1, pp.200-208] its found. In modern conflicts, there is a real danger that they will grow into continental ones and even acquire a global character.

Globalization today is a phenomenon that is rapidly entering all aspects of real life and, along with the benefits it brings, creates problems for the individual. Until recently, unimaginable processes such as the practical merging of borders, cultural unification and loss of identity are emerging. Instead of the beautiful world of dreams for the future, there are struggles for military, political and economic supremacy.

The world that is being formed as a result of globalization is very interdependent on economic and integration processes. The modern free movement of goods and services, as well as the unrestricted dissemination of information, pose serious threats to society. Among the negative consequences of globalization are the destruction of the cultural foundations of national societies and the disruption of social ties [17, pp.135-137].

The constant weakening of individual countries, the reduction of their stability and sovereignty are the main characteristics of the globalization process. As the famous Polish scientist, professor at the University of Warsaw and Leeds Sigmund Baumann points out, "expropriation begins, but this time of the state." Globalization is nothing more than a totalitarian extension of the logic of global financial markets to all aspects of life [1].

Another prominent contemporary sociologist, W. Beck, points out in his monograph "The World Risk Society" that even greater control of the dangers is needed, which hides the situation of serial produced uncertainty. He also points out that "global risk itself is a kind of organized irresponsibility" [2, pp. 14-26].

The above shows that security in its various forms in modern conditions is extremely high priority. It is related to such issues as economics, politics, law, morality, religion, traditions. The system of knowledge about security has its interconnected national and international aspects, as the focus of individual analysts are the individual sovereign states, the international community and even individual human individuals.

According to some authors, there are essential prerequisites for the gradual formation of a new scientific field, whose research field is the field of security [8, pp.5-17].

The concept of "security" is multifaceted and thus difficult to define precisely, completely and unambiguously. The notion that this is "reliability", "maximum reliability", "protection", "protection", "sustainability" and others has gained wide citizenship. In a number of Bulgarian and foreign dictionaries these concepts are defined as follows. For example:

- "secure" – trustworthy, faithful, positive, reliable, often called a safe person or secure protection;
- "security" – quality of confidence, confidence, positivity, no danger, elimination of danger, safety;
- "dangerous" – containing danger, carrying danger; used in various phrases as a dangerous enemy, etc..;
- "danger" – an opportunity for trouble, an opportunity for misfortune;
- "safety" – no danger, security;
- "protection" – preservation, protection from danger, protection from trouble, defense;
- "protection" – protection, patronage, care for someone or something, etc.;
- "self-defense" – protection with one's own forces from danger, which protects life, property, interests, status quo [4, pp.11-12].

Therefore, the term "security" can also be defined as the absence of "danger", "safety", and the term "uncertainty" - with "danger". Obviously, the pairs of expressions "security" / "uncertainty" or "danger" / "safety" complement each other.

Security (respectively - uncertainty) have many dimensions - economic, financial, psychological and others. Economic failure is often associated with political problems and severe conflicts.

One of the most developed topics is undoubtedly the idea of individual security. The report "The New Dimension of Human Security" of the United Nations Development Program (UNDP) addresses key aspects of security. The following groups are listed there:

- economic - food security with which they are connected with environmental safety and food shortages; high mortality and disease; degradation of regional and global ecosystems; deficit of clean water; Global Warming; deforestation; natural disasters that take the lives of thousands of people;
- political security - protection of the individual from political repression and other forms of violence; state guarantees for the protection of its own citizens.

In our opinion: the most meaningful is the definition, according to which: "security is conjunctive, situational clarity, objectively and subjectively guaranteeing trouble-free short- and medium-term predictability and confidence" [15, pp.7-16].

GEOPOLITICAL PROBLEMS AND CONFLICTS IN EUROPE

Ensuring national security is paramount for any country. According to Art. 20 of the Concept for National Security of Bulgaria, it represents: “a state in which the fundamental rights and freedoms of citizens, state borders, territorial integrity and independence of the country are protected, when there is no danger of armed attack, forcible change of the constitutional order, political dictates or economic coercion and when democratic functioning is guaranteed. The state, as a result of which the society and the nation preserve and increase their prosperity and prosperity“ [10].

The problem of national security is becoming increasingly relevant in today's world of refugee waves, demographic imbalances, economic, environmental and energy crises [13, pp.104-105].

National security is a multi-component system that includes various elements - demographic security, military security, political security, economic security, social security, information security, environmental security. In recent months, the medical and infectious aspects of security have been particularly important.

There is an interdependence between the various forms of national security and each of them cannot exist independently.

The rapidly evolving process of globalization has created hopes for resolving emerging conflicts within individual countries and alliances around the world, which have quickly given way to growing concern that the world is facing new risks and confrontations that require a new world order.

According to the American analyst Joseph Nye, there are at least five main alternatives for the development of the world, namely:

- return to the bipolar systemтри икономически блока
- unipolar domination
- multilayered interdependence
- multipolar system

The same author notes that it is high time to get rid of the old notions formed in the Cold War era, when order was based primarily on the sovereignty of the individual state. According to Joseph Nye, "we will live in an anarchic world". Order will be ensured both

by the balance of power between the states, as the realists claim, and by the developing international investments according to the liberal idea. This order will not always be fair. Justice and order often come into conflict with each other, even on issues of self-determination. Is it more important to keep the borders intact, or to pursue humanitarian goals while violating territorial integrity? How do these alternatives affect the principles of order? [14, pp.238-243] These disputes are not easy to resolve, especially given the new realities in the world.

Any national conflict created by the state of the national economy creates changes in national security, which poses threats to the regional economy and security. Global conflicts threaten global security.

According to Manuel Castel, global conflicts are created on various occasions. In recent years, they are mainly of two types - geoeconomic and geopolitical. They are based on the so-called "vital interests", which are the main strategies of the United States [9]. Conflicts are a cover for the concept of "economic interests" and are created and managed in areas with energy resources - coal, oil and natural gas. It is no coincidence that they are very fierce in the Middle East, involving Arab countries and countries defending their "vital interests" - the United States, Russia, Turkey and others.

The future of the geoeconomy will also be determined by the West-East communication bridge. The leading role will be played by the Eurasian Natural Communication Corridor, which will be crucial for Europe's security.

The two world geoeconomic poles - the European and the Asia-Pacific - will play a key role in the emergence and development of global conflicts. The third world geoeconomic pole, the North American pole, also has its place.

According to the famous political scientist Zbigniew Brzezinski, in the coming years four geoeconomic directions are possible for the development of transnational communications (including tourism):

1. From North America through Russia to Europe – This is a transnational corridor through Alaska and Siberia;
2. From China to Europe – passes through Russia or the "Silk Road". In 2014, it was for this reason that the Eurasian Economic Union was established, which is expanding today. Russia has a leading role;
3. Meridian corridor North - South. It is a corridor from Northern Europe through the Middle East, the Caucasus to Iran and India;
4. Far Eastern Axis - from Singapore and China through Russia to North America [3].

All these transatlantic communication corridors are crucial for the future economic redistribution of the world. Russia, China and the United States play a leading role in them. It is important for Europe's security to find its place in this geostrategic system. According to US "National Interests" doctrine, there are five outbreaks of global conflicts that could lead to world war.

These are:

- Sunni conflict. This includes the United States, Russia, Turkey, Iran, Saudi Arabia. In addition to these countries, others are occasionally included.
- Indo-Pakistani conflict. This conflict is set in their fall as colonies of England. Unofficially, Great Britain (as a former ruler with great influence), China and the United States are also involved in this conflict. It is through Pakistan that their fastest route to the Arabian Sea is, which is also the most direct connection with large parts of the world.
- East China conflict. To this day, there is a serious a dispute between China and Japan over the Senkaku archipelago, which is currently controlled by Japan.The

island of Taiwan. It can often be found in directories as well Chinese Taipei. Conflict between China and the breakaway is always possible, but also with the possible involvement of the United States.

- Ukrainian conflict. It is set in the past when it created independent state.

Later it was part of the USSR. To this day, major regional differences are clear. For example, the East (around Donetsk, Kharkiv), but also Odessa and Crimea are Russian-dominated; Western Ukraine professes Catholicism and has great Polish influence, and the region of Transcarpathia has Hungarian and Slovak influence [12, pp.149-171].

This is the conflict with the largest involvement of geopolitical players such as Ukraine, Russia, Poland, but also the United States, the European Union and NATO. As all these conflicts deepen, they could lead to regional war and even global war.

Although only in the economic field, there are those between Russia, the United States and the European Union; between Russia and Turkey (where they sometimes transfer "sparks"). These conflicts are of great importance to the whole world, as they often involve the strongest economies [7, pp.25-35].

The world is facing a number of problems. Europe is no exception to this turbulent state of modernity. As a union of sovereign states, the continent faces many threats. In general, these threats can be defined as internal and external to the European Union.

Internal threats related to problems caused by the so-called "intimate enemies of democracy". According to the famous Bulgarian philosopher and culturologist Tsvetan Todorov, who lives and works in Paris, freedom is a basic value of democracy, but there is another specific type of freedom that under certain conditions can become a threat to democracy.

The same author draws the sad conclusion that we live today in a democratization that suffers from its excessiveness and in which freedom becomes tyranny, the people become a manipulative mass, the desire to promote progress degenerates into crusading ambition [16, p.217].

Still, it is better to live in a democracy before living in totalitarian societies.

This “corrosion of society” also leads to many problems in the European Union, such as:

- Clash between different ethnic groups, peoples and races within different countries Clash between the different social strata;
- Lack of unanimous opinion of individual members in modern conditions;
- In recent years significant internal turbulence – constant economic crises, starting with the World Economic Crisis (2008) and continuing to this day in some countries (most notably Greece, Spain and others);

1. External threats to the European Union can be identified ethnic, political conflicts, organized crime, the imperial ambitions of countries such as the United States, the radicalization of Islam, the global migration crisis, terrorism and others.

2. The proliferation of cross-border organized crime is also one of the main threats to the security of citizens and the democratic foundations of society - economic crime; drug, arms and human trafficking; smuggling; production and distribution of counterfeit currency and documents, cybercrime, money laundering, etc.

A huge problem for international security within the European Union with non-EU countries with weak statehood, which are not able to guarantee the security, rights and freedoms of their citizens, to manage public relations and to fulfill their international obligations. Growing religious and cultural differences, especially in the Arab world, are creating conditions for radical conflict and political instability. In these areas, in addition to

the destruction of nation-states, something even more terrible is happening - the disintegration of nations.

This process began with the events in Lebanon, and today it is throughout the region. Much earlier, the famous thinker Jean-Marie Gounod in his book The End of Democracy (1997) called this process "Levanizing the World." According to him, "Lebanon is not that part of a partially extinct country on the map of the Middle East. From now on, it is in each of us." [5]. Then the process of disintegration of nations is in full swing in modern times - in Libya, Syria, Algeria and others. The unstable economic and political situation and the low standard of living in these Third World countries generate strong migratory pressure on European countries.

Cybercrime is a new modern direction of pressure on various countries and poses a serious threat to the security and stability of nation states. Cyberattacks block the normal functioning of information systems important for the economy, the financial system and the government.

In addition to the above-mentioned threats to Europe, there are also those related to the Environment and Energy.

In addition to these threats to the world and the EU, there are in particular those related to biological threats and in particular the pandemic of COVID-19.

In the present study, a brief analysis of the medico-geographical aspects of the pandemic is made - the origin, stages of growth in different countries and continents. The regions in the EU where it is the largest are listed. The main consequences of the pandemic are also considered - medical, economic, social, psychological and others. According to various scientists, the pandemic of COVID-19 occurs in the fall of 2019. In the 11 million city of Wuhan (Hubei Province) and is growing rapidly worldwide. Thanks to the measures taken quickly, it was limited to China, and then to the whole of East Asia (Korea, Singapore, etc.). In contrast to this region in Europe and North and South America, the measures are delayed due to various reasons, e.g. In many countries, the rulers completely deny the existence of this pandemic, and it is reduced even to the common flu. A typical example are the largest and most powerful countries in the world - the United States, Russia, Britain, India, Brazil, Argentina and others. These are the countries with many infected and dead people in the world. For political reasons, no action was taken in Italy and France, holding local or parliamentary elections; sporting and cultural events (Austria, Germany, Italy, etc.) where measures are delayed. Only in some smaller countries have more adequate decisions been made (Bulgaria, Montenegro, Kosovo, etc.) to limit it. From the end of February, the pandemic goes through the following stages:

1. Origin - in China and East Asia and its spread. Lack of measures in other countries;

2. Growth of the pandemic - the largest in Italy (mainly in the Northern regions, France, Spain, Germany and Great Britain);

3. Countries whose leadership does not recognize their existence and fall into an acute pandemic crisis (USA, Brazil, Argentina, Russia, India), which are also the largest infections and deaths. Unlike them in China, Korea and other countries, the pandemic is limited;

4. The EU will not take any coordinated action until early autumn. Restrictions on border crossings between member states are beginning have been introduced. There are only isolated cases where patients are been transported by air in border areas from France to medical centers in Germany;

5. Only at the end of the summer of 2020. The EU and its member states are launching a policy of closing and restricting travel and tourism between regions and countries in order to reduce the infection.

6. In recent months, the EU are not been united in its response to the pandemic. Eg. Austria, Spain and Bulgaria want to open winter ski resorts and Germany, France and others. on the contrary, throughout the EU.

7. In recent months, the EU has agreed on a common pandemic policy - funding, medical supplies, approvals and the purchase of the same vaccines for all member states.

In the first years of the COVID-19 pandemic, the EU faced a number of threats, the main ones being:

1. Insufficient level of development of the health systems - insufficient medical staff, beds in intensive care units, equipment, etc. There is also a problem with the different levels of medical services in the separate territorial units (Bulgaria, East Germany, Southern Italy, etc.).

2. Sharp decline in financial revenues and deterioration of the economic situation. The crisis is especially severe in entire industries such as air transport, tourism, culture and others.

3. The crisis has led to a deterioration of the social environment in the country. The number of closed companies, increasing unemployment, etc. is constantly growing.

4. In the education system there was a transition to distance learning, which lost personal contact with teachers and worsened the quality of the educational process.

5. Last but not least, the crisis affects the mental state of individuals.

The first-ever European Union Regional and Local Barometer report identifies the state of the Union at local level - in individual regions, as well as cities, municipalities and rural areas. The consequences of the crisis are asymmetrically distributed. The worst situation is in the coastal areas of Croatia, Eastern Bulgaria, in Andalusia, Castile and Leon, Valencia and the capital Madrid in Spain; Ile de France in France; most of the Italian regions, Central Macedonia and Crete in Greece. There are significant differences in the development of individual cities and municipalities. Positive examples of business support are given in Luxembourg (exemption from rents for retail outlets), Vienna, Sofia and others. lending to small and medium-sized businesses. There is also a growing interest in life in suburban and rural areas, as the settlers work through information technology. An interesting example is the organization of charters for understaffed institutions in the provinces of Burgenland and Lower Austria for 355 social workers and assistants from Romania, Bulgaria and Croatia. [17]

All these aspects lead to new changes in the regional policy and regional development of the individual countries in the EU. Assistance, which has so far been to the least developed regions in the context of the crisis, should be shifted towards the most affected. For example, in the EU, the oldest population (over 25% of the population is at or over the retirement age) is in the Lombardy region of northern Italy, where it has the highest number of retirement homes, but also the highest mortality. In Bulgaria, the number of infected is around the European average, but the country is one of the first places in terms of mortality.

CONCLUSIONS

The present study is an attempt to systematize the theoretical developments in the field of security in its various aspects. The main geopolitical problems and conflicts that affect the current development of the EU are considered. The main external and internal

threats to modern Europe are identified. In modern conditions, the most serious global problem is undoubtedly the growth of the COVID-19 pandemic and its impact on the overall economic, social and health development of society. Although humanity is already in the second stage of its expansion, so far it cannot cope with its growth. Europe, as well as the whole world, is likely to face an economic, social and pandemic crisis.

BIBLIOGRAPHY

1. Бауман, З. *Глобализацията – последиците за човека*. УИ „Климент Охридски“, 1999.
2. Бек, У. *Световното рисково общество*. „Отворено общество“, 2002, с.14-15, с.26.
3. Бжежински, З. *Стратегическа визия. Америка и кризата на глобалната сила*. 2012.
4. Григоров, В. *Лоялност и сигурност*. УИ „Климент Охридски“, 2001, с. 11-12
5. Гуно, Ж. М. *Краят на демокрацията*. 1997.
6. Димитров, Д. *Актуални проблеми пред сигурността на Европа*. В: Съвременни заплахи за сигурността на Европа, ВУСИ, Пловдив, 2016, с. 20-28.
7. Иванова, П. и Т. Личев. *Сигурност и безопасност в туризма*. Свищов, АИ „Ценов“, 2017.
8. Йончев, Д. *Сигурността като проблем в науката*. В: Актуални проблеми на сигурността, НВУ, В. Търново, 2018, с. 5-18.
9. Кастел, М..*Информационная эпоха*., М, 2000.
10. *Концепция за националната сигурност на България*, чл. 20, С, 1998
11. Костов, Д., М. Михайлов. *Глобалните геоикономически конфликти и сигурността на Европа*. В: Съвременни заплахи за сигурността на Европа, ВУСИ, Пловдив, 2016, с. 200-208.
12. Михайлов, В. *Украйна – етнополитически профил*. В: Регионални геополитически изследвания, Варна, 2009, с. 149-171.
13. Михайлов, М. *Демографската криза и националната сигурност на България*. В: Съвременни заплахи за сигурността на Европа, ВУСИ, Пловдив, 2016, с. 104-105
14. Най, Д. *Международните конфликти – теория и история*. „Изток – Запад“, 1998.
15. Русев, М. *Геополитически и геостратегически предизвикателства пред глобалната и регионалната сигурност – основни методологични и приложни аспекти*. Том 3, ВТУ, НВУ, 2009, с. 7-16
16. Тодоров, Ц. *Интимните неприятели на демокрацията*. Изток – Запад, 2013, с.20; с.217
17. Трендафилова, К. *Медиите и новите заплахи за сигурността* В: Съвременни заплахи за сигурността на Европа, ВУСИ, Пловдив, 2016, с. 135-137. https://cor.europa.eu/bg/news/Pages/eu-regional-and-local-barometer.aspx

THE PUBLIC FINANCES OF THE FRUGAL FOUR COUNTRIES IN THE CONDITIONS OF EUROPEAN ECONOMIC RECONSTRUCTION

Angelov Petko
PhD, associate professor
The "D.A.Tsenov" Academy of Economics, Svishtov, Bulgaria
e-mail: p.angelov@uni-svishtov.bg

Abstract
The paper focuses on the main measures of public finances (government revenue, government expenditure, net lending/net borrowing position) of the countries of the so-called "frugal four" for a period of twenty years (2000 – 2020), in the conditions of European economic reconstruction. The aim of the paper is to present arguments for the reported trends in the dynamics of the above mentioned measures and to justify the conservative policy of public finances management pursued by Austria, the Netherlands, Sweden and Denmark. As a result of the study of budgetary measures, an assessment of the state of public finances of the four countries was performed and the macro factors for this were derived. The state of the latter, as it is known, is dynamic and their future research and control is necessary to preserve the budgetary stability of the "frugal four" and the European Union in the current European economic reality.

Keywords: *public finance, government budget, European Union, economic reconstruction, "frugal four"*

JEL Classification: *H59, H61, H69*

INTRODUCTION

Over the last 20 years, the world economy has undergone significant changes, which has had an impact on the slowdown in global and sector development. The foundations of modern European finance, laid decades ago, have been shaken by international conflicts, such as the US – EU trade war [3], Brexit, the COVID-19 pandemic, etc. The global pandemic has its impact both in the individual financial spheres – banking [5], insurance [6], investment, and in public policy and public finance. In geopolitical aspect, there is competition among countries based on a number of economic means. As a result of globalisation and the established interstate relations, many of them today are in situation where they are trying to defend their sovereignty or that of the alliances in which they are members. The demonstration of power, as well as the strengthening of the economic positions of the individual countries, inevitably have their influence on the budget processes in the countries. In this line of thought, the main aim of this paper is to follow the trends in the main budgetary measures – government revenue, government expenditure, net lending/net borrowing position of the "frugal four" countries – Austria, Sweden, Denmark and the Netherlands.

THE STATUS OF BUDGET REVENUES AND EXPENDITURES

Among the main goals [4] of the formation of the European Union as a community is the sustainable development based on balanced economic growth and price stability, as well as strengthening of economic, social and territorial cohesion and solidarity among EU countries. The European Union's plan for support and development of weaker countries in 2020 find the opposing position of the four "frugal" countries [2] – Austria, Sweden, Denmark and the Netherlands. What the four countries have in common is that they are members of the European Union. The difference among them is that Austria and the Netherlands are among the "founding states" [8] of the Eurozone, while Sweden is among the Non-Eurozone countries and Denmark adheres to its own currency by agreeing not to

apply part of the legislation or some EU treaties. The focus of the latest EU budget positions is on the Multiannual Financial Framework for the period 2021-2027. It is based on a reasonable compromise between the EU's sustainable development and competitiveness and reduction of inequalities within the EU. For many EU countries, European funds are seen as a major driving force that helps economic movement. In unison with that, such policies are Cohesion and Common Agricultural Policy which are significant together with the policies for innovation, competitiveness and modern technologies. "Frugal four" countries adhere to the common position of greater guarantees that countries that receive EU aid, will pass reforms and that any aid should be in the form of loans and not grants. This, in turn, is a position to avoid an overall increase in the Multiannual Financial Framework of the European Union. According to Austrian Chancellor Sebastian Kurz [9] "The common market, as an essential driver of European competitiveness, is not an expensive endeavour. Above all, our contribution to the budget must remain stable, taking into account inflation and economic growth." It is essential for the stability of the EU to focus a significant share of the budget on meeting economic challenges, such as promoting the competitiveness of the economy and establishing stability in budget indicators [1].

The paper focuses on the situation and the percentage change in the main budget measures (government revenue, government expenditure and deficit/surplus) of the considered frugal and fiscally stable countries - Austria, Sweden, Denmark and the Netherlands. The data shown in the following figures are calculated or taken (deficit/surplus) on the basis of monthly data for the relevant indicators available in the European Central Bank database.

The level of government revenue varies considerably in these countries. For the studied period a dynamic percentage change is noted. There is a strong intensity in the revenues, as only in Sweden there is a partial retention of the trend in the period 2006-2009, showing a steady change in the indicator. Within the studied countries, the largest margins are seen in the Netherlands and Denmark. It is interesting to note that at the end of the analysed period Q2 – 2020 in Austria and the Netherlands government revenues decreased sharply, and in Denmark and Sweden – decreased significantly. In all four countries, in view of the outbreak of the COVID-19 pandemic, fiscal restrictions are applied, including the provision of opportunities for deferral of payments to the state budget, suspension of sanctions for non-payment of budget debts, tax exemption for people working to overcome the crisis. Figure 1 clearly shows the trend:

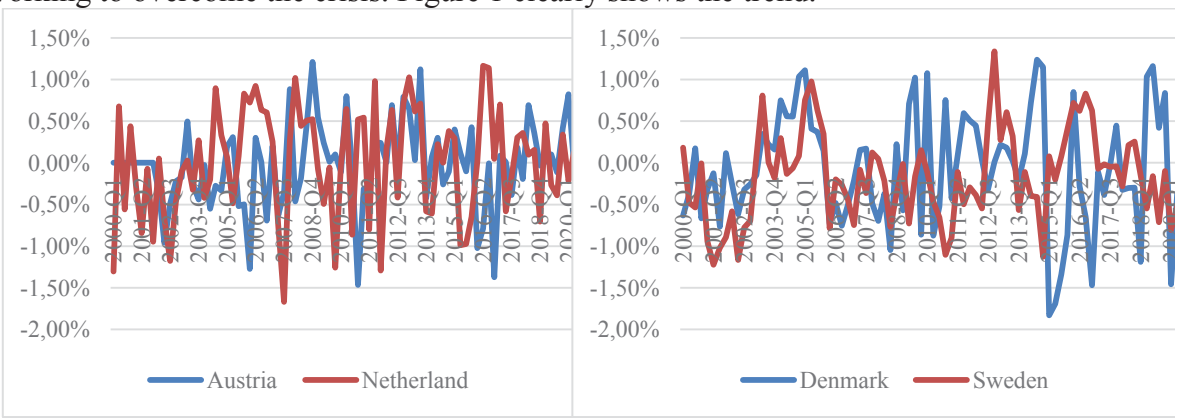


Figure 1. Total government revenue - % change compared to the previous year

Source: Author 's database calculations by: https://sdw.ecb.europa.eu

With regard to government expenditure, as shown in Figure 2, the percentage change follows the opposite of the revenue trend. Relatively stable change is observed in

all four countries considered. What they have in common is that in the period 2007-2009, there was a relative increase in government expenditure caused by rising government costs to overcome the economic crisis. The Netherlands is the country with the least change in the analysed indicator and shows stability in government expenditures, which is indicative of maintaining a stable budgetary policy. It is interesting to note that the considered "frugal countries" – Austria, the Netherlands and Sweden have a significant increase in their government expenditure in early 2020. This is due to the increasing expenditure of overcoming the social and health issues caused by COVID-19.

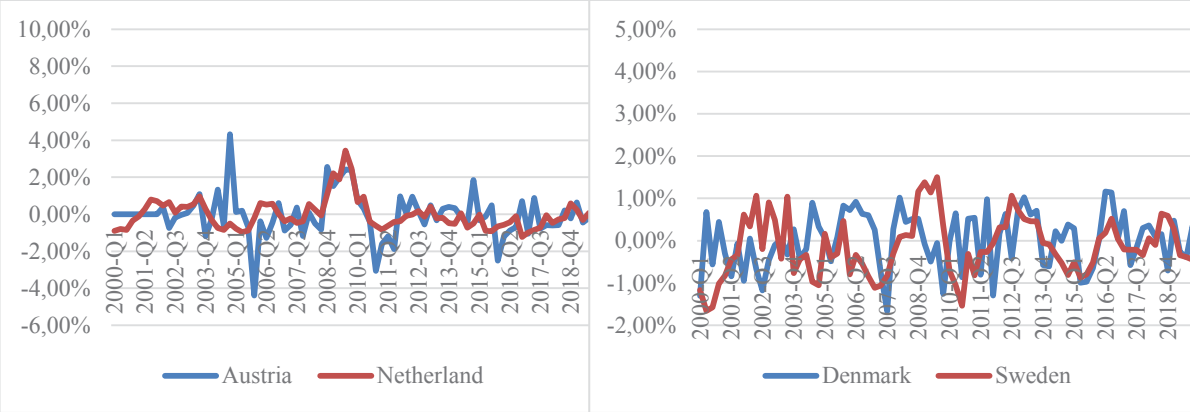


Figure 2. Total government expenditure - % change compared to the previous year
Source: Author 's database calculations by: https://sdw.ecb.europa.eu

POSITION OF INDEBTEDNESS (NET LENDING/NET BORROWING POSITION)

Referring to the data analysed above, it could be said that Austria, the Netherlands and Sweden have efficient tax administrations, and only Denmark could be ignored due to its relatively complex tax system and the lack of indirect taxes. This, in turn, has a direct impact on the economic development of the countries, which in Denmark is compensated by additional budget relief. In this line of thought, Figure 3 depicts the level of difference between the government revenue and government expenditure in absolute value.

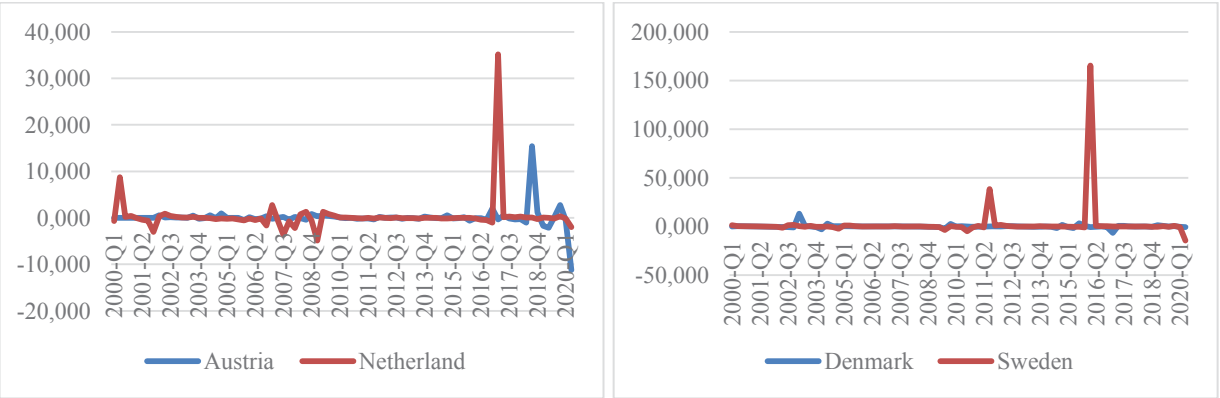


Figure 3. Net lending/net borrowing
Source: https://sdw.ecb.europa.eu

According to the data in Figure 3, the weak dynamics in the indebtedness indicator is seen. A significant excess of revenues over expenditures was observed in 2016 in Netherlands and Sweden, in 2018 in Austria, and at the end of the period (Q2 2020) again in Austria there was an excess of expenditures over revenues, resp. budget deficit. It is important to note that it is not of significant importance whether and to what extent the budget indicator deficit/surplus deviates from the set budget values, but whether there are

conditions for it to deviate to such an extent that it will negatively affect state budgets or affect the budget of the EU.

CONCLUSION

It should be noted that the four countries contribute significantly more to the EU budget than they actually get from it. The exit of the United Kingdom, which leaves a significant gap in the EU budget, has a negative impact on the budgetary measures of the countries, as well as on the work to reduce the level of economic impact of the current COVID-19 crisis. It is too early to make a definite assessment of the impact of the above factors on public finances, but it is certain that their situation is dynamic and their future study is necessary to maintain the budget stability of the "Frugal Four" and the European Union in the context of the current European economic reconstruction.

BIBLIOGRAPHY

1. Aleksandrova, A., & Pavlova-Banova, M. (2020). LOCAL FINANCES IN BULGARIA ON THE THRESHOLD OF THE THIRD DECADE AFTER THE REFORMS IN THE SECTOR. *KNOWLEDGE*, 875-881.
2. Bloomberg.bg. (2020). *Fiskalno konservativnata chetvorka se obyavi sreshtu plana na Merkel i Makron*. Retrieved 11 16, 2020, from https://www.bloombergtv.bg/a/8-novini-ot-sveta/48167-fiskalno-konservativnata-chetvorka-se-obyavi-sreshtu-plana-na-merkel-i-makron
3. Lane, A. (2020, 11 18). *US-Europe Trade War Worsens, Could Trump Defeat Change That?* Retrieved from Forbes: https://www.forbes.com/sites/alasdairlane/2020/06/30/us-europe-trade-war-worsens-could-trump-defeat-change-that/?sh=7375942c66c7
4. Union, European. (2020, 11 18). *The EU in brief*. From https://europa.eu/european-union/about-eu/eu-in-brief_en
5. Zahariev, A., Prodanov, S., Radulova, A., Zaharieva, G., Pavlova, M., Angelov, P., . . . Marinova, K. (2020). THE BANK INSOLVENCY: FROM LEHMAN BROTHERS TO COVID-19 (INTERNATIONAL REMARKS AND NATIONAL PECULIARITIES). *58th International Scientific Conference on Economic and Social Development.* Budapest.
6. Zahariev, A., Prodanov, S., Zaharieva, G., Krastev, L., Kostov, D., Pavlov, T., Zdravkov, N. (2020, September 04-05). THE BROKERAGE INSURANCE COMPANIES UNDER COVID-19 FRAMEWORK (THE BULGARIAN EXPERIENCE). *58th International Scientific Conference on Economic and Social Development.* Budapest.
7. Заркова, С. (2018). Проблеми и предизвикателства пред страните-членки на еврозоната по изпълнение на критериите по процедурата при макроикономически дисбаланси. *Алманах "Научни изследвания на докторанти", 14*, стр. 26-55.
8. Нейков, П. (2020, 11 16). *„Пестеливата четворка" в ЕС: Трябва да се простираме според чергата си*. Retrieved from investor.bg: https://www.investor.bg/analizi/91/a/pestelivata-chetvorka-v-es-triabva-da-se-prostirame-spored-chergata-si-298792

THE PROFITABILITY OF THE BULGARIAN BANKING SYSTEM IN THE CONTEXT OF THE DIGITAL TRANSFORMATION

Zarkova Silvia
PhD, Part-time lecturer
The "D.A.Tsenov" Academy of Economics, Svishtov, Bulgaria
e-mail: silvia.zarkova@yahoo.com

Abstract
The banking system is essential for the functioning of a country's economy. The stability of the banking system is based primarily on maintaining profitability and good liquidity. Bank profitability is one of the most important issues for the economy of any country and its bank security. It has a significant impact on key economic measures, such as gross domestic product, disposable income, development of the business environment and etc. This imposes the need to consider the dynamics and trends in the profitability of the banking system. This study examines the dynamics and causal links in the profitability of the Bulgarian banking system, for the period: from the country's accession in the European Union to the country's accession in the forefront of the Exchange Rate Mechanism (ERM II). As a result, the trend in the profitability of the banking sector in Bulgaria is positive, despite the hardships, the country faces, during the period 2007-2019.

Keywords: *Bulgaria, banks profitability, banking system, European union, ERM II, digital transformation*

JEL Classification: *E42, G21*

INTRODUCTION

Subordinate to European economic cycles and the strong level of dependence on the development of processes in the euro area, the banking sector in Bulgaria was faced with significant changes in many respects. The low values of bank profitability have been repeatedly highlighted in reports of the European Central Bank [1], as a key risk to the stability of the financial sector in the euro area, which the country is striving for. After the inclusion of Bulgaria in the so-called waiting room of the euro area (ERM II) on July 10, 2020 [3], maintaining a stable banking system and good level of banking security in the country has become one of its main priorities. Striving for sustainable development of the banking sector [6] and maintaining good profitability, the effects of deviations from its optimal values can be significant. Low levels of profitability over a long period of time can have a significant impact on economic growth. At the same time, higher values [2] of above-average profitability can be considered a problem and an indication of financial stability and an impending financial crisis. Keeping banks within sustainable levels of profitability is key, provided that the aim is to maintain the stability of the whole sector. The digitalization of banking services is increasingly playing a significant role in the implementation of banking processes. The need to ensure security, speed and accuracy in banking services has grown sharply in recent years. In the payment statistics of Bulgaria, the number of non-cash payments has increased significantly over the years. The trend of turning traditional banks into digital is growing. Information systems and cybersecurity in the banking sector are extremely important. Automation and speed in operations are essential to meet customer demands, but the bank needs to meet both regulatory requirements and internal laws in their performance. In the Bulgarian banking system, the entry of digitalization of services is at an early stage. More significant penetration of digital services in Bulgaria is observed precisely after the country joins the European Union following the good European examples in the banking system. Some banks can be

classified as "digital champions", which provide a wide range of products and services in digital format (personal finance management; online opening/ closing a bank account; remote service; online transactions; repayment of debts on loans, payments, etc.), others still rely on traditional service methods. In addition to the wide range of digital products and services, the "digital champions" [4] are ahead of competing traditional banks in terms of return on capital and cost to income ratio, which is an important factor that compares the costs of current operations with related incomes.

STATE OF THE PROFITABILITY OF THE BULGARIAN BANKING SYSTEM

Bank profitability is directly related to the economic activity in the country, and is influenced by innovative approaches in the industry. Impaired economic prospects [5] can have a negative impact on it by reducing the levels of credit activity. Achieving a positive financial result, both in the banking sector and in any other business area does not in itself mean that there is an effective economic result. Indicative measures of profitability are the variations for measuring profitability. It is most often based on profit, assets and equity. The determinants of profitability according to [8] can be classified into indicators measuring the profitability of the business and indicators that calculate its efficiency. The scope of the report includes the fundamental measures of bank profitability - the cost / income ratio; return on assets and return on equity.

The cost to income ratio is a coefficient that measures the value of the costs necessary to generate income. The financial logic of the indicator is based on the statement that the lower the value of the ratio, the more profitable the bank's work. Respectively, the high ratios of the indicator show that the values of the operating bank expenses are high and it is necessary to take regulatory actions in order to prevent it. Reducing cost levels could be achieved through the capabilities of digital technologies and online banking. It is through them that the efficiency of banking processes can be increased, which will contribute positively to income levels. The values of the indicator around 70-80% are considered optimal [7].

The study of key measurable indicators in banking, incl. return on assets (ROA) gives an idea of the assessment of the credit and investment policy conducted by the banking system in the country. The ratio is calculated by dividing the net profit by the total average value of bank assets. Higher values of this ratio are a positive feature of banking management.

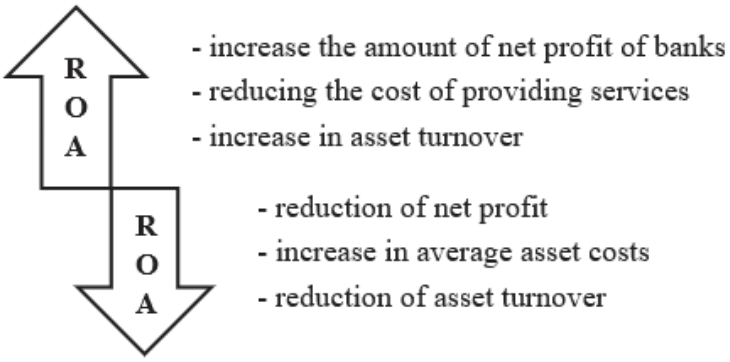


Figure 1. Effects of changes in return on assets (ROA)

Return on equity (ROE) is a measure by which one can track how effectively equity is used to generate profit. It is considered one of the most used indicators for assessing the

level of profitability of the bank. For the High values of the ratio show that the respective banking institution increases its ability to make a profit, respectively and vice versa.

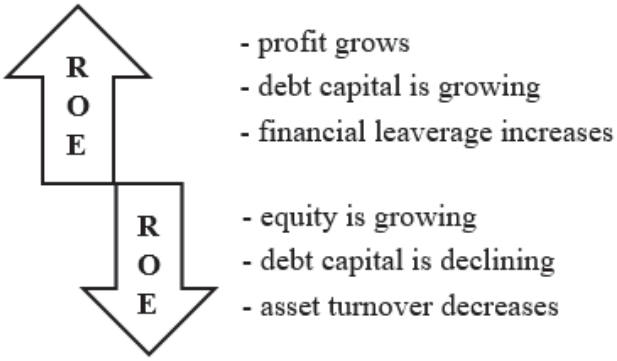


Figure 2. Effects of changes in return on equity (ROE)

It is considered that the normal limit of development of the ROA indicator is between 0.5% and 2%, and for the optimal value of ROE - between 10% and 20% [7].

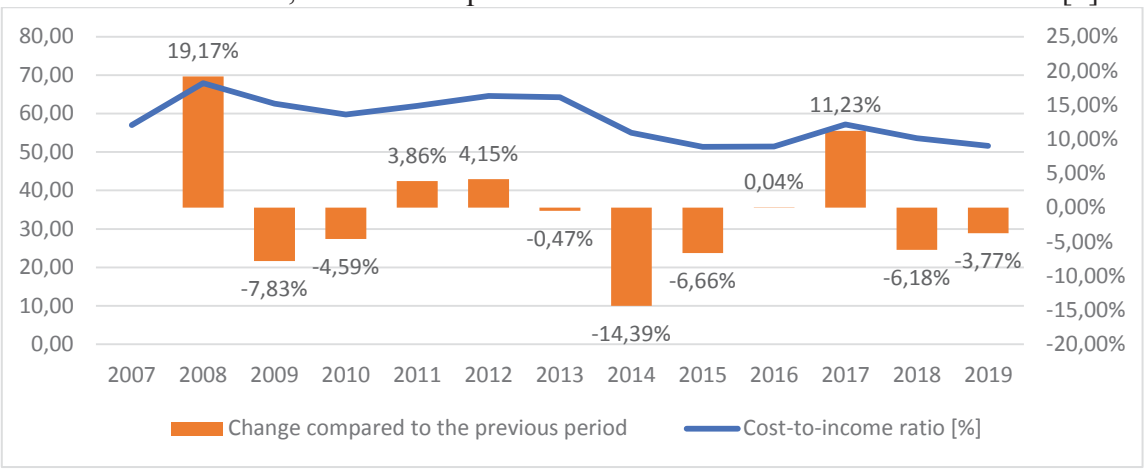


Figure 3. Cost to income ratio of the banking system of Bulgaria for the period 2007-2019

Source: European Central Bank (Statistical Data Warehouse) and author's calculations

Figure 3 can be observed the dynamics and the percentage change of the cost / income ratio, based on the net income from interest, fees and dividends, comparing them with the administrative costs in the banking system of Bulgaria for the period 2007-2019. As can be seen from the data (left scale) is that the coefficient ranges from 51% to 68%. The low values reflect the operational efficiency of the banking institutions. After 2008, there has been a gradual recovery of the sector, which has been affected by the effects of the ongoing global financial crisis. The gradual growth of income from banking operations after 2015 is primarily due to the growing income from banking operations. The classic measures of profitability - ROA and ROE are reflected in figure 4 and figure 5.

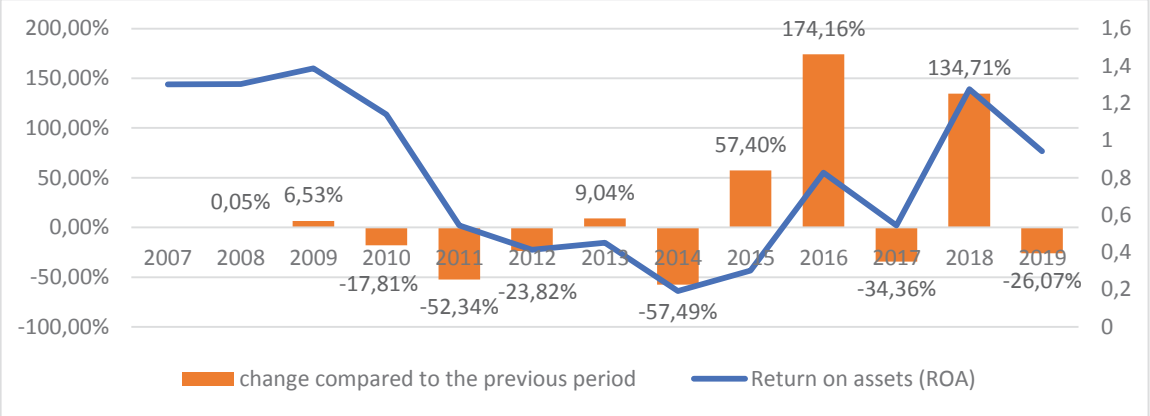


Figure 4. ROA of the banking system of Bulgaria for the period 2007-2019

Source: European Central Bank (Statistical Data Warehouse) and author's calculations

Figure 4 presents the profitability of bank assets. The dynamics of the indicator during the period shows the adherence of the banking system to the optimal values (right scale), except for the period 2012-2015 when the country is undergoing many political and economic processes, which have their negative effect. Banks often operate with significantly more borrowed capital than most other financial sectors. In this regard, when analyzing the profitability, attention should be paid to the ROE indicator, reflected in fig. 5. As can be seen from the figure (right scale) is the adherence of the indicator to the optimal limit of 20% in 2007 and its shaking in the period 2008-2015, which is due to a decrease in profit and to a greater extent the formation on a protective capital buffer in a large part of the banking institutions. In practice, the above two ratios express the ability of banks to turn their own capital and assets into profit.

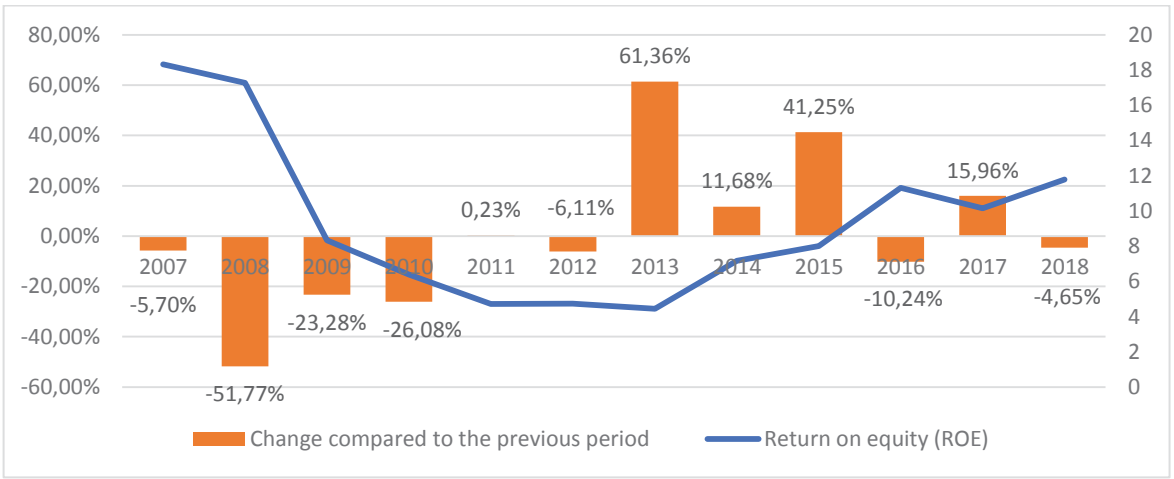


Figure 5. ROA of the banking system of Bulgaria for the period 2007-2019

Source: European Central Bank (Statistical Data Warehouse) and author's calculations

CONCLUSION

The trend in the profitability of the banking sector in Bulgaria is positive, despite the general decline in market interest rates in recent years. Given the country's accession to ERM II in 2020 and the current COVID-19 pandemic, the need for regular diagnostic analysis of annual profitability, cash flow, liquidity and solvency in order to comply with

European banking regulations and standards set in the European economic and monetary union. The profitability of the banking system reflects the economic health of the country. Given the current health crisis and the partial closure of the country's economy, bank profitability is expected to remain weak. As a key element of the country's economic system, the banking system is fundamental to helping the economy recover from the global pandemic, as many business customers will look for ways to finance and recover.

BIBLIOGRAPHY

1. Andreeva, D., Grodzicki, M., Móré, C. & Reghezza, A., 2019. Euro area bank profitability: where can consolidation help?. *Financial Stability Review*, November.
2. Cherowbrier, J., 2020. *Average bank cost-to-income ratios in Europe Q4 2019, by country.* [Online] Available at: https://www.statista.com/statistics/728483/cost-to-income-ratios-for-banks-in-europe-by-country/ [Accessed 02 11 2020].
3. ECB, 2020. *Communiqué on Bulgaria.* [Online] Available at: https://www.ecb.europa.eu/press/pr/date/2020/html/ecb.pr200710~4aa5e3565a.en.html [Accessed 2020 11 05].
4. Economy.bg, 2020. *Проучване: Българските банки са все още в начален етап на дигитализация на услугите.* [Онлайн] Available at: https://www.economy.bg/innovations/view/42113/Prouchvane-Bylgarskite-banki-sa-vse-oshte-v-nachalen-etap-na-digitalizaciya-na-uslugite [Отваряно на 15 октомври 2020].
5. Guindos, L. d., 2019. *Euro area banks: the profitability challenge.* [Online] Available at: https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190625~6d33411cff.en.html [Accessed 01 11 2020].
6. Zahariev, A. et al., 2020. *THE BANK INSOLVENCY: FROM LEHMAN BROTHERS TO COVID-19 (INTERNATIONAL REMARKS AND NATIONAL PECULIARITIES).* s.l., s.n.
7. Ангелов, П., 2016. Тенденции в развитието на финансовите параметри на банките в България. *Народностопански архив*, pp. 52-69.
8. Тодоров, Л., 2017. Доходност на бизнеса - методологични и приложни аспекти на анализа и контрола. *Анализ,* Том XXI

REVIEW OF THEORETICAL ASPECTS AND THREATS OF FINANCIAL SECURITY

Rousalinov Rousalin
PhD, Fellow
The"D.A.Tsenov" Academy of Economics, Svishtov, Bulgaria
e-mail: rousalin.rousalinov@gmail.com

Abstract
*Globalization has led to a significant change in the way economic and financial processes are carried out on a national and international scale between countries, companies, organizations and citizens from different parts of the world. Among the many changes that have taken place in the field of international finance are the introduction and use of the Internet and information and communication technologies as part of various business processes. At the same time, the issue of ensuring the proper protection of finances is of interest and is extremely important for today's environment. Building on a diverse literature this article examines the main views expressed in the economic scientific literature in the field of "**financial security**". By summarizing the various scientific studies in this area, we will reveal the main characteristics of the concept of **"financial security"**. **The main purpose** of the present paper is to study and review the theoretical bases of the term "**financial security**", to reveal its main characteristics and representations on different levels and on this basis to highlight the main threats that must be addressed in the coming years. **The research area** is the financial security both for governments and enterprises as well. In view of the above the author sets out the following **research tasks**: to outline the aspects, specifics and characteristics of the concept of "financial security"; to highlight current threats to the financial security of countries and enterprises. The complex and interdisciplinary nature of the topic predetermine the use of diverse scientific approaches and methods. The research applies a system of general scientific, theoretical and specific **research methods** - generalizing theoretical knowledge, logical analysis and summary analysis. The method of tabular presentation of characteristics is also used in the current scientific article. When forming the main conclusions of this research and interpreting the results, we used data from official sources for analysis of the considered processes. **The actuality** of the topic of this study is produced on the one hand due to the great importance of financial security for the economy, countries and enterprises, and, on the other hand by the need for further research in this economic and financial area. **The main conclusions and results** could be used to improve the financial security of different entities established in this paper.*

Keywords: *Financial Globalization, Financial Security, Enterprise Financial Security, Threats*

JEL Classification: *F3, F39*

INTRODUCTION

Globalization is one of the most important processes in today's social and economic national and international relations. Globalization is not e new phenomenon and is considered as a free flow of labor, capital and commodities in a very simple manner. It has affected different areas of world economy and the entities operating within it, but due to the specifics of this study, we will focus on one of the most important and key areas for every country, organization, corporation and enterprise in the world the financial sector with the focus on the issue of "**financial security**". The concept of financial globalization refers to the increasing interdependence of financial markets across national economies through a significant increase in transnational movement of financial instruments, services, capital, and information [8, p.5]. Financial internationalization can also be understood as the state and process of the financial activity of an economy participating in the financial activities of another economy across administrative divisions, or vice versa, the core which is "the process and state of financial integration in the world" [12, p.1]. Within the globalizing world economy, a country's financial system is attached to the globalization

process of financial institutions which have been contributing to global financial integration [8, p.5]. Globalization and especially "financial globalization" have led to a significant change in the way economic and financial processes are carried out on a national and international scale between countries, companies, organizations and citizens from different parts of the world. Financial globalization appears to be a recent phenomenon, dating from the end of the Bretton Woods System in the tumultuous years 1971 through 1973 and the increasing removal of capital controls by national governments worldwide since the 1970s [4]. It emerged in the seventies and developed during the 80s and the 90s as well.

Since its inception, it has become an ongoing process which is driven by many by many actors such as: governments, international financial institutions and organizations (International Monetary Fund, World Bank, European Union, International Finance Corporation, International Development Association, International Investment Bank and many others), national financial institutions, monetary authorities, private investors, banks and enterprises. As a result of the financial globalization world economies became more tightly integrated, which led to other changes in the field of international finance such as:

- increase in economic and financial interdependencies;
- creation of a global financial market;
- creation and dominance over the global economy by multinational corporations;
- creation of the intellectual services sector;
- intensification of activities conducted by international economic organizations;
- removing of borders in the field of international monetary relations;
- development of new technologies;
- access to a new domestic and foreign markets;
- expansion of off-shore companies;
- rising cross-border capital and payment flows;
- elimination of other boundaries in financial sector;
- increasing share of cross-border holdings of assets;
- rapid progression of foreign trade;
- establishing new rules and regulations among the many participants in the different operations;
- intense competition in different areas;
- increase intensity of foreign direct investments (FDI);
- market integration became more easily;
- many others.

Over the decades, the world has witnessed massive growth in financial markets both in terms of their scale and scope. The world financial assets - or the value of equity market capitalization, corporate and government bonds, and loans - grew from around $12 billion in 1980 to $206 trillion in 2007 [18, p.2]. Financial depth, which measures those assets relative GDP, rose from 120% to 355% of global GDP over the same period [18, p.2]. Another statistic shows that the average daily turnover of the foreign exchange market more than doubled from $1.5 trillion in 1998 to $3.2 trillion in 2007 [7, p.68]. The world of international finance is global, filled with opportunities for financing, investing, business combinations and currency dealing [20, p.5]. The economic developments during the last decades show a growing importance of services for both developed and developing economies [32, p.273]. Financial products and services became vital for survival of different entities, businesses on national and international scale.

Financial world is constantly changing due to the fast-growing use of different technologies. In the European Union alone, financial sector is the largest user of digital

technologies and plays a major part in the digital transformation of the Union. Continuous modernization of the global financial sector since the beginning of this century is one of the other outcomes from the globalization and internationalization processes. This is helping not only countries, but enterprises across the world to achieve more economic and financial stability and growth. It influences and has a beneficial effect on national, regional and global economic interactions, partnerships and cooperation for the development of global market spaces. The advancement of digitalization and computerization resulted in growing use of computers, laptops, mobile devices and networks for managing various financial operations during the different parts of the day. It is considered that these technologies are the main vectors and drivers of globalization in the financial sphere. Over time, they have facilitated access to resources, strategic partnerships, knowledge, advanced technologies and increased business opportunities on the international markets [23, p.80]. For example, today there are financial markets that are working around the world without a break (for 24 hours) - financial transactions, deals, investments and many other operations are finished much more quickly than before the time of these technologies were introduced to the business world environment. Advances in information and communication technologies have made it a lot easier for market participants and countries to collect, store, process and send information, documents and data they need to manage, monitor, analyze financial risk and to manage large sums of transactions spread across international financial centers throughout the globe. Another advantage is that as a result of all of this processes cross-border financial deals have become both easier and more secure and with a lot more participants than ever before, effectively lowering the barrier constituted by distance, be it determined by geography or other factors. Modern information technology is one of the hallmarks of the knowledge economy [10, p.22]. It is the most permeable, most widely used, most efficient, and most rapidly developing high-tech [10, p.22]. Internet finance have become one of the most used methods for different financial operations such as: financing, transaction payment and financial intermediary. It has two main characteristics. First, relying on big data, cloud computing, search engine and other network technologies, it carries out multi-dimensional collection of financial data information, mining customer information through data analysis, and realizing in-depth use of data [14, p.486]. Second, in this field a large number of big data platforms are used for data cleaning, data mining and analysis, and the processing results are more widely used, risk control data measurement, and assist business precise promotion activities [14, p.485]. There are number of studies that shown the importance of digital technologies for today's finance world. For example, around the world, digital lending companies are emerging and growing. They offer digital loans through mobile phone apps or via websites, including those that are optimized for mobile [24, p.1]. According to IMF digital financial processes have grown in recent years. Digital lending to SMEs and to individuals via online platforms, grew by 57% from a combined value of $143 billion in 2017 to $225 billion in 2019 [15, p.3]. The number of digital loans grew from 53.2 to 62.6 million between 2017 to 2019 [15, p.3].

Financial globalization also leads to a change in economic models, policies, strategies and activities of governments and corporations in our internationalized environment. Other benefits include more intensified competition between the different entities, introduction and implementing new financial products and services, the opportunity to restructure or reposition a weakly-performing financial institution or business unit, creation of new multinational companies, creation of new classes of non-bank financial institutions, creation and adaptation of new sets of rules and regulations and many others. Financial globalization has brought considerable benefits to national

economies, national and international corporations, investors and savers, but it has also changed the structure of markets, creating new risks and challenges for market participants and policymakers. One of the main challenges of financial sector nowadays is the area of "**financial security**". It is a topic of vital importance for governments and enterprises especially in today's complex economic and political environment. In addition, the issue of financial security and how it affects the development of countries and companies is crucial if we want to know how governments and enterprises control this problem. That is why we focused on the topic of financial security, because along with the increasingly advanced integration of financial processes, this is an increasingly pressing problem to be solved. The issue of ensuring the proper protection of finances is of interest and is extremely important for today's environment. **The main purpose** of the present paper is to study and review the theoretical bases of the term "financial security", to reveal its main characteristics and representations on different levels and on this basis to highlight the main threats that must be addressed in the coming years. **The actuality** of the topic of this study is produced on the one hand due to the great importance of financial security for the economy, countries and enterprises, and, on the other hand by the need for further research in this economic and financial area. The research area is the financial security both for governments and enterprises as well. In view of the above the author sets out the following **research tasks**:

- to outline the aspects, specifics and characteristics of the concept of "financial security";
- to highlight current threats to the financial security of countries and enterprises.

1. IMPORTANCE OF FINANCIAL SECURITY FOR TODAY'S GLOBALIZED WORLD

Financial security has a significant economic importance to countries, companies and people all over the globe. The globalization that took off since the second half of the last century broad an unprecedented growth in the events happening at international political and economic arena. It's one of the main drivers for the condition of financial security and the state of financial systems. Today the contemporary world is basically a global environment. This means that the world is very closely connected, and the actions of some entities depend upon the actions taken by the other entities. This can have a positive or a negative effect. For example, a positive effect are the creation and establishment of the use of millions of connected devices across the globe through the use of internet (computers, laptops and mobile phones) on the one hand and on the other the financial crises started in one point of the world and affected all participants in it. In nowadays no economy can be fully independent on its own. The constant transformation of the global economy and its constantly structural adjustment is the source of new threats to the development of economic systems. A large part of them has a financial origin given the account the importance and increasing role of financial relations across the globe. The development of an international economy and the expansion of world economic and financial relations create new specific challenges to the economic security for governments and national and international entities. One of the main parts of the economic security of each country and enterprise is the "**financial security**". It is one of the main factors for competitive and sustainable development of each country and corporation in our globalized world. The high level of "financial security" both at state level and at the level of business entity is a condition of its economic and social development and is a guarantee of a strong position at the global economic arena. At the same time "financial security" is extremely vital for the different business as well.

There aren't a country or entity in the world that can effectively implement its domestic or foreign policies without integration of financial policy with its economic interests. One of such interests in the period of economic instability and crises in different areas including the financial ones even in the most development countries are by the provision of financial security at different levels. In the ecomic and financial literature the issue of "financial security" is view on different levels, but for the purpose of this paper we will closely analyze the two main ones – "countries financial security" and "enterprise financial security".

2. THEORETIC ASPECTS OF FINANCIAL SECURITY – DEFINITIONS, TYPES AND THREATS

Financial security in the economic, financial and scientific literature is analyzed from different points of view, but the two most important ones are the "financial security of countries" and "financial security on enterprises". In this section of the paper we will analyze both of them and we will reveal the main views about what is behind the interpretation of these two terms, as special attention is given also to their main characteristics, factors and most importantly their threats.

2.1. FINANCIAL SECURITY OF COUNTRIES (STATES)

Given the relevance of this issue for today's world in the modern scientific literature, one can find numerous scientific papers devoted the definition of the concept of "financial security". In the scientific literature the term "financial security" on a country level is viewed as one of the most important components of the state's economic security in a market economy. In the modern and connected world, that we all live in, the problem of financial security is one of the most important and urgent ones for the development of countries. It is a complex concept that consist of different elements. As scientific category financial security, can be analyzed on three basic levels (tab.1). One key characteristics of countries are that national governments are major borrowers on both the domestic and international capital markets [31, p.2383]. This is very important when we analyze financial security as well and we have to know it.

Table 1. Main types of financial security

Nano financial security	This is the financial security of the citizen or individual of each country.
Micro financial security	This is financial security of economic entities (firms, companies, enterprises or others).
Macro financial security	This is the financial security of different countries or states.

Source: [29, p.11]

According to Natalia Zachosova the term "financial security" of the country means the ability of the mechanism of management of the state financial system to guarantee the maximum level of satisfaction of national and private financial interests, avoiding the conflict between them [29, p.4]. In order for a country to be competitive on a global scale, to have a strong national security and to attract more foreign investors it has to have a very good financial security. Another view of "financial security" is that it is such a state of financial resources and capabilities of the country, which are formed in its financial system or are attracted from the outside, which allows to ensure the implementation of national financial interests and financial interests of citizens and business entities by guaranteeing

its protection against external and internal threats that can interfere with their efficient use (resources and capabilities) in various segments of the financial system [29, p.8].

In addition to that understanding of this concept we find another very broad one in the article made by Galina Pochenchuk. According to her this economic and financial term have to be understood as conditioned by the ability of public authorities provide sustainability of national financial-economic development and payment-settlement system, observance of basic financial economic parameters of national economics, optimal allocation and rational utilization of budgetary resources as well as by the ability to make external borrowings optimal for the national economy and effectively utilize them, neutralize the influence of financial crises and deliberate actions of international (states, TNC, interstate formations) and national (clannish-corporate, mafia structures) economic agents on the national economic and social-political system, prevent the outflow of capitals abroad, crimes and administrative delinquencies in the financial area [19, p.32]. It highly depends on how efficient are the policies of governance and their implementation by its institutions, firms and citizens. It is the state of national financial system where necessary financial conditions for the stable social-economic development of the country are created, its sustainability to financial shocks and disbalances is provided, conditions for maintenance of its integrity and unity of national financial system are created [19, p.33]. Dmitriy Bezzubov define the financial security as part of the national security, which forms the economic direction of countering threats and dangers in the sphere of economics and finance [1]. It is vital for every country, because it is a condition for its ability on the one hand to carry out independent economic and financial national and international policies, and on the other they have to be in the line with its own national interests. Studying different publications, articles, books and researches on the topic of financial security we find out that it is a vital part and element of countries national security as well and has a significant impact on the level of economic growth in the country. It is also a key factor for the security of every person. It is multifaceted phenomenon: first it is a component of economic security, and, second, it is a subsystem of national security [11, p.305]. At the same time, financial security is a complex multi-level system, which is formed by several subsystems, each of which has its own structure and logic development [11, p.305].

Financial security is defined also as a whole range of legal regulations and self-regulation aimed at ensuring financial stability and protecting the interests of market participants using financial intermediaries, as well as all institutions responsible for controlling compliance with these regulations and self-regulation [17, p.48]. On the next table we systemized other approaches than are used when defining this economic term. They are important in order to understand its main characteristics (tab.2).

Table 2. Main approaches for understanding the term "financial security"

Approach	*Essence of the approach*
Classic (traditional)	Financial security is the state of the financial system, the level of financial resources and the level of protection against financial dangers and their consequences
Systemic	Financial security is a system of elements aimed at ensuring the implementation of financial rights and obligations of participants in financial relations
Focusing on the interests of stakeholders	Financial security is the ability to achieve the maximum satisfaction of financial interests of all categories of security object stakeholders
Resource	Financial security is the availability of sufficient financial resources of the same quality that meets the financial needs of the security object and allows to finance the fulfillment of the achievement of the goal of creation and functional tasks and to ensure sustainable development in the long term
Multi-level (structural)	Financial security is a component of a higher order system – economic security that has a complex structure and encompasses several levels of subsystems
Risk-oriented (threat-oriented)	Financial security is a successful result of taking measures to manage financial risks; the safety of the financial condition of the security object from the negative impact of external and internal threats and risks.
Complex	Financial security – a set of measures aimed at ensuring the stability and functional capacity of the pre-formed financial security system
Mixed	Combines the basic provisions of all or several of the following approaches

Source: [29, p.12-14]

Another very important vision of national financial security is that it is defined as the state of the economy, which ensures the formation of sufficient financial resources of the state in the volumes necessary to fulfill its tasks and functions with appropriate control over their legal formation and expenditureb [25]. When interpreting what financial security is for countries it can be seen as the main condition for the ability of the state to carry out independent financial and economic policies in accordance with its national interests or the state of the economy, which ensures the formation of positive financial flows of the state in the volumes necessary to fulfill its tasks and functions [25, p.161]. It can be defined also as the state of financial relations in which acceptable conditions and necessary resources are created for expanded reproduction, economic growth and growth of the population's well-being, stability, preservation of the integrity and unity of the state's financial system, and for successful opposition to internal and external factors destabilization of the financial situation in the country [25]. It's important to outline that, when we are analyzing the financial security on a state level from a theoretical point of view, the review of the development of financial systems allows us to identify **two principal sources of state revenues**: **taxes and loans** [30, p.5]. Theoretically, the use of loans is expressed as a specific movement of money among the state, companies, banks, financial institutions and households – a movement that is associated with the activities of governments as borrowers of monetary capitals [30, p.5]. Financial security of the state consists of different

elements or components **such as**: monetary security, security of the banking system, debt, budget and currency security, tax security, foreign exchange rate security, security of the insurance services market, security of the stock market and investment security. On the next Table we outline the main characteristics of these very important economic elements (tab.3).

Table 3. Main elements of state financial security and their definitions

Elements of state financial security	*Definitions*
Budget security	The ability of the budget system to ensure the financial independence of the state and the effective use of its budget funds in the process of performing its functions.
Debt security	Is a level of internal and external public debt that provides an effective solution to the general needs of the state and ensures its relative independence, the possibility of repayment of the principal amount of debt and interest without threatening the loss of sovereignty, solvency and credit rating.
Tax security	Determined by the effectiveness of the tax policy of the state, which should optimally combine the fiscal interests of the state and individual, corporate interests of taxpayers, or provide the state with such volume of tax revenues that is optimally necessary in accordance with the requirements of the proclaimed economic doctrine.
Monetary security	Is a state of the monetary system characterized by the stability of the monetary unit, the availability of credit resources and the level of inflation that provides economic growth and increase real incomes.
Security of the banking system	Is the ability of the banking system to secure the financial independence of the state in a stable and secure manner, to effectively perform its functions, to preserve from excessive depreciation and to use the financial resources of the country rationally to ensure its socio-economic development and maintenance of financial obligations.
Investment security	The level of investment that allows state optimally meet the current needs of the economy in capital investment by volume and structure, taking into account the effective use and return of the funds invested, the optimal balance between the amount of foreign investment in the country and domestic investment abroad, maintaining a positive national balance of payments.
Security of the insurance services market	The level of insurance companies' financial resources providing them with the opportunity to compensate losses if necessary and to ensure a stable financial position of the market participant and its efficiency and strategic development.
Security of the stock market	The optimum volume of its capitalization that is capable of providing a stable financial position of issuers, owners, buyers, trade organizers, traders, joint investment institutions, registrars and the state as a whole.

Source: [22, p.227]

We outlined that there are also other elements for the financial security of states **such as**: non-banking financial security sector, food security, social security, energy security and demographic security. They are as important as the ones that are established above. As we can see financial security is a complex concept. We found different

explanations of the term in order to understand its main characteristics. We also highlight its main elements which are very important for every country in the world. In order to fully understand this economic concept, we have to present its main threats. In the scientific literature the main threats which are threatening the financial security of the states are divided in two main groups internal and external (tab.4).

Table 4. Internal and External financial security threats

Internal threats	*External threats*
• Security of the financial system; banking system; financial markets; • The appropriate level of indebtedness of entities (cash and credit security); • Security of public finance; • Ineffective regulation of the financial sector; • Insufficient level of gold and foreign exchange reserves; • Reduction of investment and innovation activity; • The imperfection of the tax system and tax evasion; • Budget deficit; • Shadowing and criminalizing the economy and in particular the financial sector; • Condition of the state securities market; • High level of corruption; • Illegal outflow of capital from the country; • Large amounts of public debt; • Underdevelopment of the financial and insurance markets; • Low level of capitalization of the banking system; • Trade balance • Balance of primary incomes	• Changes in the balance of payments; • Foreign debt; • Official reserve assets; • Political instability in the country; • High level of internal and external debts; • Permanent deficit of the state budget; • High level of inflation and shadow economy; • Deep dependency on foreign creditors; • Changes in the conditions of foreign trade and world prices; • Growth in financial debt and increased value from foreign loans; • Increased competition in world markets; • Rapid progression of globalization;

Source: compiled by the author[1]

Financial security is a country's ability to resist various internal and external threats and attacks within financial development, ensure the financial system and financial sovereignty are not violated, and enable the financial system to maintain normal operations and development [13, p.19]. In order for a country to avoid or reduce the risk of the existence of these or other internal and external threats to its economy it must develop very good strategy. The strategy should include specific goals and objectives for ensuring financial security of the country to be on the one hand in accordance to its economic and social development in short and long term, and on the other to be in line with the country's international goals in order to formulate an effective mechanism to counter the financial security threats. We have to say that external and internal financial security threats are the

[1] *Note: The table is created by the author and the information in it is summarized from different official resources (published articles which are shown in references section of this paper).*

most important groups, but there are others. According to Natalia Zachosova they are: **by the nature of occurrence** (political; criminal; competitive; economic; market and technological); **by duration of action** (permanent and temporary (short, medium and long-run)); by nature of origin (macroeconomic trends; force majeure circumstances (political crises, military actions); low level of efficiency of financial system regulation; changes in legislation or its lack in certain issues; ineffective pricing policy; non-compliance with economic and prudential standards; low quality of financial products and services; money laundering and many others [29, p.58-59]. Each of these threats and the level of financial security of the states and neutralize them can be very hard thing to do. Countries have to use variety of methods which can give different results based on the quality of the measures that are taken. Every country uses its own methods which reflect on the development of the financial system.

In summary of this chapter of the paper we can say that financial security is very complex economic term. National financial security requires solving of a wide array of issues which all depend on the current circumstances on the domestic and global scene. The level of financial security of a country is an important characteristic that reflects the state of its financial system. The level of financial security of a country is an important characteristic that reflects the state of its financial system. Financial security depends on many factors, which can vary significantly, because countries have different economic development. It is also a vital part of the country's national security. The activities on the financial security of the state involve all entities: individuals, legal entities and state itself. The financial security of the state is one of the most important condition for its ability to carry out independent financial and economic policies in line with national and international interests. The security of any economic system depends on the influence of many factors of external and internal environment of its functioning, which define the parameters of the overall economic development system as a whole.

2.2. ENTERPRISE FINANCIAL SECURITY

In the modern world that we all live it is impossible to exist without finance, financial relations, and enterprises. Enterprise financial security plays a big part for the development of every country in the globe. Enterprises are the drivers of the global economy. They are the key and backbone to the economy of various countries. Their impact and contribution to the growing number of employments, trade and production of different products is very well documented in countless studies in the form of reports, articles, books and dissertations. Their development and growth depend on the access to finance from different resources that are provided by the governments. It is a major hurdle in their development. One of the largest groups of enterprises in the world are the Micro-, Small and Medium enterprises (MSMEs). According to data provided by the United Nations (UN) on a global scale formal and informal they make up over 90% of all firms and account, on average, for 70% of total employment and 50% of GDP [26]. These types of enterprises are responsible for significant employment and income generation opportunities across the world and have been identified as a major driver of poverty alleviation and development [26]. Only in the European Union there are around 23 million small and medium-sized enterprises (SMEs) in the 27 Member States. They collectively employ nearly 100 million people, make-up more than half of EU's GDP and play a key role in adding value in every sector of the economy. They represent a significant part of the private sector. Around 99% of all European companies are part of this group and are very important not only as engine of job creation, but for the increasing of innovation, competition, prosperity, as well as economic and technological sovereignty and resilience

to external shocks of EU. In the EU SMEs provide two-thirds of total employment in the Union [9, p.5]. They're variety is huge, from innovative and fast-growing companies that provide or use digital solutions, to those that face significant challenges such as acquiring the necessary skills to benefit from digital technologies [9, p.5]. They represent and are part of various sectors such as: chemical production, electronics, agriculture, construction, coal and oil production, food industry, manufacture of tobacco products, production of clothing and many others. In modern conditions, they have to deal with a number of challenges and a lot of them are in the field of "financial security". Every business micro, small, medium or large depends to a large extent on the positive results of their activities, which cannot be achieved without proper financial security. The essence of every business is described by the principles which govern its activities – the ability to generate profit, its functioning in the conditions of risk, and entrepreneurship [16, p.3]. The characteristics of a company's activities, being its targets, include innovativeness, effectiveness, development and value creation. In the process of achieving these objectives, a company is subject to the influence of the environment and the internal processes which it consciously creates, how it manages them.

In the scientific literature the term "enterprise financial security" has different interpretations by the scientists. According to Vitalina Delas, Euvgenia Nosova and Olena Yafinovych enterprise financial security can be defined as financial position of enterprise that is characterized by the balance of financial interests and the ability to ensure their implementation; resistance to the negative impact of internal and external threats of company's environment; and the ability to provide financial equilibrium and sustainable financial stability of the enterprise in the short and long run [6, p.253]. Another view of this concept is that it is considered as the dominant component of the economic security, on which depends the effective financial and economic activity of the business entity [21, p.232].

Financial security of business entities is part of state's financial security. The main reason for that is because companies creates added value which forms the GDP at the state level. In addition to that enterprises are major taxpayers, which influence the formation and level of revenue of the countries on national and local level. It is very important for any type of company from small to large. Another view of this term is that it is a condition where firms have necessary resources in the face of possible risks and dangers that they have anticipated [5, p.299]. In this sense, financial security is a very important factor that should be effectively managed by firms because lack of resources can cause many negative situations. Financial security of the enterprise can be defined also as a constituent part of economic security of the enterprise, which defines the process of development of the enterprise on the basis of certain financial resources, sufficient structure of the capital, which is used by the company, compliance with the targets and missions on the basis of the level of the internal and external threats, certain factorial influence in the changeable current and future periods of development [2, p.251]. A we already established there are numerous scientific views of this concept that can be found in the economic literature (tab.5).

Table 5. Definitions of the term "enterprise financial security"

Author	*Definition*
Baranowski A.	Degree of defendance of financial interests at all levels of financial relationships or level of financial resources support which enough to meet enterprise's needs and to fulfill existing obligations.
Blank I.	Quantitatively and qualitatively determined level of financial position of the company, which provides a stable security of its strategic and balanced financial interests from identified real and potential, external and internal threats, parameters of which are determined on the basis of its financial philosophy and which are creating the necessary preconditions of financial support of its sustainable growth in the current and future periods.
Vankovych D.	The company's financial security is an absence of financial danger to the enterprise, successful management of its operating, financial and investment activities.
Goryacheva K.	It is a financial position of the enterprise which can be characterized: firstly, by balance and quality in a set of financial tools, technologies and services used by the enterprise; secondly, resistance to external and internal threats; thirdly, the ability of financial system to ensure the implementation of the company's financial interests, goals and objectives with sufficient financial resources; fourthly, to ensure the development of the entire financial system.
Melnik L.	Financial security is a component of internal economic security of enterprise which linked with ensuring of its financial stability and financial risk neutralization. It isn't an independent object of management.
Muntiyan V.	It is a state of the most effective use of information, financial indicators, liquidity and solvency, return on equity, which are within its limit values; quality of management, use of fixed and current assets, its capital structure, norms of dividend payments on securities and market value of its securities as a synthetic indicator of the current financial and economic standing of the company and prospects for its technological and financial development.
Papehin R.	The ability of company to design and carry out financial strategy in accordance with the general purposes of corporate strategy in an uncertain and competitive environment.
Pokropyvnyy S.	Financial component is considered to be a leading and crucial among all other functional components of economic security (financial, intellectual and human resources, technical, technological, political, legal, informational, environmental, power), because finances is an "engine" of any economic system under market conditions.

Source: [6, p.253]

Considering the definition of the company's financial security, given by different scientists, we can identify the key characteristics of that category. **First**, it is part of the economic security of the enterprise. Economic security of economic entities is the state of the most effective use of their corporate resources – own, borrowed and involved, in conditions of influence on their quality and integrity of external and internal threats in the process of realizing the economic interests of the entity itself and all categories of its stakeholders [29, p.54]. **Second**, it helps firms to their efficient activity on the market they operate in. **Third**, provides a stable security of its strategic and balanced financial interests from external and internal threats. **Fourth**, it allows enterprises to identify problem areas in enterprise's activity at early stages. The **main goal of the financial security of every enterprise** is to provide the most stable and efficient current existence of the company in present and to ensure a high potential of its development and growth in the future [6, p.254]. In order for an enterprise to have a high level of financial security it must have a

very specific goals that must be followed by each structure in the company. In the next table we provide information how this can be done by the different management areas in the company (tab.6).

Table 6. Management of financial security on an enterprise level

Areas of management activities	*The task of providing financial security*	*Influence on financial security*
Financial management	Search for sources of financial resources and their effective use to secure financial autonomy.	Identification of unprofitable, idle assets.
Risk Management	Identification, assessment of financial risks and formation of measures for their minimization and counteraction to their consequences.	Assessment of liabilities at the level of risk, the formation of a secure structure of liabilities.
Human Resources Management (HR)	Ensuring the reliability and loyalty of the staff that has access to financial data and makes decisions on the areas of financial and investment activity.	Identification of risks, compensation of financial consequences of their influence.
Innovation management	Attracting innovations to improve the financial security system, assessing innovation risks.	Observance of normative values of liquidity indicators.
Manage changes	Assessment of potential threats from introducing changes, forecasting their positive consequences for the level of financial security.	Compliance with normative values of indicators of financial stability.
Investment management	Assessing the appropriateness of investments from the point of view of their impact on the state of financial security.	Determining the minimum size of capital to maintain financial security, assessing its value from different Sources.
Anti-crisis management	Counteraction to financial manifestations of crisis phenomena.	Support for incoming financial stream level higher than outgoing.
Strategic management	Establishing strategic guidelines for security oriented financial development.	Minimization of losses from the actions of competitors, counteraction to industrial espionage.
Marketing management	Support of solvent demand for goods and services of an entity.	Support of the financial security of the branches, separate structural subdivisions.
Information management	Increasing the level of trust in the company by ensuring information transparency of financial data; preventing the use of insider financial information for other purposes.	Minimizing the level of financial debts, monitoring the timeliness of settlements.
Sanitation management	Search for financial resources to take measures to minimize the threat of bankruptcy.	Take measures to prevent loss of profit, its failure to receive or ineffective use.

Source: [29, p.56-57]

Financial management of every enterprise plays and important role in ensuring financial stability and security in short and long run periods of time. It's one of their main

activities in order for the enterprise to be successful, to achieve its goals and to be better than its competitors on the market or markets their operate in. Its primary goal is to use, distribute and control the financial resources in most effective way. There are curtain objectives that must be achieved by the structures of the company. For example, they can be [21, pp.232-233] :

- ensuring financial stability and independence;
- ensuring high efficiency of financial and economic activity;
- achievement of high competitiveness in the market of goods, works, services;
- ensuring high liquidity of assets and raising the market value of the enterprise;
- support for the appropriate level of business activity and image;
- formation of information security and business secrets;
- effective organization of security of own capital and property of the enterprise.

In order for enterprises to have high level of financial security curtain steps must be applied in this process [33, pp.164-165] :

1) Monitoring of financial security – implementation of this measure involves collection, analysis, evaluation and prediction values of indicators of enterprise financial condition;
2) Definition of strategies and measures to prevent the action of threats to enterprise financial security – determination the ability of the enterprise to counteract threats on the basis of strategic analysis, evaluation the ability of companies to accumulate their own and borrowed resources to prevent crises, develop and evaluate measures aimed to leveling risks and threats to financial security during this stage;
3) The implementation of strategies and measures to prevent and neutralize threats of internal and external environment on the level of financial security.

In addition to that there are other steps than can be implement by the enterprises like: *planning measures to protect the financial resources of the enterprise and its customers; diagnosis of the level of financial security (low or high); determination of the list of areas of financial activity that need to be optimized; develop measures to improve the level of the lowest financial security indicators; budgeting and fundraising security-oriented activities; implementation of a two-tier mechanism for financial security management: strengthening the level of financial resources of the institution to achieve its financial goals and enhancing the level of protection of financial assets of clients to ensure their financial interests; comparative cost analysis for security-oriented measures and the size of the prevented damage from the impact of financial threats, hazards and risks; diagnostics of the level of financial security after the taken measures (low or high); review of strategic benchmarks for financial security* [29, p.69]. When analyzing the enterprise financial security on a company level, we have to know that there are certain types of threats that they have to manage. There are many groups of threats that can affect the company's development. For example they can be: ***internal*** *(consisting of forces and factors related to organizational structure, economic capacity, geographic boundaries of company's activity, finances, management and marketing);* ***external*** *(which consists of the factors which the company interacts with);* ***permanent*** *(they affect the company's activity constantly (scientific and technical progress, the quality of informational support, energy and environmental issues, state and interstate regulation, exchange rate and monetary system, etc.) and* ***temporary*** *(they affect the company's activity within limited period of time (seasonality, political and social conflicts, natural disasters)* [6, pp.257-258].

Threats also can be classified in other groups such as: ***depending on the subjects***: threats from unfair competition; threats from the buyers; threats from other contractors; threat caused by the employees; threats from criminal organizations; threats caused by the actions of State officials and local authorities; ***ability of realization:*** real and potential;

depending on the object of attacks: financial and informational; ***forms of manifestation:*** quantitative threats (associated with underfulfil of plans deterioration in the financial position and payment discipline and qualitative threats (related to changes that can't be quantitatively measured, namely the financial crisis, bankruptcy, corporate conflicts, falling market, freezing of bank accounts, closure of foreign markets) [6, p.259]. Of course, they can also be divided into other groups which are presented on the next table (see Table 7). There are different external and internal threats according to the type of enterprise. For example external threats can be divided into: ***budget and tax (increasing fiscal pressure on an industrial enterprise; instability of fiscal legislation); credit (increase in interest rates on loans; financial market instability); insurance (increase of insurance tariffs; delays in insurance payments; insurance fraud)*** [9, pp.59-60]. There are also different internal groups of threats such as: ***cash (decrease in sales revenue; lack of own working capital; violation of the organization of saving money) and stock (sub-optimal distribution of profit between consumption by owners and reinvestment of it in the assets of the enterprise; inefficient dividend policy of an industrial enterprise)*** [28, pp.59-60].

Table 7. Types of enterprise financial security threats

Sources of threats	*Possible ways to diversify the risks of negative scenarios*
Internal and external: conscious/unconscious actions of officials or subjects (state or municipal authorities, counterparties/competitors, international organizations)	High management efficiency, development of the corporate governance system, optimality of the enterprise organizational structure
	Ensuring a high level of education and qualification of staff
	High-quality legal protection of all aspects of the enterprise
	Enterprise staff security, its capital and property, commercial interests.
External: a combination of circumstances: the financial situation on the market for the sale of products of this enterprise, scientific discoveries and technological developments.	High competitiveness achievement due to technological independence.
	Ensuring environmental safety through minimizing the destructive impact of production results on the state of the environment.
	The information field and commercial secrets protection.

Source: Reshetnikova, N., Magomedov, M., Buklanov, D., Zakharchenko, E.(2019). The international business cooperation and its influence on enterprise financial security under globalization, p.299

Internal threats can be divided on the following subgroups: ***competitive*** *(stage of the enterprise life cycle; certain traditions, reputation and image; market share);* ***organizational*** *(enterprise pattern ownership; organizational form of production; enterprise adaptation to the external environment; specialization and concentration form of production; diversification of production; absence or inefficiency of financial planning and control);* ***financial*** *(balance sheet structure, efficiency of asset and capital management; risk level of the funding policy; balance of cash flows; policy effectiveness of profits use; diversification of financial activities; risk level of financial investments portfolio; profitable level of investment projects; amount of reserve and insurance funds; effective work with customers; efficient credit policy of the company;* ***marketing*** *(matching of marketing strategy and market policy; product portfolio policy; pricing policy; competitive level of products; the effectiveness of marketing communications; effectiveness of marketing policy; level of marketing costs);* ***innovation*** *(low level of innovation activity; progressivity level of production tools; level of product resource intensity; lack of diversification of production);* ***information*** *(perception and search for new information; ability to synthesize and analyze data; ability to draw conclusions and to retain*

information); ***related to resources*** (*satisfied technical and technological level of production; depreciation of fixed assets; level and structure of costs; capacity utilization; work-cycle time; level of inventories; level of working capital*).

External threats are also divided in different subgroups such as: **international** (*level of cyclical economic development; development of international marketing; profitability of international agreements; transforming process in the banking system; decisions or actions on the part of individual foreign States (the economic blockade, embargo*); **national** (*financial system status; efficiency of economic legislation; political stability; efficiency of the development mechanisms of the country economic policy; level of financial and economic policy of the country; footprint of economic crime and corruption; level of tax rates; currency fluctuations; inflation; national currency stability; favorable investment climate; development of the financial infrastructure; availability of natural resources; energy dependence; effectiveness of the implemented reforms; level of fundamental legal principles of entrepreneurship; level of regulation of the currency and customs policy; efficiency of statutory instruments of monetary and fiscal policy*); **market** (*variations of consumer choice; skills, traditions and norms of consumption; cultural consumption values; development of scientific and technological progress; technical and technological structure of domestic enterprises; competitive level of domestic products; level of production costs; quality level of raw materials; availability of credit resources; inflation level; level of export and import policy; efficiency of regional business policy; product quality level (product manufacturing according to the state standard requirements) and domestic markets enthusiasm as for other countries producers*). As we can see there are a lot of factors that are influencing the development of an enterprise. We can say that one of the most important ones are the level of efficiency of financial or economic policy of the country, political stability, crises in other countries and many others. All of the factors above are very important and in some way are contributing to the success or failure of the enterprise on national or international scale. There are methods and indicators that are used for assessing the financial security of an economic entity (see table 8).

Table 8. Financial and non-financial indicators for measuring enterprise financial security

Financial indicators	*Non-financial indicators*	
	Indicators of production	*Social indicators*
Total expected sales	Production dynamics	Wage arrears
Actual and necessary amount of investments	Capacity utilization rate	Loss of working hours
Innovation activity level	Rate of renovation of fixed assets	Human resources structure
Level of profitability of production	Level of congestion for a certain time	Existence of a corporate social responsibility
Capital productivity	Share of production in GDP	Level of remuneration of labor in relation to the average indicator for industry or the economy as a whole
Arrears (receivables and payables)	Assessment of competiveness	
Share of own sources of financing of working capital, materials, energy carriers for production	Structure and technical resource of the fleet of machinery and equipment	

Source: Reshetnikova, N., Magomedov, M., Buklanov, D., Zakharchenko, E.(2019). The international business cooperation and its influence on enterprise financial security under globalization., p.304

In summary of this chapter we can as that financial security is one of the most important elements for the development of the companies around the world. There is no

single definition accepted in the scientific literature, but there is agreement on its main characteristics such as: it is part of the economic security of the enterprise, the level of enterprise financial security depends on internal and external threat and factors and is a component of the financial security of the state. In order for the enterprise to be successful it has to have a very good management that knows the elements of the financial security and the methods how to protect and develop the enterprise.

CONCLUSIONS

The following conclusions can be drawn as a result of the study carried out. **First**, the system of financial security has been and will continue to be an actual object for scientific research. We found out that there are different papers, articles and books written on this subject from authors across the globe. **Second**, financial globalization has become an irreversible trend and feature of world financial development will depend even greater of this process. It is a process that will continue to affect the development of the countries and enterprises. **Third**, technologies are transforming the financial sphere creating new opportunities for widespread financial inclusion. **Fourth**, financial security as a scientific category is a complex concept and is analyzed in two main levels *macro* (*financial security of the countries*) and *micro* (*enterprise financial security*). To date, the scientific literature proposes many approaches to studying the level of financial security of countries and enterprises. In order to understand both terms we outline that there are differences, because each of them has its own specificity and characteristics that should be reflected when analyzing them. **Fifth**, the threats presented in this article are very important for the development of the economic entities. Overcoming them is a complex process and requires ongoing and wide-ranging cooperation between the governments, international institutions and organizations and the industry and enterprises itself. **Sixth**, the financial security of countries and enterprises depends on the influence of many factors of external and internal environment of its functioning, which define the parameters of the overall economic development system as a whole: its stability, sustainability, progressiveness and competitiveness. The level of financial security for countries and enterprises as well is one of the most important condition for its ability to carry out independent financial and economic policies in line with national and international interests.

In future the problem financial security will become even more important with the increasing use of digital technologies in various financial procedures and processes. It is a vital part of the financial progress and success of the economic entities. Financial security is an issue that must be approached holistically considering all the actors involved, using the many technical and legal tools available, developing new ones if needed, and always seeking cooperation in order for better protecting from its disadvantages. Financial security will also be among the main priorities when making various decisions and overcoming the main threats in this area will require joint efforts and close cooperation between countries and enterprises worldwide and is the only way for their continues and positive development.

BIBLIOGRAPHY

1. Bezzubov, D. (2016). Theoretical foundations of the system of state financial security. *Proceedings of the National Aviation University, III*(68), 163-166.
2. Blakyta, G., & Ganushchak, T. (2018). Enterprise financial security as a component of the economic security of the state. *Investment Management and Financial Innovations, 15*(2), 248-256.

3. Buyanova, M., & Rasskazov, Y. (2019). The analysis of the financial security of Russia: current trends, challenges, threats. *Science Journal of VolSU, XXI*(2), 19-33. doi:https://doi.org/10.15688/jvolsu3.2019.2.2
4. Calomiris, C., & Neal, L. (2012). History of Financial Flobalizacion (Overview). In G. Caprio, T. Beck, L. Neal, D. Arner, C. Calomiris, & N. Veron, *Handbook of Key Global Financial Markets, Institutions, and Infrastructure* (pp. 3-14). London: Elsevier Inc. .
5. Dayi, F. (2020). Financial security management in firms: an application in textile sector. *International Journal of Eurasia Social Sciences, 11*(39), 298-323.
6. Delas, V., Nosova, E., & Yafinovych, O. (2015). Financial Security of Enterprises. *Procedia Economics and Finance*, 248-266.
7. Dilip, D. (2010). *Financial Glibalization (Growth, Integration, Innovation and Crisis).* Palgrave Macmillan UK. Retrieved from https://www.springer.com/gp/book/9780230278608#aboutAuthors
8. Dincer, H., & Hacioglu, Ü. (2014). *Globalization of Financial Institutions (A Competitive Approach to Finance and Banking).* Springer International Publishing Switzerland.
9. European Commission. (2019). *Skills for SMEs (Supporting specialised skills development: Big Data, Internet of things and Cybersecurity for SMEs)* . Brussels: European Commission.
10. Guo, H. (2020). Computer and Information Technology Analysis of Internet Finance's Supporting Strategy for College Students' Innovation and Entrepreneurship. In J. Abawajy, K.-K. Choo, Z. Xu, & M. Atiquzzaman, *2020 International Conference on Applications and Techniques in Cyber Intelligence (Applications and Techniques in Cyber Intelligence (ATCI 2020))* (pp. 22-27). Cham: Springer International Publishing.
11. Haber, J., Bukhtiarova, A., Chorna, S., Iastremska, O., & Bolgar, T. (2018). Forecasting the level of financial security of the country (on the example of Ukraine). *Investment Management and Financial Innovations, 15*(3), 304-317.
12. Han, R. (2018). Financial Internationalization and Financial Security Issues. *Open Access Library Journal, 5*, 1-6.
13. He, D. (2016). *Financial Security in China (Situation Analysis and System Design).* Beijing: Springer Singapore.
14. Hu, S., & Huang, M. (2020). Internet Financial Security Based on Big Data. In J. Abawajy, K.-K. Choo, Z. Xu, & M. Atiquzzaman, *2020 International Conference on Applications and Techniques in Cyber Intelligence (Applications and Techniques in Cyber Intelligence (ATCI 2020))* (pp. 485-490). Cham: Springer International Publishing.
15. IMF. (2020). *Digital Financial Services and the Pandemic:: Opportunities and Risks for Emerging and Developing Economies.* Washington, D.C: International monetary fund.
16. Kaczmarek, J. (2019). The Mechanisms of Creating Value vs. Financial Security of Going Concern-Sustainable Management. *Sustainability, 11*(8), 1-24. Retrieved from https://www.mdpi.com/2071-1050/11/8/2278/htm
17. Komorowski, P. (2018). Financial security of a small open economy in conditions of globalization. *Theoretical and scientifical journal*, 48-54.
18. Lund, S., Daruvala, T., Dobbs, R., Harle, P., Kwek, J.-H., & Falcon, R. (2013). *Global Capital Markets.* Seoul: McKinsey Global Institute.
19. Pochenchuk,, G. (2014). Issues of country financial security governance. *Forum Scientiae Oeconomia, II*, 29-37.

20. Radkov, R., & Zahariev, A. (2016). *International Finance (Second Edition).* Veliko Tarnovo: Faber Publishing House.
21. Rushchyshyn, N., Nikonenko, U., & Kostak, Z. (2017). Formation of financial security of the enterprise based on strategic planning. *Baltic Journal of Economic Studies, 3*(4), 231-237.
22. Shevchenko, Y., Nosan, N., & Zachosova, N. (2019). Formation of Conceptual Bases for State Financial Security Supply: Strategic and Tactical Actions. *Modern Economics*(15), 224-229.
23. Szeles, M., & Saman, C. (2020). Globalization, Economic Growth and COVID-19. Insights from International Finance. *Romanian Journal of Economic Forecasting, XXIII*(3), 78-92. Retrieved from http://www.ipe.ro/rjef/rjef3_20/rjef3_2020p78-92.pdf
24. Traynor, P. (2018). *Digital Finance and Data Security.* Washington, D.C: Center for financial inclusion.
25. Tsapova, O. (2020). Financial security of the state: essence and approaches. *Reports of the National Academy of Sciences of the Republic of Kazakhstan, 4*(Number 332), 161 - 165.
26. United Nations . (2020, 12 08). *Supporting small businesses through the COVID-19 crisis*. Retrieved from www.un.org: https://www.un.org/en/observances/micro-small-medium-businesses-day
27. Vergun, A., & Topenko, Y. (2016). Evolution of views on financial security as a management unit. *Economics: time realities, 4*(26), 122-134.
28. Vivchar, O., Krzywkowska, J., Mykhailyshyn, L., & Konut-Ferens, O. (2019). Information-analytical provision of financial security of industrial enterprises: determinants, evaluation of indicators and mechanisms of strength. *Journal ofVasyl Stefanyk Precarpathian National University, 6*(3-4), 55-66. Retrieved from https://journals.pnu.edu.ua/index.php/jpnu/article/view/1841/2282
29. Zachosova, N. (2019). *Financial Security: Problems of Operational and Strategic Management, Risks and Peculiarities of Public Administration (Monograph).* Przeworsk: Higher School of Social and Economic.
30. Zahariev, A. (2012). *Debt Management* (Second revised and extended edition). Veliko Tarnovo: Abagar Publishing House.
31. Zahariev, A., Zveryakov, M., Prodanov, S., Zaharieva, G., Angelov, P., Zarkova, S., & Petrova, M. (2020). Debt management evaluation through support vector machines: on the example of Italy and Greece. *Entrepreneurship and sustainability issues*, 2382-2393. doi:http://doi.org/10.9770/jesi.2020.7.3(61)
32. Zaharieva, G. (2020). International Services Trade Competitiveness of EU-27 Countries. *Izvestiya Journal of Varna University of Economics, 3*(64), 273-296.
33. Zhuravlyova, I., & Lelyuk, S. (2014). Management of enterprise financial security and its intellectual component based on creating multiagent decision support system. *ЕКОНОМІІКА ТА УПРАВЛІІННЯ ПІІДПРИЄМСТВАМИ*, 163-170

THE CHALLENGES OF THE PANDEMIC TO THE TOURIST INDUSTRY ECONOMIC SECURITY (CASE STUDY OF BULGARIA)

Varadzhakova Desislava
PhD, Assocaite Professor
Academy of Sciences, Sofia, Bulgaria
email: dvaradzhakova@gmail.com

Mancheva-Ali Olga
PhD, Assistant
The "Cyril and St Methodius" University of Veliko Tarnovo, Bulgaria
e-mail: o.mancheva@ts.uni-vt.bg

Abstract
One of the main prerequisites for the development of tourism is the peaceful, secure and safe environment in tourist destinations. However, political and military conflicts, natural disasters and epidemics have always been part of people's lives. The instability in different regions has repeatedly been the reason for long periods of outflow of tourists over the years and their redirection to alternative destinations with similar tourist resources. The purpose of this paper is to present the impact of the pandemic to the economic actors in terms of their economic security. To achieve this goal, an analysis of the employment and unemployment in the tourism industry and of the tourism business revenues, is made. Official statistical data is used.

Keywords: *COVID-19 pandemic, economic security, tourism, Bulgaria*

JEL Clasification: *L83, Z32, J21*

INTRODUCTION

In 2020, humanity is hit by a global pandemic affecting human life and health. In this situation, the challenges in the economy reach serious scale. The lockdown in many countries lead to collapse of industries as tourism, transport, catering and entertainment. The main impact is the rising unemployment and economic insecurity for those who work in the abovementioned sectors. Unfortunately the negative effect of the pandemic is not restricted only to them. The impacts on the individual and business economic security effect indirectly to the financial capacity of the people and their willingness to travel after pandemic.

According to the UN World Tourism Organization, in the first half of 2020, international travel decreased by 65%. The summer season marked a 70% drop in the global tourism industry and a 90% drop in bookings. According to the European Commission, the losses for hoteliers, restaurateurs and tour operators amount to 85%.

Bulgaria also recorded a serious decline after more than two months of ban of the organized tours. Varna and Bourgas airports that serve the Black sea coast resorts reported a double-digit decline in the number of flights. There are only 1.1 million foreign tourists since the beginning of the year. At the same time the crisis has encouraged the domestic tourism. Bulgarians traveling inside the country are over 2.5 million. [8]

COVID-19 pandemic has not only economic impact. It has significant social consequences, which requires decisive coordinated action by world leaders. The spread of the virus is causing problems in global supply chains, financial market instability, shocks in consumer demand and negative impacts in key sectors for the global economy such as travel and tourism. The tourism business is dynamic and comprehensive. That's why it requires to be regulated at all levels of activity. [9]

The purpose of the paper is to present the impact of the COVID-19 pandemic to the economic actors in terms of their economic security. To achieve this goal, an analysis of the employment and unemployment in the tourism industry, the tourism business revenues and the expenditure groups, was made. Official statistical data is used. The main theoretical issues are considered.

THEORETICAL ISSUES

The concept of security is complex and there are many attempts to define it. According to the etymology of the word security, it comes from Latin from the noun "securitas" or the derived adjective "securus", which means fearless, carefree. Till now, the term "security" was considered identical to two other terms - "peace" and "defense". [14] Today, security is defined on a much broader scale than at the end of the 20th century, with both military and non-military (humanitarian) aspects. Modern scientists define it as a complex concept, containing the absence of danger, individual confidence, society and state confidence. Nowadays, if there is security, there is peace, but the opposite is not true. Security is much more than peace. Even if the ongoing conflicts are controlled and peace comes to the planet in an instant, it will not enjoy security, because there are still active problems, the consequences of which can make the days of mankind counted.

According to many authors, security means maintaining a certain equilibrium state, accepted as normal. The ability to balance well between risks, threats and available resources so as to maintain an acceptable normal state is a supreme form of public state administration. Sometimes the whole system of the state and society suffers strong shocks from unexpected or insurmountable threats. This means that a crisis begins. If a system is able to return to its normal state in a relatively short time before the crisis, then this system has security.

In today's world, we are facing new challenges, such as piracy, global economic crisis, nuclear proliferation, food crises, environmental disasters, etc., and from the beginning of 2020 the coronavirus pandemic. It undermines the global stability and collective and well-coordinated decisions leading to a new security concept are required therefore. This new concept should not be limited territorially to national borders only. Coordinated efforts by the international community are needed in several areas:

• activation and development of partnerships in policy making, knowledge transfer and implementation of these policies;

• comprehensive approach to ensure the greatest possible coordination between all countries, regional stakeholders and international institutions;

• multilateral vision and approach to achieve better coordination for crisis management. [5]

Five levels of security can be defined: individual security; security of a group of individuals; state security; community security by countries; world security. [15]

According to the 1994 UN Human Development Report, one of the founding documents in the field of security, the threats to human security are no longer individual, local or national, they are global. These include drugs, AIDS, terrorism, environmental pollution, nuclear proliferation, and now the COVID-19 pandemic is added to them. It also formulates the threats to human security, which can be summarized in seven directions, respectively:

- Victualing security;
- Environmental security;
- Personal security;
- Community security;

- Political security;
- Economic security
- Health security.

The victualing security is related to the unimpeded physical and economic access to food of each person. One of the main problems in providing food could be the lack of equal distribution of food products or low purchasing power of consumers.

Environmental security is linked to a clean environment. The main risks to the ecological balance are deforestation, pollution of water sources, the presence of harmful substances in the air. The cleanliness of river and sea basins is a major factor in the development and promotion of tourism. Nitrite pollution, for example, due to its high toxicity poses a direct threat to public health. [7]

Threats to the *personal security* can be grouped into the following categories: physical torture; military actions; terrorism; ethnic tension; street attacks; domestic violence; violence against children; suicide, drug abuse.

The pursuit of *community security* is manifested in the preservation of the physical and spiritual integrity of ethnic groups, their way of life and culture. One of the main threats to this type of security is the ethnic conflict. In addition to numerous victims, inter-ethnic conflicts have led to the destruction of monuments that are part of the world's cultural heritage and have long been anthropogenic tourist resources visited by tourists from around the world.

The human rights and freedoms respect is the base of the *political security*. The main threat is the political repression by governments.

Economic security of a country is a state of its economy when threats are absent or there are opportunities to neutralize them when they arise so that the state of dynamic stability is maintained. There can be no security in a weak and inefficient economy, just as there can be no economic security in a society torn apart by social conflicts. [13] According Nocheva [16] economic security can be seen as a set of conditions and factors to ensure the independence, sustainability and stability of the national economy, its sectors and activities, as well as their ability to constant renewal and improvement. Economic security must meet two conditions: First, preserving the economic independence of the country and the ability to make decisions in accordance with their own interests and the ability to maintain the achieved standard of living of the population and subsequently increase it. Second, economic security must be defined as a state of the economic system that persists until the moment when the internal market of a country does not depend on the action of external factors, ie. the negative impact from outside is offset by the reserves of the internal economy. In addition, economic security can be defined as the resilience of the national economic system to endogenous or exogenous shocks of economic or political origin, manifested in its ability to neutralize sources of threat and minimize damage caused by real economic impacts. Nocheva summarizes that *economic security is a system, process, complex of conditions that provide protection of the individual, society and the state while improving the quality and standard of living, social and health insurance, creating conditions and prerequisites for the implementation of various human life activities in various spheres of society: economy, business, transport, tourism, ecology, etc.* Angelov (2015) summarizes that the indicators used to assess the economic security are:

- Growth of the gross domestic product /GDP/;
- Level and quality of life of the population;
- Inflation rate;
- Unemployment rate;
- Structure of the economy;

- Amount of government debt;
- Property stratification of society;
- Criminalization of the economy and society;
- Technical condition of the production, the degree of its automation and computerization;
- Competitiveness;
- Country's dependence on imports of raw materials, energy and products;
- Presence and share of the grey economy;
- Condition of the foreign exchange reserve, etc.

To ensure economic security, it is necessary to have a certain minimum income for each individual to provide her/his basic human needs. It is this kind of security that is a prerequisite for satisfying the need for travel and tourism. The main threats to ensuring the economic stability of the individual can be high unemployment in the country in which he lives, work in the gray economy, unsecure terms for salaries payments or non-payment of wages and/or insurance, etc.

Health security is expressed in unimpeded access to health care and adequate measures to prevent epidemics or other health threatening factors, such as polluted water, poor quality food, etc. In the last two decades, diseases such as Bovine Spongiform Encephalopathy (BSE) or "mad cow" disease and its human equivalent, Creutzfeldt-Jakob disease, bird flu, SARS, Zika virus and others have also affected tourist destination preferences. [18] The world is currently in the second wave of the COVID-19 pandemic. It is still difficult to determine the time and exact location of the pandemic. The first officially announced cases are from the last days of 2019 from the city of Wuhan in China. COVID-19 entered Bulgaria gradually, but the "explosion" occurred after a celebration in the village of Vasilovtsi (Montana province) on February 29, 2020. As of this date (February 29), no case of COVID-19 has been announced in Bulgaria. The first registered case of coronavirus was on March 8, 2020. Of the 24 people who participated in the celebration, 11 were infected with coronavirus. Among them are two children aged 4 and 11 - grandchildren of the celebrant. This is nearly 50% of those present guests at the celebration. [12] Bulgaria is one of the first countries to introduce strict measures - closing the borders, a ban on organizing trips by tour operators, closing restaurants. All this restrictions lead to a collapse in tourism. The government immediately took action by proposing the 60:40 measure. It assure 60% of the salaries of the affected travel companies to be assured by the country's budget, and the remaining 40% are payable by the employers.

IMPACT OF PANDEMIC ON THE TOURIST SECTOR

When assessing the economic security in tourism, several main indicators are monitored, which create the share of GDP in the sector. These are:

- Revenues from nights spent by foreigners and Bulgarians;
- Expenditure on tourist trips of the population;
- Number of employees in the tourism industry.

The tourists outflow, mainly caused by the restrictions imposed by the governments for abolition of pandemic of COVID-19 spread, is the main reason for reducing the activity or bankrupt of many tourist companies in Bulgaria. Table 1 represents the data published by the National Statistical Institute of Republic of Bulgaria on the revenues from nights spent in the accommodation establishments in the period March - August 2020 compared the same months of 2019.

Table 1. Revenues from nights spent in accommodation establishments in Republic of Bulgaria in the period March-August 2020 compared to the same months of 2019

MONTH	REVENUES FROM NIGHTS SPENT /IN EURO/					
	Total		Decrease in %	By foreigners		Decrease in %
	2019	2020		2019	2020	
MARCH	24 965 111	10 826 640	**57**	12 090 735	5 092 593	**58**
APRIL	26 527 994	1 202 197	**95**	13 926 879	502 404	**96**
MAY	39 069 343	2 759 963	**93**	25 876 833	886 663	**97**
JUNE	104 324 380	11 826 204	**89**	84 841 749	3 680 621	**96**
JULY	177 331 808	62 756 049	**65**	143 619 279	32 945 256	**77**
AUGUST	193 769 094	101 907 045	**47**	153 953 759	53 641 682	**65**

Source: National Statistical Institute of Republic of Bulgaria

The data shows that the decrease in the revenues at the hospitality industry is significant. In April and May 2020 is over 90% compared to the same period of 2019. In Bulgaria there is a well established summer season covering the months from June to September with a peak season in July and August. Our country is a traditional sea destination for tourists from Germany, Great Britain, Russia, Israel, etc. Because of the restrictive measures, the decline in revenues from foreign tourists for the peak season /July and August/ is above the average compared to the total revenues for the study period. The average decrease in revenues from overnight stays for the period March - August 2020 compared to the previous year is 74%.

Table 2 presents the data on the amount of expenditures by groups (excluding tourist packages) for tourist trips of persons aged 15 and over for the first half of 2019 and 2020.

Table 2. Expenditure on tourist trips of the Bulgarian population */Excluding tourist packages/ for the first half of 2019 and 2020 /in Euro/*

Expenditure groups	January – June 2019	January – June 2020	Decrease in %
Food	64 850	38 148	41
Accommodation	36 465	18 366	50
Transport	43 306	23 036	47
Total	**144 622**	**79 551**	**45**

Source: National Statistical Institute of Republic of Bulgaria

According the data the decrease in the three main tourist activities is over 40%. the most noticeable in accommodation with 50% and the smallest in meals with 41%. The average decrease in these services in 2020 compared to 2019 is nearly 45%.

Prior to the COVID-19 pandemic, the tourism industry created the most jobs in the EU. According the latest data they reach 27.3 million, mainly in small and medium-sized enterprises. The direct and indirect share of the industry in the GDP of the 28 EU member states is 10.3%, and in the Bulgarian economy it forms nearly 12% of GDP. 11% of employment in Bulgaria is in tourism sector. During the pandemic, according to the Bulgarian National Bank data, in the second quarter of 2020 Bulgaria's GDP decreased by

9.8% compared to the first quarter of the year. 8.2% is the drop compared to the same quarter of the 2019. [2; 3]

For the purposes of the present study an analysis of the impacts of the global pandemic on the economic security of the people employed in tourism has to be done. The hotel and restaurant subsectors have the greatest economic importance for tourism, therefore the number of employees in these economic activities will be analyzed. Table 3 shows the data on the employment in the hotel and restaurant industry for the first halves of 2019 and 2020 /ie. before and during pandemic/. The data show the first two quarters of both years because the lockdown and the emergency situation in Bulgaria cover partially the first and totally the second quarters of 2020.

Table 3. Number of employees by labor and official legal contracts in the hotel and restaurant industry for the first quarter of 2019 and 2020

YEAR	*January – March*	*April –June*
2019	106 753	137 367
2020	81 864	88 891
Decrease	**23%**	**35%**

Source: National Statistical Institute of Republic of Bulgaria

The negative trend in the first half of 2020 is logical. In the first quarter of 2020 there is a decrease of 24 889 employees or about 23 % compared to 2019. In the second quarter the difference is even more noticeable and amounts to 48 476 fewer employees. It represents a decrease of about 35%. These data form an average percentage reduction of labor and official legal contracted employees in the hospitality and res taurant industry in the last two years of about 29%.

According to the Ministry of Finance, salaries in the hospitality sector decreased by more than 17% in June 2020, compared to the same in 2019 because of the lockdown the losses of the industry and the late start of the summer season.

The negative effect is not only on Bulgarian economy but on the global one. The losses of the tourism business continue and it their future scale is unpredictable. A second wave of COVID-19 is currently underway and the term of restoring economic stability and security is difficult to be pointed out.

STRATEGIES FOR ENSURING ECONOMIC SECURITY

In the current situation, two main strategies to ensure the economic security of the state are applied: [17]

- strategy for economic security through isolation and lockdown;
- economic security strategy through adaptation and opening up.

The strategy of economic security **through isolation** is possible in a short period of time and any attempts at long-term lockdown can lead to the collapse of the economy and mandatory reopening at a later stage. This process is objective and is based on the natural scarcity of the resources. It leads to a limitation of production and consumption, respectively of the economic growth, with all the consequences for the society. The impact of the restrictions does not create economic stability and conditions for economic growth.

The strategy for economic security **through adaptation and opening up** is one of the biggest challenges of the modern world, because together with the mutually beneficial exchange there is a transfer of negative trends, increasing uncertainty, instability and dependence of the economy on external factors. The globalization of the world economy is a prerequisite for the opening of national economies and their inclusion in the system of international trade. Sometimes, instead of achieving economic growth, the system is

subject of strong external factor pressure, governance is deformed and the performance of the national economy deteriorates sharply. Because of this the level of economic security becomes lower. The strategy of the economic security through opening and adaptation is an expression of the policy of liberalism in international economic relations. Sometimes global liberalism is not the best solution in current situation, as it removes all kinds of protections against foreign economic entities, which sharply increases the degree of economic dependence. In practice, economic activity in the country is subject to international control through a huge number of rules imposed by international organizations. In modern conditions, states manage to compensate these negative impacts in two ways: by concluding bilateral agreements and/or by being actively involved in international organizations and alliances. The participation in such agreements and organizations is dictated by both economic interests and national security interests.

World practice does not give an unambiguous answer for choosing an economic strategy. The choice is determined by the duration of the impact of the destabilizing factors, the level of competitiveness of the national economy and its degree of dependence. The solution is not only an economic but also a political issue and depends on the analysis of the internal and external environment.

In the analysis of the two main strategies for economic security of the state prevails in the opinion of using the strategy by adapting and opening up the economy, despite some of its weaknesses. This is necessary due to the dynamic changes in the environment and the impossibility of using the lockdown model to achieve economic security of the countries in the long run. However, the two types of strategies can be modified and combined according to the goals set by the state [10].

To overcome the pandemic in Bulgaria, the first method with complete lockdown of the economy has not been applied yet. Two types of measures have been applied:

1/ Declaring a state of emergency - On 13 March 2020, after 16 confirmed cases in one day, the government declared a state of emergency throughout the country for a period of one month, which was extended until 13 May 2020. Measures include closing schools and distance learning for students; closure of entertainment establishments: bars, restaurants, discos, etc.; full closure for two weeks of the winter resort of Bansko and partial closure of the capital Sofia for a few days; closing borders and airports; organized trips are prohibited. As a result of these bans and restrictions, tourism has been nullified.

2/ Announcement of an emergency epidemiological situation - It was declared on May 14, 2020 and is valid until now (mid-November). Restrictive measures and bans are lighter. During the summer, Bulgarians spent their vacations mainly in the country on the Black Sea coast, and a significantly smaller part compared to previous years in Greece. The measures included wearing masks in closed public places and transport, up to 30% occupancy in restaurants and entertainment establishments, keeping a distance between people of 1.5 m. At the same time, customers had higher sanitary and hygienic requirements in the accommodation establishments and restaurants and led to additional costs for hoteliers and restaurateurs. [11] Many businesses have suffered and unemployment in the tourism sector has risen. Revenues in tourism fell compared to previous years, as did travel expenses of the people.

CONCLUSION

The economic insecurity of business and tourists in the context of the global COVID-19 pandemic is an indisputable fact. Data on income and employment in tourism are alarming and require attention at national and international level. Bulgarian tourism

marks a huge decline in hospitality, restaurants, transport industry, tour operators and travel agents activities. This raises the need to rethink the follow-up actions that will lead to a change in the economic model by creating effective policies and institutions, redirecting funds and investing in new industries, technologies and markets. [Byanova N, 2020]

EU countries are adopting or are in the process of adopting budgetary and liquidity measures to increase the capacity of their health systems and to help citizens and economic activities particularly affected by the pandemic to sustain the pandemic. Strict restrictions on traffic and travel have been introduced, and on 13 May 2020 the European Commission proposed a number of measures to allow a gradual and coordinated renewal of tourism activities, as well as specific assistance to businesses in this industry. Bulgaria, as European Union member elaborated strategies and required permission for state aid measures to support the most affected industries. [European Commission, 2020] Regarding the liquidity of the small tourism enterprises in the European Union member states, the European Commission implements flexible state aid schemes, as well as EU financial assistance through the European Investment Fund. In terms of job creation, the SURE program helps EU countries to cover the expenditures of the closed business provoked by the reduced working hours or the closure because of the pandemic. This is just an example of the measures to keep the jobs of a number of employees.

The Bulgarian government is considering a package of measures to overcome the crisis with the outbreak of the pandemic in the country and the declaration of a state of emergency in March. According to the business, the initial measures are not sufficient and timely and the Bulgarian government is late in implementing them in practice. At a time when these measures were further developed after numerous bilateral meetings between the government ante the affected business, including representatives of the tourism industry, they reached a compromise option for both sides.

Due to the serious scale of the pandemic and the difficult health situation in Bulgaria with daily increase in the number of patients, the increasing restrictions by the state on business, make the tourism industry has an unpredictable future. The positive trends in tourism development in Bulgaria are not valid yet. The insecurity about the temporal horizon of the pandemic makes any strategies of reopening the country economies absolutely theoretical and unsure. The introduction of adequate measures to combat the pandemic and preserve life, health and economic security of the people must be a top priority of the state.

BIBLIOGRAPHY

1. Angelov Goran, Demography Problems and Economic Security, Socio-Economic Analyzes, 1/2015 (7), VTU press, Veliko Tarnovo, 2015, 33-39
2. Bulgarian Chamber of Commerce, https://bia-bg.com/analyses/view/24967/ accessed on 10 November 2020
3. Bulgarian Chamber of Commerce https://www.bia-bg.com/news/view/23065/, accessed on 10 November 2020
4. Byanova Nevena, The new growth strategy of EU – goals and problems, Proceedings of Annual University Scientific Conference of National Military University „V. Levski“, Veliko Tarnovo, 2020, p. 66-77
5. Dimitrov Dimitar, Tsvetkov Tsvetan, Economic Security, Crises and Environment for Innovations in the Security and Defence Sector, Yearbook UNWE 2104 (3), UNWE, Sofia, 2014, 87-124
6. European Commission https://ec.europa.eu/ accessed on 19 November 2020

7. Gartsiyanova Kristina, Nitrate Pollution of the River Water in the Black Sea Drainage Area, Problems of Geography, 1-2, 2016, BAS, 47-57
8. INSMARKET, http://insmarket.bg/ accessed on 12 November 2020
9. Mancheva-Ali Olga, Kostadinova Nadezhda, Some Aspects or the Tourists' Economy Security, Proceedings of II International Science Conference CONFSEC 2018, vol. 1, Sofia, 131-133
10. Marinov Anton, An Exemplary Model Strategy for Economic Security of Bulgaria, Management and Sustainable Development 1/2014 (44), 91-96
11. Naumov, Nikola, Desislava Varadzhakova & Alexander Naydenov (2020) Sanitation and hygiene as factors for choosing a place to stay: perceptions of the Bulgarian tourists, Anatolia, DOI: 10.1080/13032917.2020.1771742
12. Penerliev Milen, Petkov Veselin, COVID-19: Initial Geographical Analysis, SocioBrains, March 2020
13. Semerdzhiev Tsvetan, Management of Information Security, Softrade, София, 2007
14. Slatinski Nikolai, Measurements of Security, Paradigma, Sofia, 2000
15. Slatinski Nikolai, The Five Level of the Security, Military Press, Sofia, 2010
16. Slavova-Nocheva Maria, Economic Aspects of Security and Competitiveness in Times of Crisis, Sofia: VTU „T. Kableshkov", 2011.
17. Tsonkov Nikolai, Economic Security of the Bulgarian State in the Conditions of Globalization, Abstract, Military academy press „G. S. Rakovski". Sofia. 2012.
18. Varadzhakova Desislava, Safety and Security Impacts on Tourism Flows` Determination, Proceedings of Annual University Scientific Conference of National Military University „V. Levski", Veliko Tarnovo, 2017, 385-395

INNOVATIVE SECURITY OF THE REPUBLIC OF BELARUS IN THE CONTEXT OF THE NATIONAL STRATEGY OF SUSTAINABLE DEVELOPMENT

ИННОВАЦИОННАЯ БЕЗОПАСНОСТЬ РЕСПУБЛИКИ БЕЛАРУСЬ В КОНТЕКСТЕ НАЦИОНАЛЬНОЙ СТРАТЕГИИ УСТОЙЧИВОГО РАЗВИТИЯ

Пугачёва Ольга
Кандидат экономических наук, доцент
Гомельский Государственный Университет имени Ф.Скорины
e-mail: OPugacheva@gsu.by

Abstract
The relevance of the study is determined by the need to improve the innovative security of the Republic of Belarus in the context of the national strategy for sustainable development. The aim of the study is to analyze the factors of innovative security and their influence on the indicators of the development of scientific, technical and innovative activities of the Republic of Belarus. In accordance with this, the place of Belarus in the system of ratings and indicators of innovations was analyzed, on the basis of which the innovative development of countries of the world is assessed, taking into account the possibilities of Belarusian statistics of innovations and available data from international studies. It is concluded that the country's innovative development is lagging behind in comparison with world leaders, and obstacles to the development of innovations in the country associated with underestimating the role of research funding and ensuring innovative security are identified.

Keywords: *indicators innovative security, innovative economy, indicators of educational, scientific and innovative activities, sustainable development*

JEL Classification: O11, O38, O47, O52

ВВЕДЕНИЕ

Стратегической целью развития Республики Беларусь является построение национальной инновационной экономики. В научном сообществе осознается необходимость прорывных идей и соответствующих им новых технологий, поскольку важнейшим фактором развития государства в настоящее время выступает способность создавать наукоемкий продукт, имеющий большую добавленную стоимость. Научно-образовательная сфера становится важным ресурсом современной экономики, существенный рост которой обеспечивается путем создания и использования новейших научно-технических разработок.

Однако, несмотря на имеющиеся достижения в этой сфере, состояние инновационной деятельности в стране не отвечает требованиям, позволяющим получать конкурентные преимущества в глобальной экономике [1, 2, 3, 4].

Когда государство решает проблемы модернизации действующих предприятий путем импорта технологического оборудования, то это усиливает отставание от развития экономики передовых стран. Поэтому вопрос стратегического развития не может быть решен только путем заимствования производственных активов иностранных государств, даже если они являются новыми для страны. Актуальным остается вопрос о создании и использовании собственных нововведений.

Такой подход позволяет выделить понятие инновационной безопасности в качестве базового в период формирования инновационной экономики, экономики знаний.

Особую значимость вопросы инновационной безопасности приобретают в связи с тем, что в настоящее время инновационные технологии и процессы их внедрения имеют решающее значение для улучшения качества жизни, расширения возможностей развития и обеспечения национальной безопасности государства.

В большинстве экономически развитых стран уже длительное время ведутся исследования, посвященные проблемам национальной и экономической безопасности. Причем инновационная составляющая в этих исследованиях рассматривается как составная часть экономической или научно-технической (научно-технологической) безопасности.

Анализ показывает [5], что при переходе на инновационный путь развития происходят изменения не только в экономике и ее составляющих частях, но и в мировоззренческой, психологической, политической, социально-экономической, научно-технологической, образовательной и культурной сферах, институциональных структурах государства и общества, в развитии личности.

Таким образом, затрагиваются сферы, проблемы безопасного развития которых невозможно решить в рамках экономической безопасности. Для решения этих многогранных и многоаспектных проблем, появляющихся в процессе формирования инновационной экономики и безопасного ее развития, возникает объективная потребность исследования в рамках системы национальной безопасности важного направления – инновационной безопасности.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Обеспечение инновационной безопасности может быть реализовано через определенную совокупность условий и факторов: стабильность и устойчивость национальной инновационной системы, способность ее к саморегулированию, самоорганизации и саморазвитию при различных негативных воздействиях, позволяющие ей сохранять свое качество.

Устойчивость национальной инновационной системы рассматривается как одна из основных целей, поставленных в Национальной стратегии устойчивого социально-экономического развития Республики Беларусь на период до 2030 года, и раскрывается в следующей динамике основных показателей, характеризующих развитие науки и инноваций [6].

Таблица 1. Показатели развития инновационной деятельности в Национальной стратегии устойчивого социально-экономического развития Республики Беларусь на период до 2030 года

Показатели	*Годы*			
	2015	*2020*	*2025*	*2030*
Удельный вес инновационно активных организаций, в процентах к общему количеству организации	18,9	25,0	27,5	30,0
Удельный вес инновационной продукции в общем объеме отгруженной продукции организаций промышленности, процент	13,1	21,5	23,0	25,0
Доля внебюджетных источников во внутренних затратах на научные исследования и разработки, процент	55,0	60,0	65,0	70,0
Внутренние затраты на исследования и разработки, в процентах к ВВП	0,5	2,5	2,7	3,0

Источник: [6]

Для реализации стабильности и устойчивости развития национальной инновационной системы, достижении поставленных целей следует исходить из главного свойства инновационной безопасности – системности. Поэтому в структуру инновационной безопасности рекомендуется включать следующие взаимосвязанные и взаимодополняющие друг друга подсистемы (по структуре инновационного цикла) с соответствующими функциями и задачами по обеспечению безопасности на каждом цикле (этапе) инновационной деятельности [5]:

- образование и кадры – подготовка и переподготовка кадров для инновационной деятельности;
- наука – создание условий для научной деятельности, производства инноваций, новых научных идей и разработок, инновационной продукции и технологий;
- инновационная инфраструктура – привлечение инвестиций в инновационную деятельность, управление (менеджмент), маркетинг;
- финансовая инфраструктура – обеспечение инновационной деятельности финансовыми средствами;
- информационная инфраструктура – обеспечение информационной безопасности инновационной деятельности;
- защита интеллектуальной собственности – защита прав на изобретения, инновационные модели, промышленные образцы;
- производственная – подготовка производства к внедрению инноваций и внедрение инновационных научно-технических и научно-технологических разработок;
- консалтинговая – оказание поддержки и продвижение результатов инновационных научно-технических и научно-технологических разработок, инновационной продукции на отечественных и зарубежных рынках;
- реализация и коммерческое использование – продвижение инновационных научных разработок на рынках.

Проанализируем основные результаты развития некоторых из них в Республике Беларусь.

По индексу уровня образования, одной из составляющих индекса человеческого развития, Республика Беларусь сопоставима с наиболее развитыми странами Европы (0,838 в рейтинге 2017 г.). Доля работников с высшим и средним специальным образованием в общей численности работающих в экономике увеличилась с 48,1 в 2010 г. до 55,3 процента в 2017 г. [7].

Основные показатели развития высшего образования Республики Беларусь в 2013-2019 годы приводятся в таблице 2 [8].

Таблица 2. Развитие учреждений высшего образования в Республики Беларусь в 2013-2019 годы

На начало учебного года	*2012/ 2013*	*2013/ 2014*	*2014/ 2015*	*2015/ 2016*	*2016/ 2017*	*2017/ 2018*	*2018/ 2019*
Число учреждений, из них:	54	54	54	52	51	51	51
университетов	32	32	34	33	34	34	34
академий	7	7	7	9	9	9	9
Численность студентов, тыс. человек, в том числе по формам получения образования:	428,4	395,3	362,9	336,4	313,2	284,3	268,1
дневной	209,3	198,3	185,0	176,8	172,6	159,8	159,4
вечерней	0,9	1,1	1,2	1,4	1,4	1,3	1,3
заочной	218,3	195,9	176,7	158,2	139,2	123,2	107,4
Принято студентов, тыс. человек, в том числе по формам получения образования:	88,1	68,7	63,4	63,1	62,7	61,8	58,9
дневной	45,0	39,1	37,9	37,9	38,8	38,7	38,0
вечерней	0,3	0,5	0,3	0,4	0,3	0,3	0,3
заочной	42,7	29,1	25,2	24,8	23,6	22,8	20,6
Выпущено специалистов, тыс. человек, в том числе по формам получения образования:	84,6	82,7	81,1	78,0	74,6	81,0	64,9
дневной	45,6	39,2	41,4	39,1	36,5	45,1	32,2
вечерней	0,1	0,2	0,1	0,1	0,2	0,3	0,2
заочной	38,8	43,3	39,7	38,7	37,9	35,5	32,5
Численность профессорско-преподавательского состава (основной персонал), человек; из численности основного персонала:	24 612	23 856	23 296	21 993	21 623	20 871	20 256
имеют ученую степень доктора наук	1 346	1 348	1 341	1 333	1 337	1 338	1 318
кандидата наук	9 043	8 932	8 825	8 584	8 505	8 368	8 264
имеют ученое звание профессора	1 260	1 252	1 269	1 194	1 179	1 175	1 157
доцента	7 509	7 426	7 404	7 391	7 318	7 220	7 148
Численность студентов и магистрантов – иностранных граждан, обучающихся в учреждениях высшего образования Республики Беларусь, человек	12 512	13 863	14 796	15 356	15 971	15 570	16 654
Удельный вес иностранных граждан в общей численности студентов и магистрантов, процентов	2,9	3,4	4,0	4,4	4,9	5,2	5,9

Источник: [8]

Учреждения высшего образования демонстрируют следующую ситуацию. Количество студентов непрерывно сокращается с 2013 года. Если учесть данные по

количеству иностранных студентов, то получится, что по сравнению с 2013 годом количество студентов-белорусов сократилось на 57,6%. В 2019 году учреждения высшего образования выпустили 57,5 тыс. специалистов.

В 2019 году студентами стали 60 тыс. человек, из них 13,2% проживают в сельских населенных пунктах. Структура предпочтений абитуриентов в 2019 г. по сравнению с 2013 г. практически не изменилась. Ожидаемо выросла востребованность технических специальностей – 21,9% против 19,5% в 2013 г. Менее востребованными, но все же популярными остаются специальности экономического и юридического профиля – 29,2% против 34,5% в 2013 г. 10,5% абитуриентов выбрали педагогические специальности, 9% – отдали предпочтение сельскому и лесному хозяйству. 6,3% абитуриентов поступили на специальности, связанные со здравоохранением.

Продолжило обучение в магистратуре 6345 выпускников учреждений или 11% от их общего количества. Это гораздо меньше, чем в пиковом 2017 году, когда в магистратуру поступило 10396 выпускников университетов или 12,8%.

Наибольшее количество иностранных студентов, которые получают высшее образование в Беларуси – граждане Туркменистана (53,1%). Существенно выросло количество иностранных студентов, приехавшим в страну из Индии и Шри-Ланки – если в 2013 г. таких студентов было 0,8% от их общего количества, то в 2019 г. – 8%, что больше, чем китайских или российских студентов.

Среднесписочная численность работников организаций, занятых в сфере образования в 2018 г. – 414,4 тыс. человек. Количество педагогических работников из них составило 199,5 тыс. человек – меньше половины. Номинальная начисленная среднемесячная заработная плата работников образования в среднем увеличилась до 665 руб. (на 17,2%), учителей – до 791,5 руб. (на 17,5%), профессорско-преподавательского состава – 1162,5 руб. (на 17,7%). Однако меры по повышению заработной платы помогают слабо – численность учителей и преподавателей неуклонно сокращается. Общее количество педагогических работников за последние 6 лет уменьшилось на 8,5%, учителей – на 18,5%, профессорско-преподавательского состава – на 19,5%.

Проблемы высшего образования в Республики Беларусь следует рассматривать в контексте демографии, цифровизации экономики и развития рынка труда.

В Беларуси, как и в других европейских странах, усиливается процесс старения населения: доля населения в возрасте 65 лет и старше за последние семь лет увеличилась с 13,3 до 14,7 процента.

Сохранение суженного режима воспроизводства населения и его постарение, в том числе по причине оттока молодежи из страны, свидетельствуют о сохраняющейся актуальности демографических проблем в долгосрочной перспективе и их влиянии на развитие системы образования.

Цифровизация сопровождается изменением структуры экономики и потребности в работниках, обладающих новыми знаниями и профессиональными компетенциями. Согласно оценкам McKinsey, к 2035 году до 50 процентов рабочих процессов в мире будет автоматизировано. Однако в большинстве стран система образования существенно отстает от стран – цифровых лидеров, что создает риск нехватки цифровых кадров в будущем.

На рынке труда уже сейчас ощущается нехватка различных специалистов в индустрии ИТ. При этом образование плохо взаимодействует с рынком труда и не

отвечает на его запросы. Крупные ИТ-компании практически вынуждены открывать образовательные центры, чтобы готовить себе кадры самостоятельно.

Ситуация, когда все выпускники школ продолжают образование в университетах – это не совсем нормально: нет никакого отбора и ценность высшего образования невелика. Эксперты отмечают, что национальная система образования не выглядит подготовленной к нарастающим проблемам. Количество преподавателей сокращается, нагрузка на тех, кто еще работает, растет, что в свою очередь ведет к сокращению качества белорусского образования.

В соответствии с Постановлением Совета Министров Республики Беларусь от 28.03.2016 № 250 «Об утверждении Государственной программы «Образование и молодёжная политика» на 2016–2020 годы» в стране реализуется задача повышения конкурентоспособности высшего образования в мировом образовательном пространстве [9].

Достижение данной задачи оценивается целевым показателем по количеству учреждений высшего образования (УВО), вошедших в 4000 лучших университетов мира по рейтингу Webometrics и (или) в 1000 – по рейтингам QS или SIR. Целевой показатель содержит комплексную оценку достижений белорусских УВО в области образовательной и научной деятельности. Сведения о целевом показателе Государственной программы в соответствии с задачей «Повышение конкурентоспособности высшего образования в мировом образовательном пространстве» представлены в таблице 3.

Таблица 3. Сведения о целевом показателе, характеризующем задачу Государственной программы, и его значениях в 2016-2020 гг.

Наименование показателя	*Единица измерения*	*Годы*				
		2016	*2017*	*2018*	*2019*	*2020*
Количество УВО, вошедших в 4000 лучших университетов мира по рейтингу Webometrics и (или) в1000 – по рейтингам QS или SIR	единиц	8	9	9	10	10

Источник: [9]

В условиях стремительно растущего глобального спроса на высшее образование возрастает актуальность рейтингов университетов мира, результаты которых не только позволяют оценить качество высшего образования, но и влияют на него в глобальном масштабе.

Место университетов Беларуси с точки зрения их позиций в международных рейтингах в 2018 году приводится в таблице 4 [10, 11].

Таблица 4. Университеты Республики Беларусь в международных рейтингах в 2018 году

Рейтинг, агенство	*Рейтинг, полное название*	*Количество вузов и их позиция*	
Шанхайский рейтинг ShanghaiRanking Consultancy ARWU	Шанхайский предметный рейтинг по физике	1	БГУ 401-500
Рейтинг университетов мира THE Times Higher Education	Рейтинг университетов мира (Times Higher Education World Universities Ranrings) - THE	1	БГУ 1001+
	Предметные рейтинги (THE by subject) THE по «физическим наукам», по «инженерным наукам и технологиям»	1	БГУ 601-800
Рейтинг университетов мира QS Quacquarelli Symonds	Рейтинг университетов мира (Quacquarelli Symonds World University Rankings) - QS	2	БГУ 354 БНТУ 801-1000
	Рейтинг лучших университетов стран Восточной Европы и Центральной Азии (Quacquarelli Symonds Eastern Europe and Central Asia University Rankings) – QS EECA	4	БГУ 23 БНТУ 95 БГУИР 137 ГрГУ 151-160
	Рейтинг университетов по трудоустройству (QS Graduate Employment Rankings) – QS GER	1	БГУ 301-500
Рейтинг Ближневосточный технический университет, Турция	Рейтинг университетов по академическим показателям (Universities University Academic Performance) - URAP	1	БГУ 1393
Рейтинг U-Myltirank	Рейтинг U-Myltirank	6	БГУ, БГМУ, ВГМУ, ВГТУ, ПГУ, МИУ
Рейтинг Российский союз ректоров MosIUR	Московский международный рейтинг «Три миссии университета» (The Three University Missions) - MosIUR	1	БГУ 313
Рейтинг RUR	Рейтинг университетов (Round University Ranking0 - RUR	3	БГУ 706, РИВШ, 731, БГМУ, 772
Рейтинг UniRank	Рейтинг UniRank	2	БГУ 1147 ГГУ 5239
Рейтинг Webometrics WRWU	Рейтинг Webometrics (Webometrics Ranking of World Universities)- WRWU	7	БГУ 489 БНТУ 2720 БГМУ 4221 ГрГУ 3350 БГУИР 3720 ГГУ 3983 БГТУ 4584

Источник: [10, 11]

Анализ текущего состояния места УВО Республики Беларусь в этих рейтингах в 2018 году показывает, что в Webometrics ТОП-4000 попали только 4 УВО (БГУ, БНТУ, ГрГУ, БГУИР), в QS ТОП-1000 – 2 УВО (БГУ, БНТУ), а в SIR ТОП-1000 – 3 УВО (БГУ, БНТУ, БГУИР)

Для оценки развития научно-технической и инновационной деятельности Республики Беларусь проанализируем место Республики Беларусь в ведущих международных рейтингах научно-технического и инновационного развития (табл.5) [12, 13, 14, 15, 16].

Таблица 5. Положение Республики Беларусь в ведущих международных рейтингах научно-технического и инновационного развития в 2018 году

Международный рейтинг научно-технического и инновационного развития	*Положение Беларуси в рейтинге*
Индекс человеческого развития (ИЧР)	53-е место из 189 стран
Индекс конкурентоспособности промышленности (CIP)	47-е место из 150 стран
Глобальный инновационный индекс (GII)	72-е место из 129 стран
Индекс развития информационно-коммуникационных технологий (ИКТ)	32-е место из 176 стран
Рейтинг научных организаций Scimago	658-й ранг у БГУ 705-й ранг у НАН Беларуси из 784 ранговых позиций

Источник: [12, 13, 14, 15, 16]

Согласно отчету ООН 2018 года Республика Беларусь по индексу человеческого развития (ИЧР) заняла 53-е место среди 189 стран мира. При этом страна вошла в группу из 59 стран с очень высоким уровнем человеческого развития (very high human development) Среди стран ЕАЭС более высокое значение, чем у Беларуси, наблюдалось только у России, которая занимает 49-е место. Вместе с тем Республика Беларусь по ИЧР уступает всем странам ЕС [12].

В целях сравнительной оценки уровня конкурентоспособности обрабатывающей промышленности стран мира организация по промышленному развитию ООН (UNIDO) ежегодно рассчитывает индекс конкурентоспособности промышленности (Competitive Industrial Performance Index, CIP). Согласно отчету за 2018 год значение индекса для Беларуси составило 0,066, что соответствует 47-й позиции среди 150 стран. Среди стран ЕАЭС по индексу CIP Беларусь уступает только России, которая со значением 0,105 занимает 32-е место в мире. Среди государств ЕС Беларусь уступает 21 стране и находится на уровне Люксембурга и Эстонии [13].

Обобщающим показателем уровня развития инноваций в странах мира признается Глобальный инновационный индекс (Global Innovation Index - GII), который составляют специалисты из Корнелльского университета (США), Школы бизнеса INSEAD (Франция) и Всемирной организации интеллектуальной собственности (WIPO). Он оценивает страны по 81 критерию, начиная с уровня НИОКР и количества патентных заявок до объема расходов на образование. В отчете GII-2019, составленном по данным на 1 июня 2018 года, содержится информация сопоставительного анализа инновационных систем 129 стран и рейтинг стран по уровню инновационного развития [14].

Беларусь в GII-2019 занимает 72-е место, улучшив позицию, по сравнению с рейтингом 2018 года, на 14 строчек. Однако по сравнению со странами-соседями это

скромный показатель. Так, Латвия в рейтинге занимает 34-е, Латвия - 38-е, Польша - 39-е, Россия - 46-е, а Украина - 47-е место. Беларусь в рейтинге попадает в группу стран с уровнем ВВП на душу населения выше среднего. В этой группе страна занимает 19-е место из 34, но среди стран Европы - лишь 37-е из 39-ти.

Возглавили рейтинг, как и в прошлые годы, Швейцария, Швеция и США. Однако отмечается, что в настоящее время к верхним строчкам рейтинга приближаются Китай, Индия и другие страны Азии. Заметны успехи Объединённых Арабских Эмиратов, Вьетнама, Филиппин и Ирана.

Среди сильных сторон Беларуси составители рейтинга отмечают занятость женщин, соотношение учеников и учителей, количество студентов, экспорт услуг сектором информационно-коммуникационных технологий, процент компаний, предлагающих обучение сотрудникам, и ряд других направлений, преимущественно связанных со сферой образования.

Среди слабых сторон, как и в предшествующие годы, указываются нормативно-правовая база, в частности, верховенство права, недостаточная эффективность логистики, НИОКР, вопросы кредитования, творческие товары и услуги и нематериальные активы [14].

Одним из приоритетов инновационного и технологического развития Беларуси выступают информационно-коммуникационные технологии (ИКТ). В целях мониторинга развития сектора ИКТ и проведения сопоставимой оценки потенциала разных стран Международным союзом электросвязи разработан индекс развития ИКТ (ICT Development Index). Индекс включает 11 показателей, отражающий доступ к ИКТ, использование ИКТ, навыки ИКТ. В настоящее время этот индекс рассчитывается для 176 стран мира. Значения индекса изменяются в интервале от 0 до 10 баллов. По последним данным Международного союза электросвязи, значение индекса развития ИКТ для Беларуси составило 7,6 балла, что соответствует 32-й позиции в рейтинге стран мира, при этом Республика Беларусь по данному показателю впереди всех стран ЕАЭС. Среди стран ЕС Беларусь опережает 13 государств и располагается, с одной стороны, между Бельгией, Испанией и Кипром (7,8 балла), с другой — около Словении (7,4 балла) [15].

Среди международных рейтингов научных организаций одним из самых комплексных как по методологии, так и по охвату является рейтинг Scimago Institutions Ranking (рейтинг Scimago, SIR) [16]. В 2018 году рейтинговые оценки были сделаны для 5637 научных организаций из 130 стран мира, при этом в состав научных включены организации всех секторов деятельности (государственный, коммерческий, высшего образования, некоммерческих организаций). В основе методологии лежит оценка 12 индикаторов деятельности научных организаций, которые группируются в три субиндекса: исследовательская деятельность (ориентируется на комплексную оценку количества и уровня значимости опубликованных научных работ), инновационная деятельность (характеризует активность учреждения в сфере патентования результатов научной деятельности) и общественная активность (характеризует прежде всего активность посещений веб-ресурсов организации). Все научные организации мира распределяются по ранговым позициям, при этом одну ранговую позицию может занимать множество организаций. Всего для 5637 организаций предусмотрено 784 ранга. Например, по итогам 2018 года ведущей научной организацией мира в рейтинге Scimago стала Китайская академия наук, которой соответствует первый ранг. Наибольшее количество научных организаций, учтенных в рейтинге, относится к следующим странам: США (759 организаций), Китай (614), Франция (399), Индия (271), Испания

(282), Германия (254), Япония (243), Россия (202) и Великобритания (197). По итогам 2018 г. в рейтинге учтены 4 белорусских организации (в 2017 году — 2 организации). Наиболее высокие позиции занимают Белорусский государственный университет (658-й ранг) и НАН Беларуси (705-й ранг). Кроме того, в 2018 году в рейтингах были учтены Белорусский национальный технический университет (735-й ранг) и Белорусский государственный университет информатики и радиоэлектроники (745-й ранг).

На основе места Республики Беларусь в системе международных рейтингов проанализируем показатели инновационного развития страны в системе национальных показателей и сопоставим их с европейскими индикаторами инноваций.

Белорусская статистика ежегодно фиксирует показатели, отражающие уровень развития научной, научно-технической и инновационной деятельности страны, основные из которых за последние годы приводятся в таблице 6 [17].

Таблица 6. Основные показатели развития научной, научно-технической и инновационной деятельности Республики Беларусь в 2013-2018 гг.

Показатели	*Годы*					
	2013	*2014*	*2015*	*2016*	*2017*	*2018*
Наукоемкость ВВП, процентов	0,65	0,51	0,50	0,50	0,58	0,61
Количество исследователей на 1 млн. жителей, человек	1 939	1 834	1 786	1 776	1 799	1 880
Удельный вес инновационно-активных организаций в общем числе обследованных организаций промышленности, процентов	21,7	20,9	19,6	20,4	21,0	23,3
Удельный вес отгруженной инновационной продукции в общем объеме отгруженной продукции организаций промышленности, процентов	17,8	13,9	13,1	16,3	17,4	18,6
Доля экспорта наукоемкой и высокотехнологической продукции в общем объеме экспорта, процентов	28,3	27,7	30,9	33,2	31,9	33,3

Источник: [17]

Анализ данных таблицы 6 свидетельствует о положительной динамике в развитии большинства оцениваемых показателей.

За исследуемый период уровень наукоемкости ВВП был ниже порогового значения данного индикатора с позиции экономической безопасности – менее 1% ВВП. По уровню затрат на науку Беларусь уступает большинству стран Европы. В частности, для стран Европейского союза средний уровень затрат на научные исследования и разработки составляет 1,57 % от ВВП. На протяжении многих лет соответствующие затраты превышают уровень 1,0 % от ВВП в Российской Федерации (1,1% в 2018 г.). Среди стран Европы по уровню затрат на науку лидируют: Швеция (3,40%), Швейцария (3,37 %), Австрия (3,16%), Дания (3,05%) и Германия (3,02%).

Несмотря на некоторый рост показателя, характеризующего количество

исследователей на 10 тыс. населения, его уровень остается достаточно низким по сравнению с большинством стран. По этому показателю Беларусь отстает от России (26,3 чел.) и большинства стран ЕС (средний уровень — 56,7 чел.). Среди стран ЕС значение нашей страны превышает только показатели Кипра (18,5 чел.) и Румынии (14,2 чел.). Лидерские позиции по данному показателю занимают такие европейские страны, как Исландия (110,8 чел.), Швеция (108,0 чел.) и Дания (107,4 чел.)

В исследуемые годы наблюдается позитивная динамика показателя «Инновационная активность организаций промышленности». В 2018 г. зафиксировано увеличение уровня инновационной активности организаций промышленности. Так, в общей сложности 400 организаций осуществляли затраты на разработку и (или) внедрение инноваций (в 2017 г. — 372), а их удельный вес составил 24,8 % (в 2017 г. — 22,5 %). 380 организаций промышленности при этом осуществляли затраты на технологические инновации (в 2017 г. — 347). Удельный вес таких организаций составил 23,3 % (в 2017 г. — 21,0 %). Следует отметить, что уровень инновационной активности, достигнутый в 2018 г., является наиболее высоким за всю историю статистических наблюдений в Беларуси. По уровню инновационной активности организаций промышленности Беларусь в несколько раз опережает все страны ЕАЭС. Вместе с тем в среднем для стран ЕС характерен значительно больший уровень (41,5 %). Среди государств ЕС наша страна соответствует среднему уровню 13 стран, вошедших в Евросоюз после 2000 г. (30,5 %). Максимальные значения показателя в основном наблюдаются в странах, вступивших в Евросоюз до 2000 г. (в среднем – 51,1 %).

По итогам 2018 г. показатель «Удельный вес отгруженной инновационной продукции в общем объеме отгруженной продукции организациями, основным видом экономической деятельности которых является производство промышленной продукции», составил 18,6 %, что на 1,2 процентного пункта выше уровня предыдущего года (в 2017 г. — 17,4 %). Значение показателя, достигнутое в 2018 г., является самым высоким за всю историю статистических наблюдений, при этом в стоимостном выражении объем отгруженной инновационной продукции составил 7,9 млрд долл. США, что является максимальным значением с 2014 г. Как и в предыдущие годы, основной объем инновационной продукции поставляется на экспорт (67,5 %, в том числе в страны СНГ — 41,9 %). Уровень отгруженной инновационной продукции, достигнутой в Беларуси по итогам 2018 г., является одним из наиболее высоких среди всех стран Европы: в частности, только для шести стран Европы наблюдается более высокое значение. Это такие страны, как Ирландия (39,2 %), Испания (27,8 %), Великобритания (27,3 %), Словакия (25,9 %), Литва (23,3 %), Германия (19,0 %). Среди основных партнеров Беларуси по ЕАЭС фиксируется относительно низкий уровень отгруженной инновационной продукции: для России этот показатель равен 6,7 %, для Казахстана — 3,2 %.

В 2018 г. показатель «Доля экспорта наукоемкой и высокотехнологичной продукции в общем объеме белорусского экспорта» увеличился на 1,4 процентного пункта, по сравнению с 2017 г., и составил 33,3 %. В стоимостном выражении экспорт высокотехнологичной и наукоемкой продукции в 2018 г. составил 13 976,1 млн долл. США, что на 19,9 % выше уровня предыдущего года (в 2017 г. — 11 652,9 млн долл. США). Экспорт высокотехнологичной и наукоемкой продукции Республики Беларусь в 2018 г. осуществлялся в 194 страны мира. Вместе с тем, основной объем продукции (80,3 %) приходился на 16 стран: 3 страны СНГ (Россия, Украина, Казахстан); 7 стран Европейского союза (Литва, Польша, Германия, Кипр, Латвия, Великобритания, Бельгия); 4 азиатские страны (Китай, Индия, Индонезия,

Малайзия); по 1 стране из Северной и Южной Америки (США и Бразилия). Международное сопоставление доли высокотехнологичной и наукоемкой продукции в общем объеме экспорта показывает, что в настоящее время Беларусь находится на уровне таких государств Европы, как Норвегия (29,4 %), Литва (31,6 %), Болгария (32,0 %), Турция (33,1 %). При этом наименьшее значение показателя среди 35 учтенных стран характерно для России (17,0 %). В свою очередь, наибольшие значения показателя наблюдаются в странах ЕС.

Оценка научной и инновационной деятельности может быть основана на учете изобретательской и патентно-лицензионной деятельности научных организаций.

Динамика поступления патентных заявок и выдачи патентов в организациях Республики Беларусь в 2012-2018 гг. приводится в таблице 7 [17].

Таблица 7. Основные показатели патентно-лицензионной деятельности по объектам промышленной собственности (изобретения) в 2012-2018 гг., единиц

Показатели	*2012*	*2013*	*2014*	*2015*	*2016*	*2017*	*2018*
Подано заявок на патентование изобретений	1871	1634	757	691	521	524	547
Выдано патентов на изобретения	1291	1117	980	902	941	850	625
Действует патентов на изобретения	4694	4478	3913	2858	2735	2414	2135

Источник: [17]

Анализ данных таблицы 7 не позволяет сделать выводы о том, что изобретательская и патентно-лицензионная деятельность в организациях страны динамично развивается или характеризуется устойчивой позитивной тенденцией. Скорее фиксируются ежегодные колебания количества заявок, выданных и действующих патентов и их уменьшение из года в год.

Одной из основных причин негативной динамики патентно-лицензионной активности стало существенное повышение ставок патентных пошлин для национальных заявителей. В результате в несколько раз увеличились издержки на подачу, регистрацию и поддержание охранных документов.

ЗАКЛЮЧЕНИЕ

Несмотря на определенные достижения в инновационном развитии, Республика Беларусь отстает в сопоставлении показателей измерения инноваций от мировых лидеров.

Обобщая результаты исследований, можно выделить следующие основные барьеры на пути инноваций в стране:

- ✓ отсутствие законодательно закрепленных новых источников и инструментов финансирования инновационной деятельности;
- ✓ постоянный акцент практической инновационной политики на технологические инновации и отсутствие внимания к другим типам инноваций;
- ✓ неопределенность юридического статуса прав интеллектуальной собственности, возникающих в результате проведения научных исследований, финансируемых из государственного бюджета;

- ✓ слабые связи и недостаточные возможности для взаимодействия между участниками инновационной деятельности, отсутствие идущего снизу вверх сотрудничества между ними;
- ✓ сильное давление в сторону коммерциализации и отсутствие смягчающих риск финансовых механизмов в случае государственного финансирования научно-технических проектов, выражающееся в обязанности возвратить грант, если результаты исследований не удалось ввести в гражданский оборот;
- ✓ несущественная роль частного сектора в финансировании ранней стадии инноваций;
- ✓ малая доля инновационных малых и средних хозяйствующих субъектов.

Исследованные факторы инновационной безопасности и проведенный анализ их влияния на формирование национальной инновационной экономики и национальной инновационной системы показывают, что инновационная безопасность не обеспечивается комплексно и не в полной мере реализуются все подсистемы, обеспечивающие безопасность осуществления инновационного цикла.

Процесс формирования инновационной экономики затрагивает стратегические и тактические цели развития национальной экономики, меняет способы и методы достижения целей, но принципиальные задачи развития экономики остаются прежними: устойчивость, экономическая эффективность, конкурентоспособность, экономическая независимость, способность экономики к саморазвитию и прогрессу, безопасность.

БИБЛИОГРАФИЯ

1. Пугачева, О. В. *Особенности механизма развития инновационной деятельности и коммерциализации инноваций в Республике Беларусь* // Управлінський аспект забезпечення фінансової безпеки України: монографія / За ред. Черевка О.В. - Черкаси: видавець Чабаненко Ю.А. - Черкаси, 2018.- 312 с. (с. 285-311)
2. Pugacheva, Olga. *Evaluation of Innovation and Scientific Activities Development in the Republic of Belarus*. In: Journal "Economica". – ASEM, Chisinau, Republic of Moldova. – Year XXVII, No 1(107), March 2019. – 131 p. (p. 25-40)
3. Пугачева, О. В. *Оценка состояния, проблем и перспектив развития инновационной деятельности и коммерциализации инноваций в Республике Беларусь*. В: Вісник Черкаського університету (Серія «Економічні науки»). - 2018. - №3.- с. 85-98
4. Пугачева, О. В. *Анализ показателей развития науки и инновационной деятельности Беларуси в мировом контексте* // Модернизация экономики Беларуси: проблемы и пути их решения [Электронный ресурс]: междунар. науч. конф., посвящ. 50-летию экон. фак-та Гомельского гос. ун-та им. Ф. Скорины (Гомель, 18 окт. 2019 г.): сборник материалов / Гомельский гос. ун-т им. Ф. Скорины; редкол.: А. К. Костенко (гл. ред.) [и др.]. – Гомель: ГГУ им. Ф. Скорины, 2019. (с. 391-395)
5. Сакович, В. А. *Инновационная безопасность: основные понятия, сущность* / В. А. Сакович, Г. М. Бровка // Наука и техника. 2016. Т. 15, № 2. с. 144–153
6. *Национальная стратегия устойчивого социально-экономического развития Республики Беларусь на период до 2030 года* [Электронный ресурс]. – Режим доступа: http://www.economy.gov.by/uploads/files/NSUR2030/Natsionalnaja-strategija-ustojchivogo-

sotsialno-ekonomicheskogo-razvitija-Respubliki-Belarus-na-period-do-2030-goda.pdf – Дата доступа: 5.11.2020

7. *Концепция Национальной стратегии устойчивого развития Республики Беларусь на период до 2035 года* [Электронный ресурс]. – Режим доступа: http://www.economy.gov.by/uploads/files/ObsugdaemNPA/Kontseptsija-na-sajt.pdf – Дата доступа: 1.11.2020
8. *Образование в Республике Беларусь, 2019*. Национальный статистический комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.belstat.gov.by/upload/iblock/02f/02f0dcce5ea8e20041bca7728366684c.pdf – Дата доступа: 1.11.2020
9. *Об утверждении Государственной программы «Образование и молодежная политика» на 2016-2020 годы*. Постановление Совета Министров Республики Беларусь от 28 марта 2016 г.№ 250. – Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://pravo.by/document/?guid=3871&p0=C21600250 Дата доступа: 8.11.2020
10. Пугачева, О.В. *Университеты Республики Беларусь в системе международных рейтингов* // Наука та інноватика: вітчизняний і світовий досвід: Збірник матеріалів V Круглого столу, Черкаси, 16 травня 2019 р. / редкол.: О. В. Черевко (голова), С. В. Корновенко [та ін.] – Черкаси : ЧНУ ім. Б. Хмельницького, 2019. – 169 с. (с.112-115)
11. Пугачева, О.В. *Развитие инновационного поля университета в контексте показателей научно-инновационной деятельности* // Известия Гомельского государственного университета имени Ф. Скорины, № 5 (122), 2020. (с. 145-150)
12. *Индексы и индикаторы человеческого развития: Обновленные статистические данные 2018.* [Электронный ресурс]. – Режим доступа: http://hdr.undp.org/sites/default/files/2018_human_development_statistical_update_ru.pdf – Дата доступа: 29.10.2020
13. *Мировой рейтинг стран по индексу конкурентоспособности промышленности (CIP-2019)* / UNIDO STATISTICS DATA PORTAL [Электронный ресурс]. – Режим доступа: – https://stat.unido.org/ – Дата доступа: 24.10.2020
14. *Глобальный инновационный индекс (ГИИ) 2019* // THE GLOBAL INNOVATION INDEX 2019. Soumitra Dutta, Rafael Escalona Reynoso, and Antanina Garanasvili, SC Johnson College of Business, Cornell University Bruno Lanvin, INSEAD Sacha Wunsch-Vincent, Lorena Rivera León, Cashelle Hardman, and Francesca Guadagno1 , World Intellectual Property Organization (WIPO) [Электронный ресурс]. – Режим доступа: https://www.globalinnovationindex.org/gii-2019-report# – Дата доступа: 2.11.2020
15. *Информационное общество Республики Беларусь, 2019*. Национальный статистический комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: – https://www.belstat.gov.by/ofitsialnaya-statistika/publications/izdania/public_compilation/index_14277/?special_version=Y – Дата доступа: 3.11.2020
16. *БГУ в мировых рейтингах* [Электронный ресурс]. – Режим доступа: https://bsu.by/main.aspx?guid=146761 – Дата доступа: 7.11.2020
17. *О научной и инновационной деятельности в Республике Беларусь в 2019 году*. Национальный статистический комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: https://www.belstat.gov.by/upload/iblock/456/456f62d66f1339fd8affb44995e1c075.pdf – Дата доступа: 1.11.2020

THREATS TO GLOBAL ECONOMIC SECURITY. COVID-ECONOMY - 2020: RESULTS AND FORECASTS

УГРОЗЫ МИРОВОЙ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ. COVID-ЭКОНОМИКА – 2020 : ИТОГИ И ПРОГНОЗЫ

Балина Ирина
Доктор экономических наук, доцент
Славянский Университет в Республике Молдова
e-mail: balina_i_v@mail.ru

Abstract
Considered are external and internal threats to economic security, global aspects, potential and real. The basic scenarios of the Covid economy-2020 have been formulated. A preliminary analysis of the main global threats of 2020 and the trends of the next decade has been carried out. The issues of transition to a new digital economy, emerging contradictions and provoking factors are investigated.

Keywords: *Covid-economy, pandemic, recession, poverty, income differentiation.*

JEL Classification: *D33, D62, E25*

ВВЕДЕНИЕ

Термин covid-экономика является порождением 2020 года, когда, согласно Всемирной Организации Здравоохранения (ВОЗ), появился коронавирус тяжелого острого респираторного синдрома-2 (SARS-CoV-2) и зарегистрировано новое заболевание «коронавирусная инфекция COVID-19».

Covid-экономика определяет серьёзные последствия пандемии, характеризующие состояние и развитие мировой экономики, как положительные, так и отрицательные. К отрицательным можно отнести снижение темпов экономического роста, перешедшее в стагнацию и как, результат, глобальное увеличение показателей занятости, безработицы и бедности.

В то же время, следует выявить положительные стимулы – выявленная необходимость экстренной перестройки экономики, внедрение новых технологий, ускорение автоматизации производства, перераспределение ресурсов и смещение акцентов в сторону производительных секторов и предприятий.

Согласно рекомендациям Международного валютного фонда (МВФ) не следует забывать, что и новая экономика должна непременно оставаться «зелёной», т.е., не оказывать существенного воздействия на природные активы, поддерживать сохранение стабильности экосистемы и ресурсов, способствовать снижению негативного воздействия на природу. Только таким образом можно достичь баланса между социальной политикой, экономикой и экологией.

КРАТКАЯ ИСТОРИЧЕСКАЯ СПРАВКА

11-го февраля 2020 года, Международный комитет по таксономии вирусов присвоил новому вирусу наименование SARS-CoV-2 (коронавирус тяжелого острого респираторного синдрома-2). Данное название обосновано тем, что вирус имеет генетическое родство с возбудителем вспышки ТОРС в 2003 г. Это разные вирусы, хотя и связанные генетически.

Согласно рекомендациям, разработанным ранее совместно со Всемирной организацией по охране здоровья животных (МЭБ), а также Продовольственной и сельскохозяйственной организацией Объединенных Наций (ФАО), 11 февраля 2020 г. Всемирная организация здравоохранения (ВОЗ) объявила о присвоении данному заболеванию названия «COVID-19», ранее известного как «новый коронавирус 2019 г.» [1].

Заболевание и название вируса не всегда совпадают, как в данном случае. Так, например, СПИДОМ мы называем вирус ВИЧ, или называем заболевание корь вирусом rubeola. Официальные наименования заболеваний в Международной классификации болезней (МКБ) определяет ВОЗ.

Объявленная пандемия COVID-19 явилась текущей глобальной пандемией коронавирусной инфекции COVID-19, вызванной коронавирусом SARS-CoV-2, которой к сожалению на настоящий момент ни учёные, ни политики – пргматики не в состоянии определить дату окончания.

Вспышка впервые была зафиксирована в Ухане, в Китае, в декабре 2019 года. 30 января 2020 года ВОЗ объявила эту вспышку чрезвычайной ситуацией в области общественного здравоохранения, имеющей международное значение, а 11 марта — пандемией. По состоянию на 9 декабря 2020 года, в ходе пандемии было зарегистрировано свыше 69,1 млн. случаев заболевания по всему миру; более 1,573 млн. человек скончалось и более 47,8 млн. выздоровело [2]. К сожалению, количество погибших от данного заболевания в настоящее время сравнивают с цифрами 2-ой мировой войны.

То, что касается в целом коронавирусов, то это явление было известно и ранее. Коронавирусы (лат. Coronaviridae) - это семейство вирусов, включающее на май 2020 года 43 вида РНК-содержащих вирусов, объединённых в два подсемейства, которые поражают млекопитающих (включая человека), птиц и земноводных. Название связано со строением вируса, шиповидные отростки которого напоминают солнечную корону. Известно 7 коронавирусов, поражающих человека [3]:

1) HCoV-229E — Alphacoronavirus, впервые выявлен в середине 1960-х годов;
2) HCoV-NL63 — Alphacoronavirus, возбудитель был выявлен в Нидерландах в 2004 году;
3) HCoV-OC43 — Betacoronavirus A, возбудитель выявлен в 1967 году;
4) HCoV-HKU1[en] — Betacoronavirus A, возбудитель обнаружен в Гонконге в 2005 году;
5) SARS-CoV — Betacoronavirus B, возбудитель тяжёлого острого респираторного синдрома, первый случай заболевания которым был зарегистрирован в 2002 году;
6) MERS-CoV — Betacoronavirus C, возбудитель ближневосточного респираторного синдрома, вспышка которого произошла в 2015 году;
7) SARS-CoV-2 — Betacoronavirus B, выявленный во второй половине 2019 года, вызвавший пандемию пневмонии нового типа COVID-19, и к весне 2020 года ставший всемирной проблемой, в результате чего были закрыты многие границы и введены экстренные меры безопасности (карантин, строгая изоляция и так далее).

ТЕКУЩЕЕ СОСТОЯНИЕ

Статистику заболеваний по странам и территориям можно проследить с точки зрения хронологии распространения вируса COVID-19 по миру в соответствии с репозиторием данных Центра системной науки и техники имени Джонса Хопкинса [4].

Количество заболевших новым коронавирусом COVID-19 продолжает расти. В разных странах наблюдается разная летальность от инфекции. Так, в Австрии на сегодняшний день этот показатель составляет 0,4%, а в Италии - 9,3%. При этом верхняя цифра все время меняется. Выборочные данные по странам мира приведены ниже (табл.1).

Таблица 1. Пандемия COVID-19 по странам (выборочно) по состоянию на 4 декабря 2020 года

Страны и территории	Заражено	Выздоровело	Умерло	Летальность	На 1 млн.
Всего	**63 181 334**	**43 689 804**	**1 467 245**	**2,5**	**6493**
США[122][123]	13 617 362	6 594 109	271 296	2,0	30817
Индия[124]	9 431 691	8 847 600	137 139	1,5	6177
Бразилия[125]	6 336 278	5 601 804	173 165	2,7	26531
Россия[126]	2 322 056	1 803 467	40 464	1,7	12157
Франция[127][128]	2 230 571	164 029	53 506	2,4	27361
Венгрия[185]	79 199	20 078	1819	2,3	8205
Молдавия[186]	76 040	55 782	1785	2,3	18865
Иордания[187]	72 607	7600	829	1,1	709

Источник: COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU). *ArcGIS*. Johns Hopkins University https://github.com/CSSEGISandData/COVID-19 . Дата обращения: 4 декабря 2020 года

Anews разобрал приводимые специалистам цифры и попытался предположить, какова реальная доля умерших среди всех заразившихся.

Опасность любого инфекционного заболевания определяется двумя факторами: способность к распространению и летальность. Вирус может характеризоваться низкой летальностью, но если он хорошо распространяется, то им заразятся очень многие и суммарно погибнет большое число людей. Классический пример такого вируса - корь, один его носитель может заразить 11-18 человек. Если вирус слабо распространяется, но высоколетален, он тоже очень опасен.

Например, коронавирусы SARS (тяжёлый острый респираторный синдром, атипичная пневмония) и MERS (ближневосточный респираторный синдром) убивали 9,6% и 35% заболевших, соответственно.

Наблюдаемая летальность (CFR) от 0,4 до 10%. в каждой отдельной стране зависит от целого ряда местных факторов, а определить IFR еще в процессе эпидемии пытаются своими методами математики-эпидемиологи [5].

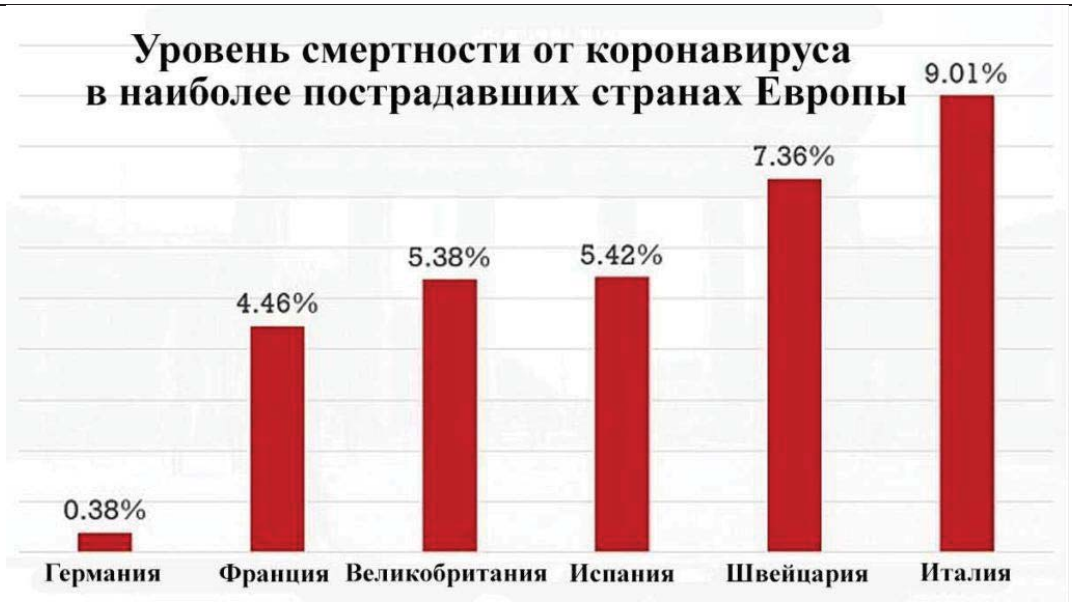


Рисунок 1. Летальность Covid-19 в странах Европы (выборочно)

На диаграмме приведены данные по 6 странам Европы, которые наряду с Германией являются шестью наиболее пострадавшими странами в Европе: уровень смертности здесь значительно ниже, чем в Великобритании (5,3%), Италии (9,0%), Франции (4,5%), Швейцарии (7,4%) или Испании (5,4%).

Этот факт довольно сложно объяснить, ведь в Германии относительно старое население, сопоставимая с другими странами система здравоохранения и, как и в других странах, там были введены общегосударственные карантинные меры.

Вполне возможно, что одним из факторов является то, что, как сообщается, власти этой страны с присущей немцам дотошностью и тщательностью ищут все возможные случаи заражения — а это может означать, что данный уровень смертности является более достоверной картиной коронавирусного кризиса.

Так что смертность в других странах тоже может быть на самом деле намного ниже, просто очень много выживших от COVID-19 людей никогда не были зарегистрированы как инфицированные коронавирусом.

И подтверждением вышесказанного является ситуация в Южной Корее, где после проведения властями массового тестирования уровень смертности составил низкие 1,2%.

Одной из мер, позволяющих оперативно реагировать на ситуацию с covid-экономикой является продолжение тотального мониторинга ситуации в мире – заболеваемости, летальности. В настоящее время такой мониторинг отражает достаточно оперативно общепланетарную картину в целом. Например, для контроля состояния в любой точке Земли есть on-line мониторинг. Примеры показаны ниже (см. рис.2-5).

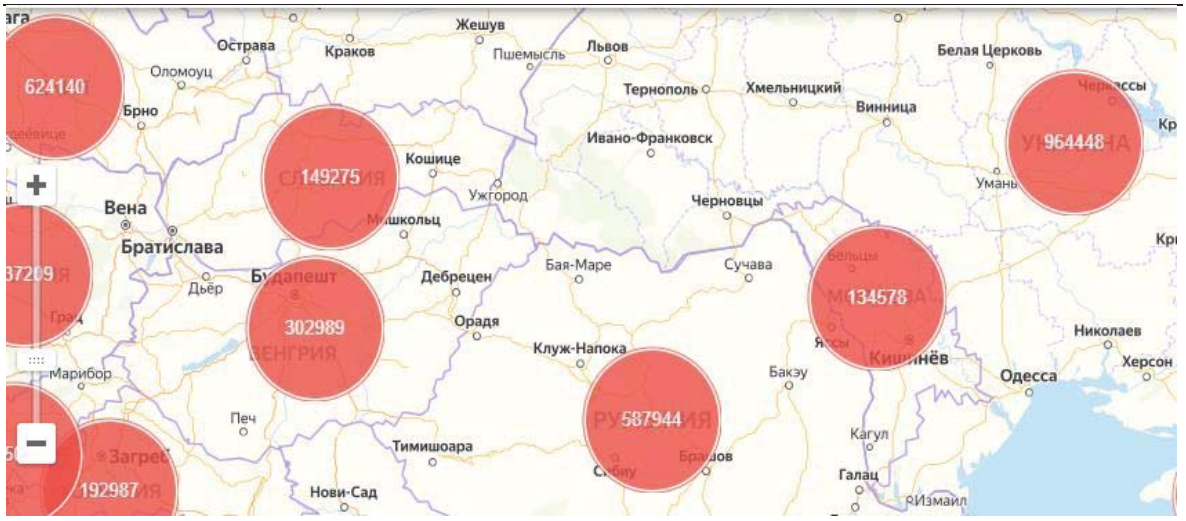


Рисунок 2. Мониторинг ситуации заболеваемости COVID-19 в Европе/ РМ (выборочно)

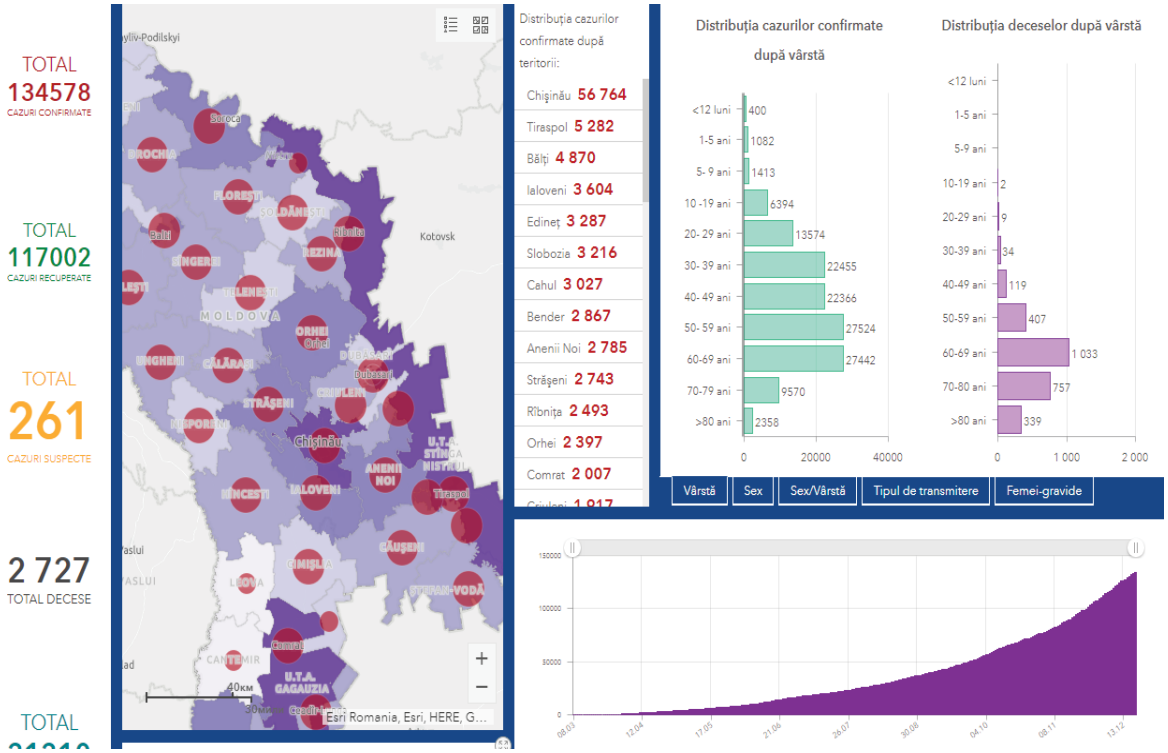


Рисунок 3. Мониторинг ситуации заболеваемости COVID-19 в РМ

Источник: Республиканский мониторинг ситуации с Covid-19 в Республике Молдова http://covidmoldova.live

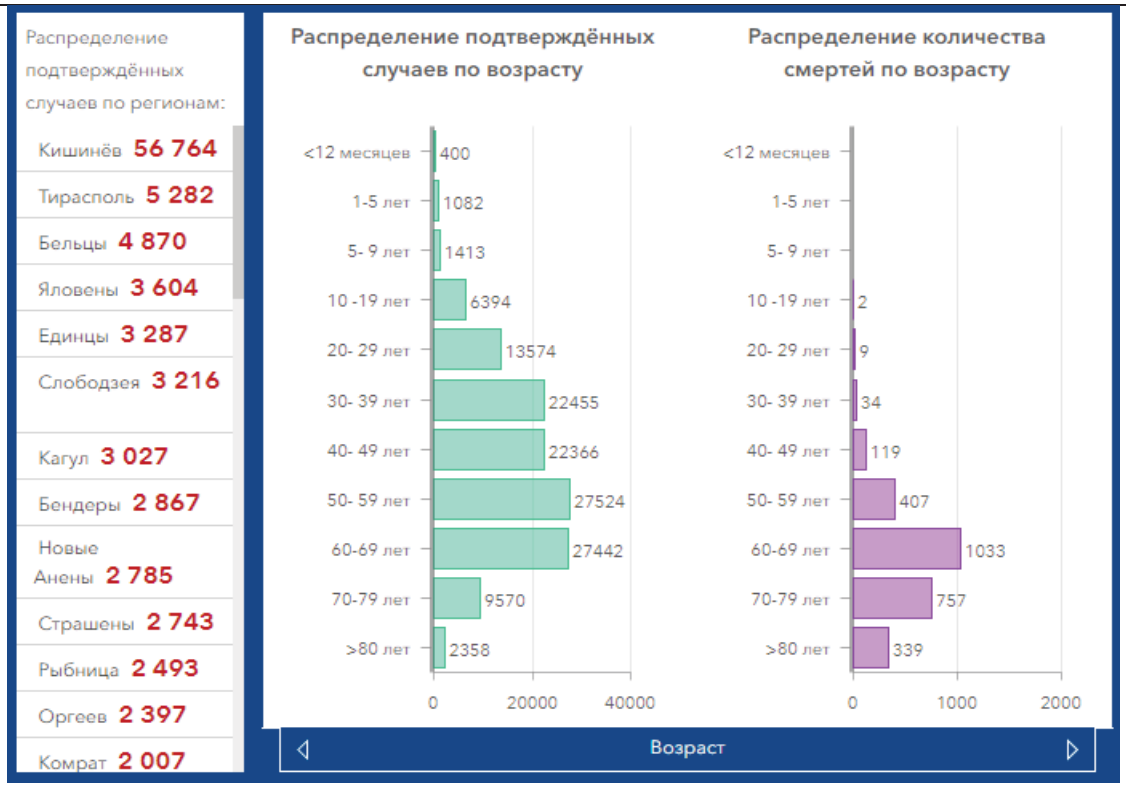


Рисунок 4. Ежедневный on-line мониторинг *«COVID-19 în Republica Moldova: situaţia la zi»*

Источник: https://locals.md/2020/v-moldove-pristupyat-k-massovomu-testirovaniyu-naseleniya-na-koronavirus/

Анализ распространения заболеваемости по территории РМ показал, что территориями с самым большим количеством случаев заражения являются: Бэлць, Тараклия, АТО Гагаузия, Кишинев, Сорока.

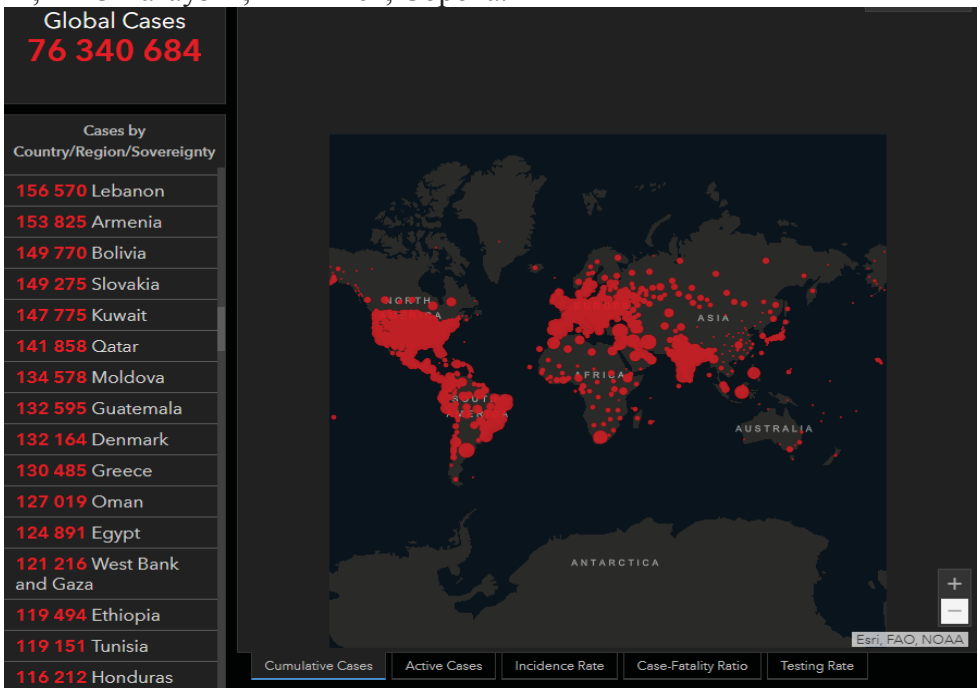


Рисунок 5. Мониторинг ситуации заболеваемости COVID-19 в мире

Источник: https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6 . Дата последнего обновления: 20.12.2020 г. 10:28

По состоянию на 18 января 2021 года общее количество заболевших в мире увеличилось на 24, 9% и составило 95 118 418 чел. Дата последнего обновления: 18.01.2021 г. 13:21 (рис. 5).

Для сравнения – выборка данных по Республике Молдова показала увеличение на 13, 58% и составила 134 578 заражённых на 20 декабря 2020 года и 152 854 на текущий момент 18 января 2021 года (рис. № 2). Эти цифры соответствуют мониторингу на официальном ресурсе РМ (рис. 4).

ПРОГНОЗЫ ПО РАЗВИТИЮ ПАНДЕМИИ

По мнению различных вирусологов из Великобритании и Германии, пандемия может продлиться от одного до двух лет. Американский профессор-эпидемиолог Джастин Лесслер считает, что COVID-19, с одной стороны, не исчезнет, а с другой – не станет препятствием для нормализации жизни, которая наступит благодаря вакцинам или благодаря приобретению населением иммунитета естественным путём.

Сотрудники университета Джонса Хопкинса провели компьютерное моделирование развития пандемии, по итогам которого составлен прогноз для разных стран при условии сохранения или введения противоэпидемических мер. Согласно этому прогнозу, карантинные меры в большинстве стран можно будет отменять не ранее августа–сентября 2020 года [1]. К сожалению, прогноз не оправдался и, более того, в настоящее время мы наблюдаем 2 и 3 волну пандемии.

Аналитики Morgan Stanley проанализировали ситуацию и выпустили доклад по США, согласно которому первая волна заболевших должна была выйти на работу в начале июня 2020 года, вторая – в августе, а школы открыться к октябрю 2020 года. Они прогнозируют появление экспериментальной вакцины и применение её для вакцинации медицинского персонала в ноябре 2020 года, а массовую вакцинацию – весной 2021 года [7]. Однако, как показывает действительность вакцинация в ряде стран уже началась и даже имеет примеры летального исхода (США, Норвегия и др.), с 18 января в России приступили к массовой вакцинации всех желающих, даже при отстутствии страховых полисов, в Республике Молдова с февраля 2021 г. планируется вакцинация населения по категориям (врачи, педагоги, лица, старше 60 лет и др.).

Еще в середине апреля 2020 года многие прогнозы были основаны на сценарии V-образного восстановления мировой экономики – за быстрым провалом последует быстрый рост по мере отмены ограничений, введенных из-за пандемии COVID-19. Ожидалось, что докризисного уровня экономика сможет достичь уже к концу года. Но по мере продления карантина, роста безработицы и осознания влияния кризиса на потребительский спрос и международные производственные цепочки прогнозы стали ухудшаться. Эксперты начали рисовать пессимистичные траектории – более длительного U-образного восстановления и даже L-образного: в этом сценарии второй волны пандемии и продления мер социального дистанцирования возвращение на докризисный уровень откладывается надолго [8].

Многие руководители компаний и экономисты теперь говорят о траектории деловой активности, которая напоминает галочку на логотипе Nike: после стремительного провала начнется длительное, болезненное восстановление, пишет The Wall Street Journal. Многие экономики вернутся на уровень 2019 г. в лучшем случае к концу следующего года. «Восстановление не будет быстрым, – приводит газета слова Марка Шнайдера, генерального директора Nestle. – Процесс займет несколько кварталов, если не лет».

Что касается общемировой проблемы бедности, приведем примеры по Республике Молдова. В экономике страны, и в частности, в распределительных отношениях, произошли негативные сдвиги, приведшие к снижению уровня жизни большинства населения, нарушению обоснованной дифференциации доходов по различным социальным слоям и регионам. В таких условиях важнейшим элементом политики в области распределения и доходов становится система социальных гарантий, защиты и поддержки населения, включающая механизмы долговременного действия, функционирующие на основе государственных законодательных актов в сфере заработной платы, пенсионного и социального обеспечения.

Так в РМ, планируется следующий этап повышения заработной платы работникам здравоохранения, материальная поддержка пенсионерам (Праламент РМ утвердил получение доплаты к пенсии в сумме 1000 леев к пасхальным праздникам пенсионерам, имеющим размер пенсии ниже 4000 лей. Продолжается изучение и удовлетворение запросов и требований работников аграрного сектора, перевозчиков, гоститничного и туристического бизнеса (как показал декабрь 2020 г., в том числе и силовым образом – демонстрации, уличные протесты, сопротивление работникам органов внутренних дел и др.)

Именно из-за этих сдвигов в экономике остро стала ощущаться проблема социального неравенства в обществе. Стали чаще употребляться понятия: неимущие, бедные, малоимущие. В связи с этим расширяется круг проблем, которые надо решить для снижения уровня бедности, и значит – уточнить приоритеты и способы государственной поддержки представителей различных социальных групп бедного населения.

В целом если говорить об оптимистичности прогнозов, то, по мнению большинства экспертов, выход из коронавирусного кризиса, восстановление наиболее пострадавших отраслей экономики явится следствием развития процесса глобальной вакцинации. Серьезная трансформация затронет лишь отдельные индустрии и модели управления бизнесом, уверены участники проекта РБК Talks

Уже к лету 2020-го крупные экономисты, в том числе представители американских школ, назвали происходящее в мире из-за коронавируса не кризисом, а шоком. Его особенность, в отличие от кризиса, в том, что он внешний и не коренится внутри системы. Поэтому, как только уходят факторы, его вызвавшие, пандемия и влияние на экономику со стороны властей, все возвращается на свои места. Это же произойдет и с мировой экономикой, говорит основатель инвестиционной группы The Movchan's Андрей Мовчан.

По мнению Олега Вьюгина, экономиста, председателя и независимого директора наблюдательного совета Московской биржи: «Решение вопроса неравенства станет главным вызовом для постковидной экономики, и, возможно, приведет к пересмотру основ современного капитализма, считает» [9].

Российский эксперт Андрей Мовчан считает, что Китай теперь будет «сдвигаться» в сторону американской позиции: открывать свои рынки так же, как это делает США, придерживаться тех же норм и правил в ведении промышленной разведки и информационных войн, которые соблюдают Соединенные Штаты. Также не ожидается с приходом Байдена взрывного роста зеленой энергетики. Нефтяная инфраструктура в США пока остается довольно мощной, а инициативы новой администрации Белого дома встретят сопротивление республиканцев в Конгрессе.

ЗАКЛЮЧЕНИЕ

На основании исследований, проведенных в данной работе можно сформулировать следующие **Выводы:**

I. Приоритетным направлением мониторинга состояния мировой экономики следует считать тщательное отслеживание угроз и максимально корректный анализ и расчет рисков по итогам последствий пандемии коронавируса.

II. Наблюдаемая рецессия 2020 года стала уникальным примером рукотворного кризиса в мировой экономике. Которая, не смотря на значительную глубину падения рынков, остаётся процессом управляемым.

III. Государства, каждое в силу своего уровня развития и возможностей оказывают беспрецедентную поддержку населению и предприятиям, что может позволить уже в 2021 году частично ликвидировать последствия кризиса.

IV. В качестве основных последствий covid-20 можно определить: усиление социальной и имущественной дифференциации населения; неравномерность социально-экономического развития стран/ районов/ регионов; нищета и бедность; низкий уровень занятости; безработица среди экономически активного населения; криминализация экономических отношений.

Рекомендации:

I. С одной стороны, положительными последствиями ковид-экономики являются ускорение технологическй революции, повышение автоматизации и роботизации во всех сферах экономики и жизни, но они же уменьшают вклад человека в создание дополнительной стоимости, порождают обострение неравенства и предполагают необходимос пересмотра процессов распределение благ.

II. С точки зрения банковской системы государств следует усилить контроль Центробанков за государственными расходами для снижения скорости пандемического спада

III. Исходя из того, что на текущий момент одной из главных и наиболее остро стоящих проблем остаётся бедность населения, потребуется разработка и внерение целой серии реформ с целью сокращения пропасти между социальными слоями общества в таких областях как здравоохранение, образование, жилищная реформа и др.

БИБЛИОГРАФИЯ

1. Свободная Internet – энциклопедия Википедия. [Электронный ресурс] https://ru.wikipedia.org/wiki/Пандемия_COVID-19 Дата обращения: 25.11.2020 г.
2. COVID-19 Dashboard by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University (JHU) (англ.). ArcGIS. Johns Hopkins University. [Электронный ресурс] Дата обращения: 9.10.2020 г.
3. Свободная Internet – энциклопедия Википедия. [Электронный ресурс] https://ru.wikipedia.org/wiki/Коронавирусы Дата обращения: 25.11.2020 г.
4. Распространение вируса COVID-19 по миру в соответствии с репозиторием данных Центра системной науки и техники имени Джонса Хопкинса (англ.). https://github.com/CSSEGISandData/COVID-19. Дата обращения: 4.12. 2020 г.
5. От 0,4 до 10%. Какова реальная летальность коронавируса COVID-19. [Электронный ресурс] Режим обращения: https://yandex.ru/turbo/anews.com/s/razvlechenija/126419903-ot-0-4-do-10-kakova-realynaja-letalynosty-koronavirusa-covid-19.html Дата обращения: 02.12.2020 г.

6. On-line мониторинг заболеваемости COVID-19 в мире https://gisanddata.maps.arcgis.com/apps/opsdashboard/index.html#/bda7594740fd40299423467b48e9ecf6. [Электронный ресурс] Дата обращения: 12.12.2020 г.
7. COVID-19 : A Prescription To Get The US Back To Work: [англ.]. — Morgan Stanley, 2020. — 3 April. — P. 2. — 18 p.
8. Q&A: How is COVID-19 transmitted? (англ.). World Health Organization (9 July 2020). Дата обращения: 16 июля 2020. Архивировано 15 июля 2020 года. РБК Talks. [Электронный ресурс] https://quote.rbc.ru/news/article/5fda3cde9a7947336931f589 . Дата обращения: 12.12.2020 г.

INSTITUTIONAL CONFIGURATION OF THE SECURITY SISTEM OF THE TRANSFORMING ECONOMIES IN THE CONTEXT OF INTEGRATION PROCESSES

PROIECTAREA INSTITUȚIONALĂ A SECURITĂȚII ECONOMIILOR ÎN TRANSFORMARE ÎN CONTEXTUL PROCESELOR DE INTEGRARE

Ignatiuc Diana
Doctor în științe economice, conferențiar universitar
Academia de Studii Economice a Moldovei
e-mail: ignatiuc_diana@yahoo.com

Abstract
Successful implementation of state efforts in ensuring the long-term economic sustainability of the Republic of Moldova and national projects and programs of socio-economic development of the country in terms of increasing the number and complexity of challenges and threats are determined by institutional efficiency of the national security system. The purpose of the article is to argue the need for institutional redesign of the entire national security system of the Republic of Moldova starting from the analysis of the constitutional and legislative framework of national security and highlighting the advantages and disadvantages of the existing security system.

Keywords: *security, national economic security, institutional security projection, institutional security models*

JEL Classification: *E02, F52, H11*

INTRODUCERE

Transformările globale contemporane caracterizate prin dinamismul şi caracterul imprevizibil al dezvoltării sociale, progresul tehnico-ştiinţific rapid, creşterea gradului de integrare şi de internaţionalizare a vieţii politice, sociale, economice contribuie la creşterea gradului de aprofundare şi complexitate al relaţiilor şi interdependenţelor dintre întreprinderile din diferite state şi dintre economiile naţionale, la intensificarea proceselor concurenţiale între agenţii economici pe plan naţional, regional şi internaţional. Toate aceste procese şi fenomene asigură agenţilor economici noi posibilităţi de dezvoltare şi de valorificare a potențialului economic disponibil, însă, în acelaşi timp, contribuie la creşterea ameninţărilor şi riscurilor globale. În virtutea acestor procese şi fenomene problema asigurării securităţii economice devine o sarcină esenţială.

În acest context comunităţile politice, economice, sociale şi ştiinţifice abordează pe larg problema asigurării securităţii naţionale şi a securităţii economice naţionale ca parte componentă a acesteia. Apărarea intereselor naţionale pe plan regional şi mondial, atenuarea ameninţărilor interne şi externe reprezintă o prioritate a strategiei de dezvoltare socio-economică a statelor într-o lume marcată tot mai mult de intensificarea proceselor integraționiste.

CONȚINUTUL ARTICOLULUI

Securitatea economică națională (SEN) este o categorie multidimensională care cuprinde diferite aspecte ale activității social – economice a țării și este parte componentă a securității naționale (SN). Adică, institutul SEN face parte din institutul SN, relația de interdependență dintre acestea fiind asemănătoare raportului particular – general. Însă, în

circuitul ştiinţific nu există o opinie unanim acceptată privind definirea conceptelor de „securitate" şi „securitate economică". Securitatea este abordată de mulţi autori atât ca lipsă totală a unor ameninţări, cât şi ca menţinere a acestora la un nivel care nu influenţează nivelul de securitate al sistemului. Securitatea economică, la rândul său, este analizată în circuitul ştiinţific ca o categorie complexă, stratificată, cu mai multe semnificaţii, fiind interpretată drept capacitate a economiei de a asigura suveranitatea geopolitică a ţării, de a determina în mod independent politica economică a statului şi de a se adapta la noile condiţii de dezvoltare. Securitatea economică este aprecierea sistematică a situaţiei economice de pe poziţia apărării intereselor naţionale.

Strategia Securităţii Naţionale defineşte securitatea naţională drept „condiţia fundamentală a existenţei poporului din Republica Moldova, a statului moldovenesc şi este un obiectiv al ţării" [1] iar politica de securitate a Republicii Moldova drept „un ansamblu de concepte, norme juridice şi acţiuni orientate spre promovarea şi protejarea intereselor naţionale prin identificarea, prevenirea şi contracararea ameninţărilor şi a riscurilor cu impact asupra securităţii statului" [1].

În același timp există o serie de acte și documente juridice care ne permit să conturăm o imagine generală cu privire la sistemul securității naționale a Republicii Moldova, inclusiv interesele naționale, amenințările, riscurile, obiectivele, mecanismele de implementare, instituțiile și mandatele acestora în domeniul dat.

Cadrul constituțional și legislativ al securității naționale a Republicii Moldova este determinat de următoarele documente oficiale:

- Constituţia Republicii Moldova (1994);
- Concepţia Securităţii Naţionale (2008);
- Strategia Securităţii Naţionale (2011);
- Strategia militară / Doctrina militară (1995);
- Legea securităţii statului (1995);
- Legea privind organele securităţii statului (1995);
- Legea cu privire la apărarea naţională (2003);
- Legea cu privire la poliţie (1990/2013);
- Legile, strategiile sectoriale şi programele de guvernare;
- alte.

În baza unei analize critice a documentelor oficiale care conturează cadrul normativ general în domeniul securității naționale (Constituţia Republicii Moldova, Concepţia Securităţii Naţionale, Strategia Securităţii Naţionale), prezentată în continuare în articol, putem evidenția mai multe dezavantaje a sistemului instituțional a securității naționale, care marchează, în mod, inevitabil și securitatea economică națională.

Constituţia Republicii Moldova reprezintă documentul juridic de bază pentru elaborarea şi implementarea politicii de securitate naţionale. Constituţia defineşte sistemul general de valori şi principii supreme pentru Republica Moldova, care servesc drept fundament pentru conceptualizarea şi elaborarea politicii de securitate a statului. Aceste valori şi principii poartă un caracter universal, pot fi regăsite în actele juridice fundamentale ale mai multor state ale lumii şi reprezintă fundamentul tradiţional pentru elaborarea politicilor de securitate a ţărilor. [2, p.10]

Concepţia Securităţii Naţionale aprobată de Parlamentul Republicii Moldova la 22 mai 2008 prin legea Nr.112 „reflectă evaluarea generală a mediului de securitate pe plan naţional şi internaţional în care operează Republica Moldova şi care defineşte scopul securităţii naţionale, liniile directorii de bază pentru securitatea naţională, valorile şi principiile generale ce urmează a fi protejate de statul şi de societatea moldovenească" [3]

și este documentul în care sunt conturate prioritățile statului în domeniul securității naționale.

Analiza structurii și conținutului Concepției Securității Naționale arată aplicabilitatea practică limitată, incoerență și caracterul declarativ al prevederilor actului normativ. Conform viziunii mai multor specialiști în domeniu, cele mai importante dezavantaje ale acestui document sunt următoarele: [2, p.13]

➢ *Definirea neadecvată a intereselor naționale, scopului securității naționale, obiectivelor și valorilor*

➢ *Lipsa definirii principiilor securității naționale.* Cu excepția „principiului de neutralitate permanentă", Concepția nu definește alte principii ale securității naționale, deși definirea acestora este declarată în denumirea capitolului 1.

➢ *Determinarea eronată a amenințărilor la adresa securității naționale*. Concepția include următoarele amenințări la adresa securității naționale: conflictul transnistrean, riscurile apariției unor tensiuni interetnice, amenințarea terorismului internațional, amenințările de origine economică și socială, amenințările din domeniul tehnologiilor informaționale, amenințările care derivă din activitatea umană, factorii tehnogeni și calamitățile naturale precum și amenințarea crimei organizate și a corupției. Astfel, în acest actu normativ putem evidenția erori de ordin metodologic și conceptul (riscurile și amenințările sunt reflectate ca fiind categorii identice), în plus, această listă nu poate fi considerată completă (nu sunt identificate amenințările securității militare, amenințările securității economice sunt evidențiate neexhaustiv, etc.).

➢ *Lipsa definirii sistemului de asigurare a securității naționale, rolului și misiunilor instituțiilor.*

În baza analizei Concepției Securității Naționale a Republicii Moldova mai putem constata că „instrumentul principal pentru asigurarea securității naționale se preconizează a fi cooperarea internațională, iar rolul instituțiilor Republicii Moldova și importanța efortului pe plan intern în asigurarea securității naționale nu sunt definite. Totodată și această cooperare se vede una pur formală și lipsită de consistență, dată fiind ruptura dintre declarațiile de intenții de participare la eforturi și organizații internaționale și capacitățile naționale limitate, lipsa unor acțiuni pentru consolidarea acestora și lipsa unor mecanisme constituite pentru a realiza aceste intenții. O asemenea structură, împreună cu deficiențele principiale de conținut menționate mai sus, promovează ancorarea continuă a Republicii Moldova în lista statelor „beneficiare de securitate" și nu în cea de „producători de securitate" [2, p. 15]

La rândul său, în **Strategia Securității Naționale a Republicii Moldova** aprobată de Parlamentul Republicii Moldova la 15 iulie 2011 se menționează că aceasta pornește de la interesele naționale, răspunde la amenințările și la riscurile cu impact asupra securității naționale, stabilește obiectivele sistemului de securitate națională, identifică mijloacele și căile de asigurare a securității naționale.

Strategia Securității Naționale determină interesele naționale, principalele amenințări, riscuri și vulnerabilități pentru securitatea națională; principalele repere ale politicii externe și politicii de apărare ce țin de asigurarea securității naționale; căile de asigurare a securității naționale; liniile directoare pentru reformarea sectorului de securitate națională. [2] Strategia Securității Naționale a Republicii Moldova tratează mai multe probleme ce țin de securitate în același mod ca și Strategia Securității Europene, conform căreia „securitatea națională a unui stat european nu mai poate fi privită ca un fenomen izolat", aceasta „ține cont de abordarea multilaterală a securității naționale, de caracterul ei multidimensional și interdependent, determinat atât de starea de lucruri din domeniile

politic, militar şi cel al ordinii publice din ţară, cât şi de situaţia din sfera economică, socială, ecologică, energetică şi de altă natură". [2, p. 16]

Dinamismul şi caracterul imprevizibil al transformărilor social – economice şi politice care marchează dezvoltarea Republicii Moldova în contextul intensificării proceselor de globalizare, regionalizare şi de integrare tot mai activă a statului nostru în circuitul internaţional au generat noi riscuri şi ameninţări pentru securitatea naţională. Toate acestea au impus necesitatea completării Strategiei Naţionale de Securitate. Astfel,în anul 2017 este aprobată Strategia Naţională de Ordine şi Securitate Publică pentru anii 2017-2020 şi Planul de acţiuni privind implementarea acesteia. Însă, dezavantajele majore a sistemului instituţional de securitate naţională prezentate anterior nu au fost atenuate nici în acest document.

Deci, în proiectarea instituţională a securităţii economice a Republicii Moldova (economie în tranziţie, cu aspiraţii evidente de integrare în Uniunea Europeană) pornim de elaborarea Strategiei Securităţii Economice Naţionale în care să fie clar conceptualizată categoria "*securitate economică naţională"*, la determinarea scopului, obiectivelor, instrumentelor specifice utilizate şi a paradigmei instituţionale a acesteia.

La etapa actuală în teorie şi practică se disting două paradigme ale proiectării instituţionale a securităţii economice:

1) homocentrică – axată pe om şi pe necesităţile lui. Ideea de bază a acestei paradigme este următoarea: *asigurând securitatea economice a fiecărui cetăţean, statul garantează securitatea economică naţională*. Ca concept acesta apare în SUA în anul 1934. O nuanţă importantă în această paradigmă ale proiectării instituţionale a securităţii este centrarea pe om, şi nu pe individ. Această abordare ia în considerare faptul că, fiind o fiinţă socială, omul trebuie să trăiască în armonie cu alţi oameni şi că securitatea economică personală a unui individ luat în parte nu poate fi asigurată din contul securităţii economice personale a altor oameni.

2) civilcentrică – axată pe necesităţile statului. În acest caz – *asigurând securitatea economică naţională este garantată şi securitatea economică personală a fiecărui cetăţean*. Această abordare a securităţii economice este în prezent dominantă în practica mondială.

Identificarea acestor paradigme presupune prezenţa unei opoziţii între interesele private (individuale) şi publice (de stat). Cu toate acestea, această opoziţie în cadrul fiecărei paradigme, nu este o distribuţie a priorităţilor, ci o relaţie cauză-efect - care instrumente ar trebui utilizate pentru a asigura atât securitatea naţională, cât şi securitatea a unui cetăţean individual.

Dar, ţinem să menţionăm că, în lumea contemporană, marcată de procesele de globalizare, regionalizare şi de integrare, şi, în acelaşi timp, zbuciumată de multiple şi diverse crize (economice, sociale, politice, militare, de sănătate, etc.) este greu de stabilit ce este prioritar pentru securitatea economică naţională – asigurarea securităţii economice a statului sau a securităţii economice personale a cetăţenilor săi. Mai corect este să vorbim doar despre un proces continuu de automenţinere cu feedback pozitiv: o creştere a securităţii economice a unui stat duce la o creştere a securităţii economice a unui cetăţean (şi invers). Însă, în acelaşi timp, în elaborarea Strategie Securităţii Economice este necesar de determinat pe ce aspect al securităţii economice naţionale (a statului sau personală) să fie concentrate eforturile iniţiale. Doar astfel poate fi proiectat un model instituţional eficient al securităţii economice naţionale în care securitatea economică a ţării nu este construită în detrimentul securităţii economice personale a populaţiei, iar populaţia nu îşi măreşte securitatea economică din contul securităţii economice a statului.

În plus, principiile de bază a paradigmelor homocentrice și civilcentrice, prezentate anterior, pot fi utilizate combinat în țările în tranziția, în diferite perioade de timp, în funcție de obiectivele specifice și subiectul cheie al securității economice. Astfel, de exemplu, securitatea economică națională poate fi axat pe asigurarea intereselor primare ale elitei naționale, care, la rândul său, creează în continuare condiții pentru securitatea economică a statului (ca sursă de resurse pentru însușire) și pentru securitatea economică a societății și a individului (deoarece stabilitatea socială este o garanție pe termen lung și asigură posibilitatea însușirii resurselor de către elită). Cu alte cuvinte, între societate în ansamblu (care este reprezentată de stat și care reprezintă subiectul cheie a securității economice în paradigma civilcentrică) și individ (subiectul cheie al paradigmei homocentrice) există diferite grupuri sociale și straturi care pot fi suficient de influente pentru a reorienta obiectivele securității economice naționale către realizarea interesele. Putem numi această paradigmă securității economice naționale centrată pe elită – sau ***elitacentrică.***

Exemple ale acestei paradigme printre țările cu o economie în tranziție pot fi Rusia în perioada anilor 1995-2000, când statul funcționa de fapt în interesul grupărilor oligarhice și Ucraina pe toată durata independenței sale. Desigur, paradigma centrată pe elită, nu a fost reflectată în mod explicit în documentele fundamentale ale securității economice naționale ale vreunui stat. Cu toate acestea, în practică, este implementat destul de des (în special în statele subdezvoltate - cum ar fi Guineea Ecuatorială, de exemplu). [4]

În plus, în teoria economică pot fi evidențiate următoarele modele instituționale de proiectare a securității economice naționale:

1) Modelul anglo-saxon care presupune separarea strictă a securității economice în securitatea financiară a unui cetățean individual și aspectele economice ale securității naționale. Conform acestui model securitatea economică națională se bazează pe un nivel avansat al competitivității economiei naționale, pe ocuparea poziției de lider absolut în comerțul internațional și pe o dominație tehnologică necondiționată. [4] Drept instrumente folosite pentru ocuparea și menținerea poziției de lider sunt accesul liber la piețele globale de desfacere și accesul gratuit la materii prime, precum și reglementarea regulilor comerciale internaționale. Dominația tehnologică necondiționată, în acest caz, este asigurată de cvasi- renta tehnologică.

O versiune independentă a modelului anglosaxon reprezintă strategia americană a securității economice naționale. Această strategie, pe lângă trăsăturile caracteristice modelului anglosaxon se mai bazează în plus pe convertibilitatea deplină a dolarului în cadrul circuitului economico-financiar global, și transformarea lui în instrument de dominație economică globală [5].

Principalele amenințări a securității economice naționale conform modelului anglosaxon provin din uzurparea poziției de lider în comerțul internațional (spionaj industrial, utilizare neautorizată a proprietății intelectuale, copiere, constrângerea transferului de tehnologie, politică națională activă de inovare în afara economiei globale etc.) și din restricții privind accesul la resurse.

Un exemplu tipic al primului tip de amenințare este politica promovată de China, care dezvoltă independent o economie inovatoare, pretinzând la ocuparea poziției de lider tehnologic în noua ordine economică mondială (considerăm că, tocmai pentru a suprima aceste aspirații, au fost impuse măsurile restrictive anti-chineze ale administrației Donald Trump) [6]. Exemplu de al doilea tip de amenințare poate fi considerat embargoul petrolier din partea OPEC în 1973. Acest embargo s-a dovedit a fi extrem de amenințător pentru Statele Unite, atât din punct de vedere economic, cât și din punct de vedere social, și, prin

urmare, o atenție deosebită în modelul american al securității economice naționale este acordată securității energetice.

Modelul anglo-saxonă poate fi greu atribuit paradigmei homocentrice sau civilcentrice . În diferite perioade de timp, preferințele statului și ale mediului științific au fluctuat în favoarea uneia dintre aceste paradigme.

2) Modelul asiatic. Acest model este elaborat în special de cercetătorii din China și Japonia. Conform acestui model securitatea economică națională este rezultatul suveranității economice a statului și a securității aprovizionării cu resurse. Spre deosebire de modelul anglo-saxon, nu se acordă prioritate dominanței economice, ci apărării împotriva dominanței economice externe. În consecință, principalele amenințări la adresa securității economice naționale sunt riscul hegemoniei corporațiilor transnaționale în cadrul sistemului economic național (inclusiv prin suprimarea întreprinderilor naționale) și limitarea livrărilor de resurse (în special a celor energetice). Instrumentele pentru asigurarea securității economice naționale sunt garantarea aprovizionării cu resurse prin diversificarea furnizorilor și construirea sistemelor de aprovizionare logistică sigure, precum și un control strict asupra intrării companiilor străine pe pieţele naționale.

Modelul asiatic se caracterizează printr-un nivel avansat de civita - centricitate - până la negarea completă (în versiunea chineză) a capacității unui individ de a înțelege care este propriul său bine și binele statului.

3) Modelul țărilor în tranziție. Țările în tranziție, numite și economii în tranziție, se caracterizează prin transformări structurale care au ca scop dezvoltarea unor instituții bazate pe economia de piață. De obicei sunt considerate țări în tranziție statele Europei Centrale și de Est și statele membre ale fostei URSS, însă definiția economiei de tranziție se referă la toate țările care încearcă să-și schimbe elementele constituționale de bază. Modelul instituțional a securității economice al majorității țărilor în tranziție (în special al statelor membre ale fostei URSS) este unul bazat pe înțelegerea problemelor social - economice care au apărut odată cu prăbușirea economiei planificate și cu tranziția către un sistem de piață. Modelele țărilor în tranziție se disting prin cea mai mare varietate de abordări privind înțelegerea esenței securității economice naționale, a amenințărilor și instrumentele pentru atenuarea lor. Putem evidenția două cele mai evidente avantaje al acestui tip de model: în primul rând, sunt luate în considerație atât amenințările de ordin intern, cât și extern (în modelele anglo-saxone și asiatice, prioritatea este acordată amenințărilor externe), și, în al doilea rând, acordă o mare atenție elaborării metodelor cantitative de evaluare a securității economice naționale, ceea ce permite nu doar întreprinderea măsurilor de ridicare a nivelului de securitate, dar și evaluarea cantitativă a eficienței acestor masuri.

CONCLUZII

În baza celor prezentate anterior, putem concluziona că, se impune necesitatea proiectării instituționale a întregului sistem de securitate națională a Republicii Moldova pornind de la determinarea structurii acestui sistem (de exemplu, securitate militară, securitate informațională, securitate economică, etc.) cu definirea exactă a componentelor acestuia precum și identificarea instituțiilor responsabile pentru asigurarea fiecărui tip de securitate națională. În continuare se impune necesitatea revizuirii și lărgirii numărului de amenințări a securității naționale și a corelării exacte a acestora cu tipurile de securitate. Modele instituționale de proiectare a securității economice naționale, prezentate anterior, sunt într-o oarecare măsură abstracte,deoarece în forma sa pură nu sunt utilizate în practică în nici o țară din lume. În plus, aceste modele au atât avantaje cât și dezavantaje. În această ordine de idei, în Republica Moldova, economie în tranziție cu strategii de dezvoltare

contradictorii și cu o mare volatilitate, se impune necesitatea elaborării și implementării unui model specific care ar permite asigurarea unui nivel avansat al securității, apărarea intereselor naționale și valorificarea avantajelor competitive ale țării noastre în condițiile dezvoltării durabile.

BIBLIOGRAFIE

1. Strategia Securităţii Naţionale adoptată la 15 iulie 2011 de Parlamentul Republicii Moldova. Disponibil pe: https://www.legis.md/cautare/getResults?doc_id=105346&lang=ro
2. Pîntea I., Mînzarari D., Zghibarţa P. , Croitoru V., alt. Legislația Republicii Moldova cu privire la sectorul de securitate și apărare națională. Studiu elaborat cu suportul NATO și a Centrului de la Geneva pentru Controlul Democratic asupra Forţelor Armate. Chișinău, 2015. Disponibil pe: https://www.academia.edu/34897793/LEGISLA%C5%A2IA_REPUBLICII_MOLDOVA_CU_PRIVIRE_LA_SECTORUL_DE_SECURITATE_%C5%9EI_AP%C4%82RARE_NA%C5%A2IONAL%C4%82
3. Concepţia Securităţii Naţionale a Republicii Moldova. Disponibil pe: https://www.legis.md/cautare/getResults?doc_id=24400&lang=ro
4. Цейковец Н. В. Концептуальные подходы к пониманию и обеспечению национальной экономической безопасности: научные теории и государственные стратегии. Журнал Экономической Ассоциации. Москва, 2016. – № 1(29). С. 129-159. ISSN: 2221-2264
5. Рукинов М. В. Векторы технологических трансформаций и перспективы безопасного развития экономики России в условиях нового технологического уклада. Известия Санкт-Петербургского государственного экономического университета. Санкт-Петербург, № 1(121),2020. С. 7-15. ISSN 2311-3464 Disponibil pe: https://unecon.ru/sites/default/files/izvestiya_no_1-2020.pdf
6. Ronis Sheila R. Economic security: Neglected dimension of national security. Washington, DC: National Defense University Press, 2011. – 130 p. Disponibil pe: https://ndupress.ndu.edu/Portals/68/Documents/Books/economic-security.pdf

BURNOUT SYNDROME – A FACTOR OF DESTABILITY OF NATIONAL SECURITY

SINDROMUL BURNOUT – FACTOR DE DESTABILIZARE A SECURITĂȚII NAȚIONALE

Cepraga Lucia
Doctor în științe filologice, conferențiar universitar
Academia de Studii Economice a Moldovei
e-mail: cepragalucia@gmail.com

Bîrsan Svetlana
Doctor în științe filologice, conferențiar universitar
Academia de Studii Economice a Moldovei
e-mail: s.birsan08@gmail.com

Abstract
The concept of national security provides for the whole set of actions aimed at ensuring the security of a state. Security policy is in itself a set of concepts, legal norms and actions aimed at promoting and protecting national interests. The Republic of Moldova is not a deviation, and the vital national interests lie in ensuring independence, constitutional order, the promotion of democratic values and the rule of law; respect for and protection of fundamental human rights; ensuring peace, welfare and prosperity of the state. The development of a security culture, including by forming an appropriate behavior to maintain the security climate, can be achieved, in our opinion, through a quality education, globally, and through an effective security education, strictly speaking. The promotion of educational policies in terms of quality of life, democracy and the level of security are becoming, more recently, more and more felt in our country. Or, education is the cornerstone of social and economic development.

In this article, the authors set out to talk about burnout syndrome, which especially affects professions that involve interaction with other people and refers to the phenomena of personal deformity, which occur as a result of internal accumulation of negative emotions, without the possibility of to externalize or release them. Here the phenomenon of emotional burning is analyzed in various ways. Therefore, the didactic activity involves the accumulation of positive / negative affective experiences that influence the individual's behavior and inevitably lead to the development of certain affective behavioral tendencies, either constructive or destructive.

Keywords: *national security, security culture, education, burnout syndrome, burnout.*

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

Motto: „Educația este cea mai puternică armă
pe care voi o puteți folosi pentru a schimba lumea.”
(Nelson Mandela)

INTRODUCERE

Etimologic, termenul de „securitate” provine din limba latină, unde *securitas, -atis* și înseamnă „lipsă de primejdii; siguranță, pace, calm; sentiment de încredere pe care îl dă cuiva absența oricărui pericol”. În Oxford English Dictionary, noțiunea de „securitate” este definită ca fiind „condiția de a fi protejat sau de a nu fi expus unui pericol, sentimentul de siguranță sau de eliberare în absența pericolului”. Astfel, securitatea reprezintă, la modul general, „a fi la adăpost de orice pericol în corelație și cu existența unui sentiment de încredere și de liniște pe care îl dă cuiva absența oricărui pericol.”[1]

„Adăpost de orice pericol", „sentiment de încredere și „...de liniște" aceste aspecte ne-am dori să fie distincte pentru societatea noastră, totuși, astăzi, ca niciodată, suntem martori oculari ai unor coliziuni de interese dintre cele mai fulminante.

Mass-media abundă în știri ce fac, într-un fel sau în altul, trimitere la noțiunea de *securitate națională* (printre care, de ultimă oră, ar fi și problema SIS-ului, mai exact, la cheremul cui să fie acest organism specializat în securitatea statului. O lungă perioadă de timp, conceptul de *securitate națională* a fost asimilat celui de *apărare militară*. Când vorbim de „securitate națională" oamenii au tendința să o asocieze cu puști, tancuri și avioane sau servicii secrete. Acestea sunt însă doar umbra proiectată pe un zid al unui montaj complex la care participă nu doar soldații, ci întreaga societate." Am putea afirma că astăzi se constată o reconsiderare a conceptului, precum și o revalorificare a acestuia, *securitate națională* fiind corelată cu numeroși factori ce participă la apărarea intereselor naționale.

„Conceptul securității naționale prevede întregul ansamblu de acțiuni orientate spre asigurarea securității unui stat. Politica de securitate reprezintă, în sine, un ansamblu de concepte, norme juridice și acțiuni orientate spre promovarea și protejarea intereselor naționale prin identificarea, prevenirea și contracararea riscurilor și amenințărilor la adresa securității statului respectiv. Republica Moldova nu reprezintă o abatere, iar interesele naționale vitale rezidă în asigurarea independenței, suveranității și integrității teritoriale, a ordinii constituționale, a promovării valorilor democratice și a statului de drept; respectarea și protejarea drepturilor fundamentale ale omului; asigurarea păcii, bunăstării populației și prosperității statului." [3, p. 248]

Evenimentele din ultimele decenii demonstrează că mediul de securitate internațional este, prin natura sa, unul dinamic și complex, caracterizat prin volatilitate și imprevizibilitate. Prin poziționarea sa geografică, Republica Moldova este parte integrantă a arhitecturii de securitate a bazinului Mării Negre – zonă de interes pentru un șir de actori regionali și internaționali puternici. „În prezent, securitatea națională a unui stat european nu mai poate fi privită în izolare. Instabilitățile și pericolele în Europa și la periferiile continentului afectează starea securității tuturor statelor europene, impunând cooperare internațională intensă și eforturi comune. Asigurarea securității naționale este o necesitate pentru toate societățile contemporane, dar ea nu se poate realiza decât cu ajutorul tuturor membrilor săi." [3, p. 249]

Conform Concepției securității naționale a Republicii Moldova, la baza dezvoltării sistemului național de apărare vor sta valorile și interesele Republicii Moldova, enunțate în Strategia securității naționale. Valorile naționale sunt centrate pe respectarea fără echivoc a supremației legii, inclusiv pe respectarea strictă a demnității umane, a egalității în drepturi și a libertății, a dreptului la exprimare, precum și a identității etnice și culturale.[8]

Urmărind dezvoltarea valorilor naționale, considerăm imperativă crearea unei *culturi de securitate*, care reprezintă „o sumă de valori, norme, atitudini sau acțiuni ce determină înțelegerea și asimilarea conceptului de securitate" [1].

CONȚINUT

Dezvoltarea unei culturi de securitate, inclusiv prin formarea unui comportament adecvat menținerii climatului de securitate poate fi realizată, în opinia noastră, printr-o educație de calitate, in globo, și printr-o educație de securitate eficientă, in stricto. Promovarea politicilor educaționale prin prisma calității vieții, a democrației și nivelului de siguranță devin, în ultima perioadă, tot mai resimțite în țara noastră. Or, educația este piatra de temelie a dezvoltării sociale și economice. Educația este cea mai puternică armă pe care

voi o puteți folosi pentru a schimba lumea, susținea Nelson Mandela. Securitatea națională a unui stat, a unei societăți depinde de factorul uman, iar „singurul motor generator de resursă umană, susține Marian Stas, profesor la Harvard Kennedy School din SUA, pentru fiecare generație este, nimic altceva decât ***educația***. Educația, afirmă același Marian Stas, profesor de matematici aplicate, trainer în procese de transformare organizațională și președinte al Asociației Clubul Liderii Mileniului Trei, într-un amplu interviu acordat pentru ziare.com, doare mai mult decât Sănătatea! Educația este în momentul de față amenințare la adresa securității naționale, pentru că resursa umană ineptă absolventă de școală va deveni peste 10 ani resursă umană adultă ineptă, oameni care vor fragiliza fibra nației, țesutul social, oameni incapabili să funcționeze în lumea în care trăim." [2]

De altfel, în 2015 România a introdus **educația** în Strategia Națională de Apărare a României. Iar Republica Moldova, chiar și cu o întârziere atât de resimțită în ziua de azi, ar trebui să-i urmeze exemplul. Astfel, se promovează ideea conform căreia în afara elementelor care țin de apărare, ordine publică sau de activitatea de informații și contrainformații, securitatea nu mai poate fi separată astăzi de un mediu economic competitiv, de stabilitatea financiar-bugetară, de existența unor sisteme publice - **educație**, sănătate, pensii - funcționale și adaptate schimbărilor, de protecția infrastructurilor critice sau de capacitatea de a răspunde la problemele de mediu.

Ca și în cazul României, de ce nu și al UE, necesitatea extinderii conceptului de securitate națională în RM ar trebui să fie motivată și de „asigurarea convergenței cu principiile europene de securitate, dezvoltate în Strategia de Securitate Europeana și Strategia de Securitate Internă a Uniunii Europene, în care securitatea și dezvoltarea sunt plasate într-o relație de directă proporționalitate. În plus, **extinderea conceptului de securitate națională vizează asigurarea unei reziliențe sporite a instituțiilor de stat și a societății civile în fata unor posibile situații de criză**, fortuite sau persistente, într-un mediu internațional de securitate impredictibil și într-un context de securitate complex".[13]

La temelia unei societăți, unei țări puternice, se află populația. Iar fundamentarea unei țări puternice se face doar prin educație. O țară construită pe valori, competențe, patriotism, integritate și viziune strategică este o țară care poate garanta statul de drept, siguranța și securitatea națională. O populație educată, care are o cultură de securitate, nu va fi niciodată ușor de manipulat, nu va închide ochii la derapajele statului de drept și își va exercita drepturile și responsabilitățile ce-i revin din statul de cetățean al statului.

Noi, cadrele didactice, ne petrecem o bună parte a timpului la locul de muncă, fiind implicați în relații atât cu beneficiarii serviciilor oferite, adică studenții, cât și cu alți colegi de serviciu: profesori, manageri etc. Toate aceste relații, necesită un mare efort emotiv, psihic, intelectual și chiar fizic. În același timp, munca îndeplinită, adică activitățile didactice (predare, îndrumare, evaluare) necesită și ele un mare efort. Pregătirea unui curs sau a unui seminar invocă mai multe ore de studiu, iar realizarea activităților de cercetare implică analiza articolelor, materialelor științifice, lucrărilor de specialitate. Toate aceste activități sunt consumatoare de resurse (de timp, dar și de finanțe), cadrele didactice renunțând, de multe ori, la propriile necesități. De facto, am putea spune că, arderea emoțională în domeniul educațional capătă un aspect de epidemie. La prima vedere, s-ar părea că ceva nu este în regulă cu oamenii care au devenit atât de vulnerabili în fața stresului. Totuși, majoritatea specialiștilor sunt de părere că, de fapt, s-a schimbat fundamental tot ceea ce ține de locul și modul nostru de lucru. [12] Astăzi, serviciul a devenit un loc rece, ostil, un mediu pretențios, ceea ce conduce la epuizarea emoțională, fizică și spirituală. „Emoțiile și sentimentele, atât de omenești, au devenit, pentru mulți, adevărate obstacole, dacă nu chiar inamici, în calea succesului. Cerințele zilnice exagerate

legate de serviciu, de familie și de performanța noastră proprie nu fac altceva decât să ne erodeze energia și entuziasmul". [4] Bucuria succesului și emoțiile realizărilor sunt din ce în ce mai dificil de atins, iar aceasta conduce inevitabil la diminuarea dedicației profesionale. „Când stocul emoțional este epuizat, asistăm la o dezumanizare a persoanei. Ca rezultat, organismul nostru nu reușește să facă față situației stresante și, în aceste condiții, se dezvoltă arderea emoțională." [5]

Noțiunea de „ardere profesională" sau termenul „burnout" este folosit mai mult cu referință la profesiile sociale. Conceptul de „ardere profesională" (professional burnout) a fost propus de către A. Morrow, pentru a defini starea în care se pomenesc specialiștii din grupurile profesionale de risc, termenul prezentând un echivalent al stării de stres. [7] Descrierea fenomenului a fost realizată anterior acestei definiții. Conform unor opinii, ea aparține psihologului american Freudenberger care a analizat starea de demoralizare, decepție, manifestări de tensiune, astenie și suprasolicitare pe care le suportau angajații clinicilor psihiatrice. [11] Și Freudenberger, autorul ideii epuizării profesionale, a menționat că acest fenomen are răspândire mai ales în sfera așa numitelor profesii sociale, în care specialistul se confruntă cu problemele altor persoane. Alt fondator al ideii arderii profesionale, Christina Maslach, a definit acest fenomen ca sindrom al epuizării fizice și emoționale, incluzând formarea unei autoevaluări negative, atitudini de repulsie față de activitatea de muncă și pierderea capacității de compasiune și înțelegere a clienților. Sindromul arderii profesionale este văzut ca o totalitate de trăiri negative, legate de locul de muncă, de colectivul profesional și întreaga organizație, instituție, întreprindere în care persoana își exercită activitatea. Se manifestă mai frecvent totuși la specialiștii din domeniul socialului, drept caracteristici de bază având: starea de apatie socială, rezultată din suprasolicitarea emoțională; manifestarea unor trăiri și atitudini negative față de colegi și clienți; autoaprecierea profesională joasă - sentimentul de incompetență, lipsa de aptitudini creative, inovatoare, uneori suportarea stării de vinovăție provocate de autoevaluarea insuficienței rezultatelor activității profesionale.

Sindromul burnout afectează în mod special profesiile ce presupun interacțiunea cu alți oameni și se referă la fenomenele de deformare personală, ce apare ca rezultat al acumulării interne a emoțiilor negative, fără posibilitatea de a le exterioriza sau a le elibera. Fenomenul arderii emoționale este analizat sub diverse aspecte de către specialiștii în domeniu. [11] Sub aspect clinic, sindromul burnout desemnează eșuarea, uzura și epuizarea energiei sau resurselor, care îi provoacă individului o scădere globală a întregului potențial. Sub aspect social-psihologic, arderea emoțională se prezintă ca o stare de oboseală psihică, de decepționare și apare la oamenii cu așa-numitele profesii auxiliare. Sub aspect organizatoric, sindromul burnout este văzut ca un proces în care un profesionist angajat anterior se eliberează de la munca sa, ca răspuns la stresul sau la tensiunea resimțită. Și aspectul social-istoric, evidențiază impactul societății în dezvoltarea sindromului burnout, reducând rolul individului ca atare în dezvoltarea acestei dereglări. Într-un cadru analitic distinct sunt prezentate componentele sindromului arderii emoționale. Astfel, Christina Maslach identifică trei componente, și anume: epuizare emoțională, depersonalizare, reducerea realizărilor personale.

Arderea emoțională a fost în mod tradițional considerată o problemă exclusiv individuală, un defect în personalitatea profesorului. Deseori auzim angajați blamându-se: „Dacă nu pot să rezist presiunii, ar trebui să plec din domeniul". Acest tip de gândire nu admite că profesorii pot lucra în medii școlare care creează epuizare. În fiecare an cadre didactice talentate, care ar fi putut fi salvate, renunță la meserie. Anume din această cauză, astăzi, sindromul burnout este abordat întâi de toate ca o problemă ce ține de locul de muncă și doar în al doilea rând ca fiind o problemă individuală. O analiză a componentelor

și a fenomenului arderii emoționale în general, poate facilita înțelegerea modului în care profesorii concep munca lor și, implicit, evaluarea stadiului actual al situației din domeniul învățământului superior.

Actualmente, studiile de specialitate constată că tot mai frecvent tinerii sunt vulnerabili față de arderea emoționala. Potrivit diferitor cercetări, un numărul copleșitor de profesori suferă de sindromul burnout chiar și după 20 de ani de muncă în școală,, iar până la vârsta de 40 de ani toți profesorii sunt „arși emoțional." În context menționăm și despre existența mai mulți factori care ar favoriza dezvoltarea sindromului burnout la tineri. [6] Debutul în orice profesie constituie o provocare majoră pentru orice nou angajat. Este o perioadă de formare în care cunoștințele, aptitudinile și atitudinile dobândite în timpul unui program de educație sunt aplicate în practică. Este o perioadă de tranziție care poate fi stresantă precum și provocatoare, motivul fiind cerințele la care trebuie să răspundă persoana. Majoritatea tinerilor cred că, odată angajați, se vor putea realiza atât în plan profesional, cât și financiar, ceea ce adesea nu coincide cu realitatea. Profesorii care manifestă emoții negative la locul de muncă și care au pierdut interesul față de ceea ce fac au probabil mai multe șanse să prezinte sindromul burnout. Sentimentul de frustrare și eșec, care apare în situațiile de suprasolicitare profesională, asociată cu discrepanța dintre cerințe și posibilitățile de realizare este un declanșator al arderii profesionale. Se constată că trăirea sentimentului de nerealizare, frustrare în plan profesional, comportamentul de workaholic pot cauza dezvoltarea sindromului burnout. Astfel, volumul mare de lucru, presiunea timpului, lipsa suportului din partea colegilor și administrației, ambiguitatea rolului, lipsa posibilității de a ține sub control situația contribuie la apariția vulnerabilității tinerilor față de arderea emoționala. Unii cercetători identifică o corelație semnificativă între nivelul înalt al empatiei și apariția arderii emoționale. În viziunea psihologului rus Maria Borisova, la tinerii profesori, cu stagiu de până la 5 ani, empatia este nominalizată ca cea mai importantă trăsătură profesională. Odată cu creșterea stagiului în muncă, drept cea mai importantă trăsătură profesională apare profesionalismul/cunoștințele, empatia pierzând din importanță. Respectiv, prezența nivelului înalt al empatiei la cadrele didactice tinere ar putea servi ca motiv pentru dezvoltarea sindromului burnout. Reciprocitate emoțională, care predispune orientarea spre celălalt, din punctul nostru de vedere, poate fi să declanșeze arderea emoțională. Frecvent se întâmplă ca din lipsa experienței dictată de vârsta tânără, cadrele ce lucrează cu oamenii, percep totul prea emoțional, implicându-se fără rezerve în tot ceea ce se întâmplă la serviciu. Cu timpul, resursele emoțional-energetice se epuizează și apare necesitatea de a le conserva, a le restabili." [9]

Atunci când vorbim despre arderea emoțională, putem afirma că satisfacția în muncă este un factor important. Satisfacția minimizată în muncă poate conduce la dezvoltarea arderii emoționale la cadrele didactice. Există corelații semnificative între satisfacția în muncă, epuizarea emoțională, depersonalizarea și reducerea realizărilor personale la cadrele didactice în general. Totodată, se constată corelații semnificative între conducere, relații interpersonale și epuizarea emoțională, depersonalizarea; între organizare, comunicare și epuizarea emoțională, depersonalizarea, reducerea realizărilor personale și între remunerare, promovare și epuizarea emoțională.

CONCLUZII

Generalizând, menționăm că în condițiile în care informația ne invadează, timpul parcă se contractă, sarcinile de la serviciu devin din ce în ce mai multe, mai complexe, mai diversificate și mai urgente, devine tot mai complicat și mai greu de controlat echilibrul afectiv, capacitatea de a relaționa și reacționa și, respectiv, consecințele activității noastre.

Emoțiile reprezintă, în primul rând, reflectarea psihică a atitudinii subiectului față de lumea înconjurătoare, atât timp cât ele sunt pozitive, intră în rezonanță cu stările altora și comunicarea acestor trăiri fără a fi afectat cel de alături, induc indiscutabil creșterea echilibrului emoțional, comunicării interpersonale, motivației și satisfacției profesionale. Activitatea didactică presupune cumularea unor experiențe afective pozitive/negative, ce influențează comportamentul individului și conduc inevitabil la dezvoltarea anumitor tendințe comportamentale afective fie constructive, fie distructive.

Consolidarea proceselor democratice, ridicarea nivelului de trai, promovarea coeziunii sociale și coordonarea intereselor fundamentale ale statului și societății nu pot fi realizate în afara unui cadru adecvat de securitate. Se consideră că obiectivul esențial al politicii de securitate și al activității instituțiilor nu constă în oferirea unui sentiment abstract de securitate, ci în *crearea și menținerea unor condiții favorabile pentru dezvoltarea economică, socială, politică și culturală a țării*. Din acest motiv, *asigurarea securității naționale este scopul central urmărit de orice stat atât în realizarea politicii interne, cât și a celei externe*.

BIBLIOGRAFIE

1. ALBU, Natalia. Conceptele de securitate și securitate națională: teorii și politici."[1] *Studii de securitate și apărare. Publicație științifică* // https://ibn.idsi.md/sites/default/files/imag_file/Conceptele%20de%20securitate%20si%20securitate%20nationala.pdf
2. BADEA**,** Camelia. Educația este în momentul de față amenințare la adresa securității naționale
3. CUROŞ, Liudmila. Educaţia – pilon sigur al securităţii umane. p. 248-249 // https://ibn.idsi.md/sites/default/files/imag_file/247-254_0.pdf
4. DRUNCEA, Simona. De la stres la sindromul burnout. Simptome și soluții// http://www.psychologies.ro/sanatate-2/de-la-stres-la-sindrom-burnout-simptome-sisolutii-2141466
5. GORINCIOI V., PLATON C. Stresul și sindromul arderii emoţionale la profesorii universitari. //În: Studia Universitatis, 2013. nr 1. pp. 224-228.
6. GORINCIOI, Veronica. Studiul sindromului arderii emoționale la cadrele didactice universitare din perspectiva de gen// http://www.cnaa.md/files/theses/2015/22335/veronica_gorincioi_thesis.pdf
7. LOSÂI, Elena, Arderea profesională la cadrele didactice// http://dir.upsc.md:8080/xmlui/bitstream/handle/123456789/1391/Conf_Tendinte_modenne_psihologie_2017_p5-11.pdf?sequence=1&isAllowed=y
8. Strategia națională de apărare a RM, aprobată prin HG nr.134 din 13.06.2018 // www.legis.md
9. БОЙКО, В.В. Энергия эмоций в общении: взгляд на себя и на других.// https://gigabaza.ru/doc/147901.html
10. БУЗМАКОВА, Надежда. Феномен эмоционального «выгорания» и особенности его проявления у педагогов Феномен эмоционального «выгорания» и особенности его проявления у педагогов (doshkolnik.ru)
11. ВОДОПЬЯНОВА, Н. СТАРЧЕНКОВА, Е. Синдром выгорания диагностика и профилактика.// avidreaders.ru
12. ТРУШИНА, Екатерина. Профессиональное выгорание педагогов// Профессиональное выгорание педагогов (b17.ru)
13. https://www.presidency.ro/ro/strategia-nationala-de-aparare-a-tarii1444725665
14. https://ziare.com/scoala/educatie/educatia-este-in-momentul-de-fata-amenintare-la-adresa-securitatii-nationale-presedintele-iohannis-sa-puna-tema-pe-masa-csat-interviu-1589801

HUMAN CAPITAL IN THE CONTEXT OF THE FUNCTIONING OF THE LABOR MARKET IN THE DIGITAL ERA

CAPITALUL UMAN ÎN CONTEXTUL FUNCȚIONĂRII PIEȚEI MUNCII ÎN ERA DIGITALĂ

Abramihin Cezara
Doctor în științe economice, conferențiar universitar
Academia de Studii Economice a Moldovei
e-mail: czr777@gmail.com

Abstract
The digitalization of the economy puts employees and employers in front of the need to adapt to the new conditions. The widespread digitization of business models and entire branches will lead to the partial replacement of the human labor force with robotic labor and the release of a significant share of the living labor force, which will create new difficulties for companies and the state. The development of the digital economy leads to qualitative changes in the labor market and human capital and leads to the formation of a new socio-economic paradigm.

Keywords: *skills, abilities, human capital, competitiveness, labor market.*

JEL Classification: *J0, J08, J4, I2, I25, I28*

INTRODUCERE

Capitalul uman este o sumă de trăsături, toate cunoștințele, talentele, abilitățile, dar și experiența, inteligența, educația, judecata și înțelepciunea deținute individual și colectiv de către indivizii unei populații. Capitalul uman este și capacitatea unei persoane de a genera venituri. [4]

Este necesar să se facă distincția între competitivitatea capitalului uman al individului și competitivitatea persoanei însuși pe piața muncii. Prima este legată de potențialul său de a obține succese în angajare sau în dezvoltarea carierei; a doua - de realizarea acestui potențial, care depinde atât de factorii obiectivi cât și de cei subiectivi: productivitatea muncii, atitudinile șefilor, discriminări posibile și propriul comportament.

CONSIDERAȚII GENERALE

Digitalizarea economiei pune angajații și angajatorii în fața nevoii de adaptare la noile condiții. În deceniile următoare digitalizarea pe scară largă a modelelor de business și a ramurilor întregi va duce la înlocuirea parțială a forței de muncă umane cu forța de muncă robotizată și eliberarea unei cote semnificative a forței de muncă vii, ceea ce va crea noi dificultăți pentru companii și stat. Dezvoltarea economiei digitale a condus la schimbări calitative pe piața muncii și a capitalului uman și a condus la formarea unei noi paradigme socio-economice.

În același timp, tehnologiile și platformele digitale pot avea și un impact pozitiv vizibil asupra pieței muncii. Impactul digitalizării asupra dinamicii ocupării forței de muncă nu poate fi ușor de separat de impactul altor tendințe, cum ar fi o recesiune economică generală sau o transferare a producției în străinătate. Dar, totuși, unele efecte sunt evidente. Raportul Institutului Global McKinsey privind piața forței de muncă din SUA indică faptul că recuperarea din recesiuni a fost însoțită de mai puține locuri de muncă. În crize economice, companiile mari caută să îmbunătățească productivitatea nu

prin creșterea producției sau introducerea de inovații, ci prin reducerea numărului de angajați. Automatizarea producției a devenit un proces permanent și locurile de muncă sunt afectate în perioadele de încetinire economică sau recesiune [1]. În plus, introducerea tehnologiilor digitale duce la o reducere a numărului de lucrători cu calificări medii. Roboții înlocuiesc lucrătorii de pe benzi transportoare, iar sistemele informaționale încep să efectueze operațiuni din responsabilitățile contabililor, secretarilor și a alor lucrători de birou.

Digitalizarea a accelerat creșterea decalajului între angajații cu salarii reduse și cu salarii mari. Companiile digitale arată cea mai mare creștere a salariilor, dar în ceea ce privește numărul de locuri de muncă, ponderea lor în structura generală a economiei este mică.

Pe de altă parte, digitalizarea are și un impact pozitiv asupra pieței muncii, datorită apariției unor noi profesii care nu existau până acum. În plus, dezvoltarea platformelor Internet crește mobilitatea lucrătorilor.

În viitor, prin colectarea de informații despre necesitatea în anumiți specialiști, oamenii vor putea să-și planifice mai bine studiile și carierele. Tehnologiile digitale creează ascensoare sociale, estompează granițele geografice, permit rezidenților din localități îndepărtate să primească educație de calitate, să-și îmbunătățească calificările și să găsească un loc de muncă, nefiind limitați de oportunitățile condiționate de localitatea în care se află. Piața muncii este amenințată de pierderea locurilor de muncă, compensată parțial de o creștere a eficienței pieței muncii. Experții digitali sunt de acord că automatizarea va avea un impact semnificativ asupra pieței forței de muncă în următoarele decenii. Conform estimărilor Institutului Global McKinsey [2], până în 2036 ăn lume vor fi automatizate până la 50% din procese de muncă. Acest lucru va duce la disponibilizări semnificative de personal, la o reducere a numărului de locuri de muncă de nivel mediu și la o creștere a diferențelor salariale.

Într-o analiză comparativă a structurii pieței forței de muncă din diferite țări [3], s-au împărțit condiționat toți angajații din economie în trei categorii: 1) „Abilități"; 2) „Regulă"; 3) „Cunoștințe" în conformitate cu abordarea lui J. Rasmussen pentru clasificarea sarcinilor care sunt stabilite pentru angajați [5].

Categoria „Abilități" include angajații ale căror activități sunt legate în principal de munca manuală, mai mult de 50%, totodată, pentru ei nu necesită instruire specială, instruirea lor se desfășoară în cadrul cursurilor de formare pe termen scurt (munca deridicătorilor, vânzătorilor, șoferilor, hamalilor, agenților de pază etc). Categoria „Abilități" dețin nivelul de bază de aptitudini: îndeplinesc sarcini mecanice.

Categoria „Regulă" este alcătuită din angajați care efectuează mai mult de 50% din munca tehnică și de rutină, în care procesul decizional se bazează pe reguli și instrucțiuni clare. Pentru pregătirea acestora, este necesară o pregătire specializată și aplicativă (munca lăcătușilor, contabililor, asistentelor medicale, administratorilor de birouri). Categoria „Regulă" dețin nivel mediu de calificare: îndeplinesc sarcini cognitive de rutină.

Categoria „Cunoștințe" include angajații a căror muncă în pondere mai mare de 50% necesită muncă analitică, improvizație în condiții de incertitudine, în același timp există un nivel ridicat de autonomie în procesul decizional. Categoria „Cunoștințe" execută munca intelectuala foarte calificată: îndeplinesc sarcini cognitive complicate. Pentru pregătirea lor, este necesar un nivel ridicat de educație cu un ciclu lung de formare (munca profesorilor, medicilor, cercetătorilor, inginerilor de înaltă calificare, managerilor).

Diferența-cheie între țările moderne cu traiectorie de dezvoltare „superioară" față de restul țărilor este structura pieței muncii, și anume, în aceste țări mai mult de 25% dintre angajați dețin posturile așa-numitei categorii „Cunoștințe" (tab.1).

Tabelul 1. Trei segmente de țări cu ponderile angajaților în categoriile: „Abilități"; „Regulă"; „Cunoștințe"

Caracteristicile tipului de economie	*Țările*	*Angajații din categoria „Abilități" (%)*	*Angajații din categoria „Regulă" (%)*	*Angajații din categoria „Cunoștințe" (%)*
Economia resurselor: Populație tânără neinstruită, Vârsta medie 21 ani Educație terțiară – 5% Index de dezvoltare umana – scăzut PIB – med. 1750 $/locuitor Economie digitală foarte slab dezvoltată	Etiopia	67	32	1
	Uganda	57	41	2
	Zimbabve	57	41	2
Perioada de tranziție: Populație instruită îmbătrânindă, Vârsta medie 35 ani Educație terțiară – 50% Index de dezvoltare umana – mediu PIB – med. 29000 $/locuitor Acoperire cu internet 50% din populație	Malaezia	51	41	8
	Arabia Saudită	43	49	8
	Kazahstan	50	39	11
	Brazilia	40	45	15
	Rusia	35	48	17
Economia cunoștințelor: Populație foarte instruită îmbătrânindă, Vârsta medie 45 ani Educație terțiară – 60% Index de dezvoltare umana cel mai înalt PIB cel mai înalt – med. 52000$/ locuitor Acoperire cu internet practic totală – 85% din populație	Coreea de Sud	25	53	22
	Japonia	30	45	25
	SUA	17	59	24
	Germania	15	56	29
	Singapur	18	48	34
	Marea Britanie	18	37	45

Sursa: [3, p.12]

Proporția ridicată de angajați din categoria „Cunoștințe" implicați în munca cognitivă non-rutină este astăzi principalul motor al dezvoltării capitalului uman și un indicator al competitivității globale a economiei, iar efectul acestui indicator cu timpul doar va crește.

Examinând această situație prin prisma dezvoltării pieței forței de muncă [3, 6], putem afirma că motorul dezvoltării capitalului uman ca factor de creștere economică este dezvoltarea unei metodologii de gestionare a capitalului uman cu scopul de a crește numărul angajaților din categoria „Cunoștințe".

În același timp, rolul decisiv este atribuit creării unui spațiu profesional și educațional unic în triada tuturor participanților la acest proces: statul, sistemul de învățământ superior și angajatorii. În următorii 5-10 ani, structura economică și piețele forței de muncă vor fi modelate de tendințele cheie care afectează deja structura ocupării forței de muncă în economia globală și vor continua să stimuleze schimbări semnificative pe termen mediu.

Țările dezvoltate discută deja în mod activ despre ce măsuri ar trebui luate în acest sens: de a efectua o recalificare masivă, de a stabili un venit de bază garantat sau de a introduce un impozit pe roboți propus recent de Bill Gates? Anumite măsuri de această natură sunt deja în curs de pilotare în unele țări.

Cu toate acestea, tehnologiile de inteligență artificială au un impact pozitiv asupra pieței muncii. De exemplu, platformele digitale creează noi oportunități de muncă; ele contribuie la dezvoltarea abilităților și calificărilor suplimentare, în special pentru

persoanele care anterior nu aveau astfel de oportunităţi din cauza constrângerilor sociale sau geografice. Apar noi profesii legate de digital și locuri de muncă bine plătite.

Un exemplu ilustrativ este General Electric, o companie tradițională de inginerie americană care și-a propus să devină una dintre cele mai mari zece companii de dezvoltare software din lume până în 2020 și acum atrage activ specialiști digitali calificați. În special, General Electric intenționează să mărească numărul de dezvoltatori din personalul său la 20 de mii de oameni. Pentru o companie de inginerie, aceasta este o strategie revoluționară și un obiectiv fără precedent. Ocuparea forței de muncă pe segmentele care necesită calificări mai mici va fi caracterizată de o concurență sporită pentru locurile de muncă. În același timp, sarcina angajaților cu înaltă calificare va crește constant. Până în 2025, ținând seama și de îmbătrânirea populației și de intrarea pe piața muncii a lucrătorilor tineri din generația Z, natura concurenței pentru angajați se va schimba semnificativ. Până în 2025, generația Z (născută în 1997 și mai tânără) va reprezenta aproximativ 25% din forța de muncă totală [2].

Aceștia sunt persoanele care au folosit tehnologii digitale încă de la naștere (nativi digitali) și au acces nelimitat la informații. Creșterea personală, echilibrul dintre viața profesională și viața personală pentru ei este în prioritate comparativ cu recompensa financiară și cariera. Spre deosebire de generațiile anterioare, generația Z sunt predispuți de a schimba destul de des nu numai angajatorii, ci și domeniile de activitate. Ei au adesea un set de competențe digitale mai avansat decât profesorii și supraveghetorii lor. În lupta pentru noi angajări, organizațiile vor trebui să se adapteze valorilor lor.

Într-un astfel de mediu, forța de muncă digitală este un atu strategic. Deficitul său va duce inevitabil la o încetinire a ratelor de creștere atât a economiei digitale, cât și a economiei țărilor în ansamblu. Astfel, furnizarea pieței muncii cu numărul necesar de specialiști calificați în tehnologiile digitale devine o prioritate de stat, iar această sarcină va trebui realizată cu ajutorul unui sistem modern de educație de înaltă calitate.

Digitalizarea va facilita căutarea personalului, va reduce timpul necesar pentru a găsi un loc de muncă, va crește productivitatea angajaților, va îmbunătăți situația cu implicarea personalului în economie prin lucrul la distanță și va oferi acces la educație de calitate.

Din partea statului, a afacerilor și a instituțiilor de învățământ, vor fi necesare acțiuni timpurii coordonate pentru pregătirea viitoarelor schimbări, precum și pentru recalificarea și angajarea personalului eliberat.

Odată cu continuarea transformarilor digitale a sectoarelor economice, introducerea sistemelor de automatizare și robotizare, creșterea productivității muncii și înlocuirea canalelor de servicii fizice cu cele digitale, tot mai multe locuri de muncă pot dispărărea. Potrivit McKinsey Global Institute, până în 2036 pot fi automatizate de la 2 până la 50% din muncă, exprimată în om-ore, iar până în 2066 această pondere poate ajunge de la 46 la 99%. Acest proces va afecta în primul rând locurile de muncă care necesită calificări medii, deoarece este cel mai ușor de automatizat acele tipuri de muncă care necesită executarea unor operații fizice repetitive, previzibile, precum și activități pentru colectarea și analiza informațiilor. [2]

Pentru dezvoltarea cu succes a economiei digitale, sistemul de educație și recalificare trebuie să ofere economiei specialiști care îndeplinesc cerințele erei digitale. Statele care vor reuși să își adapteze infrastructura educațională la noile nevoi vor putea să își consolideze semnificativ pozițiile economice în tranziția către economia digitală.

CONCLUZII

Capitalul uman este un factor-cheie într-o economie digitală competitivă. Evoluția relațiilor sociale a condus la faptul că informațiile, cunoștințele și personalul digital devin factori importați de producție.

Pentru a crea capital uman care să răspundă nevoilor pieței muncii într-o economie digitală, este necesar:

1. Actualizarea programelor de educație și formare profesională învechite pentru acoperirea lipsurilor de competențe digitale necesare într-o economie modernă.
2. Pe termen lung, sistemul de învățământ la toate nivelurile are nevoie de o transformare mai ambițioasă bazată pe principii precum învățarea continuă; flexibilitatea traiectoriilor educaționale; modularitatea cursurilor educaționale. În același timp, atenția ar trebui să se concentreze asupra dezvoltării abilităților personale, sociale și a abilităților de rezolvare a problemelor interdisciplinare, concentrate pe practic. Totodată este necesar de concentrat pe utilizarea metodelor moderne de instruire, formatelor și instrumentelor didactice noi, inclusiv instrumentelor educaționale digitale și formatelor de educație la distanță.
3. Pentru a asigura dezvoltarea profesională a unui astfel de personal în Moldova, este necesar să se îmbunătățească platformele de interacțiune dintre studenți și potențiali angajatori, să se creeze condiții favorabile pentru dezvoltarea companiilor tehnologice și a startapp-urilor și să se ia măsuri pentru îmbunătățirea calității vieții în ansamblu.
4. Dezvoltarea de noi centre de excelență în cele mai solicitate domenii tehnologice. Există un dezechilibru al competențelor pe piața muncii, ceea ce duce la o situație în care va exista atât șomaj, cât și o lipsă de personal calificat
5. Să fie dezvoltată interacțiunea între organizațiile educaționale și de cercetare, cu comunitatea de afaceri și cu agențiile guvernamentale, pentru a asigura relevanța și semnificația programelor educaționale și pentru a reduce timpul de adaptare a sistemului educațional la cerințele pieței. În plus, în afară de modernizarea sistemului de pregătire a cadrelor, este de asemenea necesar să se asigure posibilitatea autorealizării cadrelor în Republica Moldova.

BIBLIOGRAFIE

1. Aboody D., Lev B. *Information asymmetry, R&D, and insider gains* // The Journal of Finance, 2000. – № 6.
2. Akerlof G.A. *The Market for 'Lemons': Quality Uncertainty and the Market Mechanism.* Quarterly // Journal of Economics, 1970. – № 84(3).
3. Butenco V., Polunin C., Cotov I., Sîciova E. Rossia 2025: *Ot cadrov k talantam.* The Boston Consulting Group. REVIEW. N42, 2017. pp. 8 – 19.
4. Kuzminov Ya.I., Ovcharova L.N., Yakobson L.I. (2016). *Chelovecheskiy kapital kak faktor sotsialno-ekonomicheskogo razvitiya* [Human capital as a factor of socioeconomic development] Annual report on social policy.
5. Rasmussen I., Skills, Rules, and Knowledge; Signals, Signs, and Symbols, and other distinctions in Human Performance models, 1983.
6. *The Global Talent Competitiveness Index 2019. Entrepreneurial Talent and Global Competitiveness*. Bruno Lanvin Felipe Monteiro Editors, ISBN: 979-10-95870-18-0. Available at: https://gtcistudy.com/wp-content/uploads/2019/01/GTCI-2019-Report.pdf

ENSURING THE SUSTAINABLE ECONOMIC SECURITY OF THE REPUBLIC OF MOLDOVA IN THE EUROPEAN INTEGRATION CONTEXT

ASIGURAREA SECURITĂȚII ECONOMICE DURABILE A REPUBLICII MOLDOVA ÎN CONTEXTUL INTEGRĂRII EUROPENE

Furculița Tatiana
Doctorand, Academia de Administrare Publică
e-mail: jardantt@gmail.com

Dulschi Silvia
Doctor în științe economice, conferențiar universitar
Academia de Administrare Publică
e-mail: silvia_moldovan@mail.ru

Abstract
As matters stand, the country's economic security is one of the most important condition for the development of the state, by ensuring a high level of quality of life of citizens and increasing the income of the population, which intensifies the purchasing power and gives the citizens the sense of security. European integration offers perspectives and strategic development opportunities for economic security, including for the reform of public administration, by increasing their professional development and achieving a new model of human resource performance, in order to develop and promote effective policies and strategies at national level, for ensuring a sustainable economic security. The authors analyze the opportunities to ensure economic security, in the conditions of European integration, and for benefits at national level. As a research method, the comparative method, the systemic method and the analytical method were used. The research recommends measures to ensure sustainable economic security for the country's European course.

Keywords: *economic security, European integration, sustainable development, public administration, performance model, globalization, national interest, economic security, economic goals*

JEL Classification: *P4 10 Other Economic Systems: Planning, Coordination, and Reform*

INTRODUCERE

Republica Moldova și Uniunea Europeană (UE) au o relație de cooperare începând cu anul 1994, atunci când a fost semnat Acordul de Parteneriat şi Cooperare dintre Comunitățile Europene și statele lor membre, pe de o parte, și Republica Moldova, pe de altă parte.

Un pas important în procesul integrării europene a Republicii Moldova a constituit semnarea la Bruxelles, la 27 iunie 2014, Acordului de Asociere a Republicii Moldova cu Uniunea Europeană [1, p.9].

În domeniul politicii externe şi de securitate comună a Uniunii Europene, Acordul de Asociere prevede intensificarea dialogului politic UE-Moldova şi cooperarea în vederea convergenței graduale în sectoarele acoperite de Politica Externă și de Securitatea Comună (PESC), și anume abordează aspecte privind următoarele:

- ✓ Promovarea păcii și a justiției internaționale;
- ✓ Prevenirea conflictelor şi gestionarea situaţiilor de criză;
- ✓ Promovarea stabilităţii, securităţii şi dezvoltării democratice în regiune. Soluţionarea paşnică a conflictelor regionale;
- ✓ Combaterea proliferării armelor de distrugere în masă şi materialelor conexe, precum şi a mijloacelor de livrare a acestora;

- ✓ Combaterea terorismului;
- ✓ Combaterea comerţului ilicit cu arme de calibru mic şi armament uşor, inclusiv cu muniţiile pentru acestea.

Prin urmare, Republica Moldova se angajează în sensul acordării de sprijin activ şi necondiţionat pentru implementarea politicii externe şi de securitate comună, în spiritul loialităţii şi al solidarităţii reciproce. Perspectiva participării Republicii Moldova la politica externă și de securitate comună a Uniunii Europene reprezintă o contribuție la asigurarea securităţii internaţionale. O cooperare complexă şi de durată în domeniu dat va spori creşterea rolului Uniunii Europene în soluţionarea conflictului transnistrean, implicit participarea la o nouă misiune internaţională în Zona de Securitate.

De asemenea, prin Acordul de Asociere, Republica Moldova își propune crearea unei administrații publice eficiente, responsabile, credibile, transparente și deschise în relația cu beneficiarii serviciilor sale, contribuind, astfel, la sporirea capacităților instituționale și ale resurselor umane ale administrației publice centrale și locale pentru a îmbunătăți eficiența activității acestora. O astfel de administrație își va concentra efortul în punerea în aplicare a legii și furnizarea de servicii publice de calitate. În acest sens, cetățenii Republicii Moldova vor beneficia de procese decizionale coerente, resurse umane competente și bine gestionate, o structură instituțională administrativă adecvată, proceduri de funcționare clare, simple (e-guvernanță), o atitudine și cultură organizațională centrate pe promovarea interesului public, precum și un management eficient și transparent al cheltuielilor publice. Reformarea administrației publice va asigura reducerea birocrației și eliminarea corupției. Reforma în domeniul administrației publice este implementată în R. Moldova cu suportul UE.

Proiectul ”Suport pentru modernizarea serviciului public din Republica Moldova în corespundere cu cele mai bune practici europene” presupune ajustarea cadrului normativ conform celor mai bune practici europene, planificarea și implementarea programului național de instruire a funcționarilor publici, crearea unei rețele de experți în domeniul resurselor umane și dezvoltarea capacităților tuturor secretarilor de stat din cadrul ministerelor. Prin urmare, va fi atins un nou nivel de performanță al funcționarilor publici.

CONSIDERAȚII GENERALE

Securitatea economică, ca fenomen social complex, reprezintă un obiect de cercetare științifică pentru mulți cercetători din diferite domenii, care stduiază problema respectivă, ținând cont de specificul și particularitățile acesteia. Astfel, economiștii care cercetează problematica asigurării securității economice la nivel național, se orientează spre studierea relațiilor economice din perspectiva principiului securității, care presupune existența atât a infrastructurii economice, cât și a forței de muncă calificate, cu un nivel înalt de productivitate.

Noţiunea de „securitate economică” este întâlnită extrem de des în strategiile naționale, inclusă ca prioritate în agendele conferințelor internaționale, fără ca în literatura de specialitate să existe definiţii unanim acceptate de toți cercetătorii din domeniu. În cele mai multe lucrări adiacente temei, se întâlnesc definiţii sau explicaţii intuitive referitoare conceptului, ca de exemplu: „siguranța zilei de mâine”, care intră în substituţie cu alți termeni ca: prosperitate, bunăstare, standard de viaţă adecvat, independenţă economică, etc.

O explicaţie succintă a modului în care au evoluat conceptele de securitate economică, subliniază că acestea au cunoscut două abordări:

- ✓ Microeconomică – standarde înalte de viaţă pentru cetăţeni;
- ✓ Macroeconomică – creşterea puterii economice naţionale.

În același timp, securitatea economică reprezintă totalitatea condițiilor interne și externe, propice creșterii efective dinamice a economiei naționale, capacității sale de a satisface necesitățile societății, statului, individului, asigurând competitivitatea pe piețele externe, protejând de pericole și pierderi de diferit gen [2, p.67].

Sub aspect teoretico-practic, securitatea economică a unei țări, poate fi analizată în următoarele modalități:

- din punct de vedere economic, securitatea cetățenilor este resimțită prin independența financiară a acestora; altfel spus, lipsa veniturilor, șomajul, nivelul de sărăcie, se echivalează cu un sentiment de nesiguranță;
- din punct de vedere social, securitatea cetățenilor este asigurată și de comportamentul societății în mediul economic al țării, prin reacția societății la diferite probleme de ordin general: infracțiuni, droguri, poluare etc.

Nivelul securității economice, măsurat atât în natură, cât și în grade diferite, afectează interesele tuturor statelor lumii, reprezentând în același timp acea stare de siguranță și protecție economică de amenințările externe și interne. Este important de evidențiat facptul că scopul unei politici eficiente în domeniul securității economice este de a asigura o dezvoltare economică durabilă pentru satisfacerea nevoilor sociale și economice ale cetățenilor țării la un cost optim de muncă și utilizarea rațional-ecologică a resurselor mediului înconjurător.

Autorii subliniază că un indicator al sporirii nivelului securității economice este reprezentat de creșterea stabilă a productivității muncii, cu minim 5% pe an. De asemenea, autorii sunt de părere că securitatea economică a unei țări depinde și de nivelul de dezvoltare al forțelor de producție și al relațiilor economice, dar și de forța de muncă calificată și existența unui sistem de perfecționare a acesteia. Prin urmare, buna funcționare a sectorului securității economice naționale este indispensabilă de activitatea instituțiilor cu competențe proprii pe multiplele dimensiuni ale securității, și aici sunt incluse toate ministerele și organizațiile de stat din administrația publică centrală și locală, care participă nemijlocit la elaborarea și promovarea unor politici economice, menite să atingă obiectivele statului sub aspect economic. Așadar, este evident și rolul funcționarilor publici în asigurarea securității economice naționale, prin valorificarea la maxim a acestor resurse umane. Se impune, astfel, crearea unui nou model de performanță a funcționarilor publici, racordat la standardele UE, conform prevederilor Acordului de Asociere. În rezultat, se va obține dezvoltarea profesională a angajaților din instituțiile publice și elaborarea unor reglementări corecte și echitabile în vederea asigurării securității economice, și promovarea politicilor necesare.

Securitatea economică, în esența sa, vizează asigurarea condițiilor pentru menținerea activității economice în parametrii normali și contracararea a numeroase tipuri de atacuri dintre cele mai importante sunt următoarele: fraude financiare, dependențe strategice, ciber-criminalitate, spionaj industrial, corupție, economie subterană, etc. [7, p.127].

În opinia autorilor, securitatea economică a Republicii Moldova este amenințată și de următorii factori:

- lipsa de protecție a intereselor economice strategice a țării;
- blocarea accesului la resurse strategice de energie electrică, gaze naturale, apă potabilă etc.;
- distrugerea cu intenție sau din culpă a unor elemente ale infrastructurii țării ori monopolizarea acestora;
- subminarea intereselor financiar-bancare strategice ale Republicii Moldova;
- calamități naturale, ce pot determina situații de urgență în Republica Moldova;

- instabilitatea sistemelor informaționale;
- fenomenul accentuat al corupției;
- prelucrarea necalitativă și utilizarea nesatisfăcătoare a informațiilor ce vizează interesele naționale;
- utilizarea anumitor tehnologii uzate sau depășite;
- emigrarea specialiștilor de înaltă calificare și slăbirea potențialului de cercetare-dezvoltare a țării etc.

O diferită abordare a amenințărilor asupra securității economice în lumea contemporană, este analiza efectelor pe care aceste amenințări le au asupra întregului mapamond. În opinia economistei Lavinia Florea, actualmente dintre cele mai importante amenințări globale asupra securității economice se disting:

- Sărăcia;
- Șomajul;
- Crizele financiare;
- Lipsa competitivității economice;
- Protecția socială deficitară;
- Delocalizările și externalizările [3, p.35].

Nici un stat nu posedă 100% resurse necesare (materii prime, piață de desfacere, potențial științific și tehnologic, infrastructură, etc) și nu este de sine-stătător, astfel, fiecare țară este nevoită să participe la comerțul internațional pentru a obține materiale esențiale pentru dezvoltarea sa internă. Statele mici întotdeauna au fost forțate să participe în relațiile comerciale, care să permită străinilor să joace rol important pentru supraviețuirea lor și, în același timp, a se face vulnerabile, deoarece sunt mai slabe economic și au piețe interne mai mici, acestea nu au nici un control asupra puterilor mai mari, dar fără a se deschide nu au posibilitate de a deveni competitive.

Creșterea rapidă, echilibrată și durabilă a economiei este vitală pentru atingerea obiectivelor politicii de securitate a Republicii Moldova. Este în interesul național al Republicii Moldova de a promova diversificarea relațiilor economice externe. În acest scop este important de a menține un mediu economic stabil, care, alături de alți factori, asigură atractivitatea Republicii Moldova pentru capitalul străin.

Republica Moldova asigură credibilitatea sistemului său financiar. În scopul aplanării crizelor internaționale și a consecințelor lor economice, este necesar de a asigura o stabilitate durabilă și rezerva de fonduri în cadrul sistemului financiar al țării.

Scopul politici economice este de a atinge o dezvoltare economică și socială durabilă. Având în vedere că mediul macroeconomic stabil constituie o precondiție importantă a creșterii, prezervarea acestuia devine o sarcină primordială a politicii economice a Guvernului [4].

În acest sens, prioritățile Republicii Moldova pe termen lung sunt următoarele: crearea condițiilor favorabile pentru funcționarea economiei, stimularea creării structurilor industriale eficiente și competitive, precum și reducerea disproporțiilor și riscurilor economice. În afară de aceste sarcini, este necesar de a ameliora politica națională de impozitare, atrăgând o atenție deosebită colectării impozitelor.

În scopul asigurării securității economice, este necesar de a diversifica economia și a o orienta spre bunuri și servicii cu valoare adăugată înaltă. Pe parcursul diversificării economiei naționale este necesar de a spori semnificația industriilor de perspectivă care până în prezent nu au fost dezvoltate, între timp, utilizând la maxim, avantajele industriilor curente. Republica Moldova va promova politica dezvoltării bazate pe inovare, crearea și

funcţionarea sistemului inovaţional. Se va încuraja consolidarea competitivităţii şi cuceririi noilor pieţe externe

Creând condiţii necesare pentru dezvoltarea economiei, este important de a crea un mediu favorabil pentru promovarea businessului, de a dezvolta o politică de stat de asistenţă orientată spre acest obiectiv, de a ameliora sistemul fiscal şi administrarea acestuia, precum şi de a crea un sistem de trening şi consultanţă pentru agenţii economici şi oamenii de afaceri.

Pentru consolidarea securităţii economice durabile, economiştii contemporani, dar nu numai, au ajuns la concluzia că parteneriatele strategice au un rol semnificativ. Securitatea prin cooperare se bazează pe asocierea partenerilor în vederea atingerii unor valori comune, printre care prioritare sunt democraţia respectarea drepturilor şi libertăţilor omului, supremaţia legii, economii bazate pe piaţă liberă, echitate socială şi progres. Parteneriatele sunt modalităţi eficiente de securitate economică, politică, informaţională şi militară a statelor şi entităţilor internaţionale şi regionale. Într-o epocă în care pericolele şi ameninţările se succed cu o repeziciune greu de contracarat şi de gestionat, ele oferă modalităţi eficiente de concentrare şi fuziune a eforturilor pe treapta cea mai directă de securitate, cea bilaterală (între 2 state) sau multilaterală (între mai multe state). Fiind o soluţie de stabilitate, stabilizare şi siguranţă într-o lume a nesiguranţei, haosului şi confruntării, parteneriatele cunosc o dinamică fără precedent. De aceea, epoca globalizării este, prin excelenţă, o epocă a dinamicii parteneriatelor.

Un posibil model al asigurării **securităţii economice durabile** se bazează pe doi piloni de bază: securitatea economică internă – dezvoltare economică durabilă, promovarea unor politici pentru creşterea bunăstării populaţiei; securitate economică externă – colabolare strânsă cu organizaţiile internaţionale, promvare unei politici externe consecvente şi echilibrate, îndeplinirea condiţiilor parteneriatelor şi oferirea garanţiilor partenerilor externi [6, p.115].

Experienţa UE în domeniul asigurării securităţii economice se caracteriează de o intensă cooperare în domeniul economic, iar apogeul acestei colaborări comunitare, al puterii economice europene o constă în capacităţile sale economice şi financiare remarcabile, unele dintre cele mai moderne din lume. Iniţiativele şi strategiile îşi arată deja roadele, întrucât în a doua jumătate a anului 2013 UE înregistrează un trend pozitiv a PIB-ului, ceea ce semnifică sfârşitul recesiunii.

Indicatori economici ai UE au oferit în cea mai mare parte semnale pozitive începând din aprilie 2013, şi sugerează în continuare o creştere modestă în a doua jumătate a anului. Recuperarea rămâne supusă şi fragilă pentru că obstacolele generate de criza economico –financiară nu sunt depăşite şi continuă să influienţeze activitatea economică.

Pentru **asigurarea securităţii economice durabile** a UE este creată piaţa internă unică, care acoperă întreg spaţiul statelor membre - fără frontiere interne. În cadrul acestui spaţiu este asigurată libera circulaţie a persoanelor, serviciilor, mărfurilor şi capitalului. În mod practic, crearea spaţiului unic regional evită fragmentarea pieţei. În acest scop sistemul garantează libertatea de stabilire: fiecare agent economic are dreptul de a stabili şi a dezvolta afaceri într-un alt stat membru al UE [8, p.125].

Pentru asigurarea securităţii economice naţionale, un aspect important este reprezentat de monitorizarea situaţiei securităţii economice a Republicii Moldova, şi de stabilirea unor măsuri pentru prevenirea şi apariţia unor eventuale pericole. Autorii propun următoarele acţiuni ca măsuri de asigurare a securităţii economice:

- reducerea PIB-ului per locuitor şi ridicarea nivelului calităţii vieţii populaţiei la un nivel mai apropiat de cel mediu al UE, pentru diminuarea decalajului evident dintre acestea, să devină ca obiectiv economic strategic promovat la nivel naţional;

- crearea unui mediu de afaceri favorabil activităților de inovare, dar și promovarea unei politici bine definite în domeniu, referitoare la stimularea activităților de cercetare-dezvoltare-inovare, cu accent deosebit pe inovare și transfer tehnologic, pentru o valorificare rapidă a rezultatelor, în scopul majorării considerabile a productivității muncii;
- creșterea calității managementului economic la toate nivelurile, pentru utilizarea eficientă a resurselor financiare proprii disponibile, dar și atragerea surselor de finanțare suplimentare în scopuri de investiții, pentru dotarea cu tehnologii modern, cercetări științifice, dezvoltare tehnologică, activități de inovare, dar și formarea și perfecționarea resurselor umane, pentru creșterea performanțelor acestora;
- asigurarea potențialului reproductiv al țării și soluționarea problemei exodului masiv de creativitate și inteligență;
- promovarea la nivel național a unor politici de economisire a resurselor ce vor contribui la consolidarea securității energetice, prin economisirea riguroasă a energiei și sporirea rentabilității producției, eficienței, transportului și consumului de energie;
- reorganizarea structurală a economiei, prin efectuarea investițiilor de proporții ca urmare a ameliorării climatului investițional;
- implicarea activă a statului și sectorului privat în menținerea unui mediu de afaceri favorabil investițiilor de capital autohton și străin, care sunt destinate modernizării și dezvoltării durabile a țării;
- continuarea politicilor de atragere a investițiilor străine directe;
- asigurarea unor condiții prielnice pentru desfășurarea exporturilor și importurilor și a unui raport de schimb internațional favorabil.

CONCLUZII

În concluzie, pentru elaborarea concepției naționale de securitate economică a Republicii Moldova, este necesară trecerea de la practicile obișnuite la o dezvoltare durabilă, în contextul integrării europene, printr-un nivel înalt de reglementare de către stat a proceselor economice, ce va reglementa și va garanta o dezvoltare continuă și eficientă a economiei, care în rezultat ar asigura soluționarea echilibrată a obiectivelor social-economice, a problemelor protejării mediului ambiant cu scopul satisfacerii necesităților generațiilor actuale și viitoare.

Din sectorul securității naționale a Republicii Moldova, fac parte și instituțiile de stat cu atribuții în anumite domenii de seuritate, care activează în conformitate cu legislația în vigoare, și care au ca obiectiv de activitate protejarea cetățenilor și a statului.

Stabilitatea este primordială în asigurarea securității economice durabile, iar un stat este puternic dezvoltat din punct de vedere economic, dacă este stabil.

Fortificarea securității economice durabile în epoca fenomenelor de globalizare și regionalizare poate fi realizată prin intermediul parteneriatelor strategice, or vectorul strategic al politicii externe al Republicii Moldova este integrarea europeană. Acest parteneriat semnifică: consolidarea puterii economice, reducerea riscurilor, realizarea intereselor economice și pe cale de consecință – fortificarea securității economice a țării, asigurarea condițiilor pentru gestionarea crizelor, consolidarea stabilității, etc. Accesul oportun, util și benefic la o piață imensă, oferă posibilitatea dezvoltării unui sistem economic bazat pe inovare, competitivitate, colaborare cu instituțiile internaționale [Munteanu C., 2015, p.3].

Securitatea economică durabilă a Republicii Moldova poate fi obținută prin: *dezvoltarea unui sistem educațional modern* – astfel încât să avem forță de muncă calificată și competitivă, *reducerea economiei subterane* – crearea condițiilor pentru ca activitățile din

economia subterană să se transforme în activități oficiale, *diversificarea piețelor de desfacere* – diminuarea dependenței și crearea unei imagini poozitive a țării dincolo de hotarele ei, *diversificarea surselor de energie* – reducerea dependenței de monopolul rusesc și încadrarea în piața energetică europeană, *reintegrarea teritoriului Republicii Moldova*.

Parcursul european per general și Acordul de Asociere în particular înseamnă pentru Republica Moldova instrumentul principal în acest sens: reforme pentru combaterea corupției, dezvoltarea statului de drept, dezvoltarea durabilă a unei economii de piață viabile, creșterea securității energetice, etc Actualmente se discută sectorial despre domenii care necesită intensificarea eforturilor şi acţiunilor, cum ar fi: reforma justiţiei, combaterea corupţiei şi sectorul bancar.

BIBLIOGRAFIE

1. Creangă I., Bostan O. Beneficiile acordului de asociere UE-RM, Chișinău, 2015. IDIS Viitorul. Disponibil on-line [http://dcfta.md/uploads/0/images/large/4946294-md-ghid-ue-final.pdf]. Accesat: 25.11.2020
2. Daniliuc A. Securitatea economică a Republicii Moldova: Amenințări și perspective. În Revista: Vector European, nr. 1, din 2018. ISSN: 2345-1106. p.67-70
3. Florea L. Globalizare şi securitatea economică. Ed. Lumen, Iaşi 2006, p.30-39
4. Hotărârea Parlamentului nr. 153 din 15.07.2011, pentru aprobarea Strategiei securității naționale a Republicii Moldova. În Monitorul Oficial nr. 170-175, art. 499
5. 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, ISBN 978-617-7172-39-9
6. Munteanu C. Asigurarea securității economice durabile a Republicii Moldova în procesul asocierii la Uniunea Europeană. Teză de doctor în științe economice. 2016. p.191
7. Șoimu O., Trofimov V. Securitatea economică a Republicii Moldova: unele probleme și căi de soluționare. În: Revista Științifică a Universității de Stat din Moldova, 2007, nr.8. Seria Științe exacte și economice. ISSN 1857-2073. p.126-128
8. Țurcanu V., Cojocaru V. Securitatea economică a statului mic. Cazul Republicii Moldova. În Revista Administrarea Publică, nr. 2 (90), 2016. ISSN: 1813-8489. p.124-134

CENTRAL BANKS IN ACHIEVING FINANCIAL STABILITY

Mariana M. Daou
PhD, student
The "D.A. Tsenov" Academy of Economics, Svishtov, Bulgaria
e-mail: mfmanagement17@gmail.com

Abstract
The main objective of this paper is to analyze the evolving role of central banks in fostering financial stability and look at some current issues that have practical and operational relevance. Since the last global financial crisis in 2008-09, an increasing attention has been devoted to maintaining overall financial system stability and central banks have played strong roles in domestic financial stability policy, but the full scopes of their financial stability mandates are ambiguous. Over the past ten years, prudent macroprudential policy has served the European zone well in cushioning the impact of the global financial crisis in 2008-09. However, today the global economic outlook remains highly uncertain, credit risks, prolonged environment of low interest rates, the growing corporate liabilities and households liquidity pressures may morph into insolvencies that may have implications for the financial stability in the medium term. Since the credibility of macroprudential policy greatly influences the management of the systematic risks in the financial markets and also the effectiveness of monetary policy, central banks in EU zone and worldwide have become more involved in dealing and monitoring closely the financial stability. Generally, financial stability is its ability to facilitate and enhance economic processes, manage risks, and absorb shocks. This paper also discusses some of the existing efforts to construct an aggregate financial stability index and its application. To summarize the discussion below, financial stability has been a fundamental objective of central banks. Indeed, many central banks including the Federal Reserve and ECB were established financial stability as part of their mandate. The paper argues that central banks may contribute to financial stability in four different ways: 1) as crisis managers - as lenders of last resort, in an acute financial crisis; 2) through focusing their regular monetary policy on the right objective and using macroprudential policy on decisions and 3) may act as prudential regulators and supervisors themselves and 4) through their communication and or information policy. In relation to the above, policy coordination between the central banks and the government is crucial to promote financial stability.

Keywords: *central banks, macroprudential policy, monetary policy, systematic risks, financial stability, economic development, financial stability index, National Bank of Moldova*

JEL Classification: *E52 E58 E63 H63*

INTRODUCTION

The main objective of this paper is to analyze the evolving role of central banks in fostering financial stability and look at some current issues that have practical and operational relevance. The paper is structured as follow Section 2 begins by setting out various definitions and concepts of financial stability. It distinguishes between narrow and boarder scope of financial stability and pays attention to the concept of financial stability index, in Section 3, we review how central banks address financial stability in their mandate. In Section 4, we provide a comprehensive view of the main macroprudential policies and tools in fostering financial stability, in Section 5 we examine the supervisory role of central banks and its effect on financial stability, Section 6 we discuss the role of National Bank of Moldova in financial stability and its recent attempts to stabilization. The final section 7 concludes with general observations and recommendations.

WHAT IS FINANCIAL STABILITY?

Since the international crises at the end of the 90s*, also strengthened by the financial and economic crisis in 2007-09, **financial stability** has become often discussed

issues in today's economic literature. The evaluation of financial stability and its soundness is a complex task and involves a large number of multidimensional criteria and evaluation techniques. At present, a single approach to the definition of the concept of financial stability has not been developed in world practice. It is useful to define financial stability since the we aim to examine the question how much weight should be attached to financial stability versus other central bank objectives and also in assessing how central banks are pursuing their financial stability objectives. The narrow definition can be presented as a state in which the financial system is resistant to economic shocks and smoothly fulfils its basic functions preventing the build-up of bubbles; and second, it is about making the system more resilient. However, the broader definitions of financial stability include the macro-economic dimension of financial stability and interactions between the financial and real sectors.

For the purpose of this paper, we have employed the broader concept where financial stability can be defined as "a financial system is in a range of stability whenever it is capable of facilitating (rather than impeding) the performance of an economy, and of dissipating financial imbalances that arise endogenously or as a result of significant adverse and unanticipated events" (IMF, 2004)

Financial stability relates to the ability of a financial system (1) to facilitate the performance of an economy – contributing to the efficient allocation of real economic resources, the rate of output growth, and facilitating saving, investment, and wealth accumulation (b) to assess, price, and managing financial risks; and (c) to maintain its ability to absorbs shocks—primarily through self-corrective mechanisms (Schinasi, 2004). Some researchers have defined financial stability it in terms of what it is not—a situation in which financial instability and or imbalances impair the real economy. A similar approach is taken by Allen and Wood (2006) who define the characteristics of an episode of financial instability first and then define financial stability as a state of affairs in which episodes of instability are unlikely to occur.

Schinasi (2004) reports in an annex various definition of financial stability. We narrow ourselves to report the one provided by Roger Ferguson of the Board of Governors of the US Federal Reserve System (made in 2003): *"It seems useful...to define financial stability...by defining its opposite: financial instability. In my view, the most useful concept of financial instability for central banks and other authorities involves some notion of market failure or externalities that can potentially impinge on real economic activity……, I'll define* ***financial instability*** *as a situation characterized by these three basic criteria: (i) some important set of* ***financial asset prices seem to have diverged sharply*** *from fundamentals; and/or (ii)* ***market functioning and credit availability****, domestically and perhaps internationally,* ***have been significantly distorted****; with the result that (iii)* ***aggregate spending deviates*** *(or is likely to deviate) significantly, either above or below, from the economy's ability to produce."*

Through the last years, the central banks monitoring process has been widening its scope including regular analyzes of risks and threats to the stability of the financial system. This has resulted into the publication of Financial Stability Reports (FSR) and in many of the subject reports financial stability assessment has been taking into consideration risks arising not only from inside the traditional banking system, but also from outside the banks' balance sheet. The words of a central bank can be powerful and they can affect markets in either direction. Such communication can encourage market participants to behave more prudently and also improve market discipline by sharing their views on relevant risks, central bankers create greater transparency about vulnerabilities in the financial sector. Many central banks in their financial stability reports try to evaluate

financial stability related risks focusing on various market segments and banking related variables. Today, central banks reports seem not only to concentrate on the banks' performance discussing banking ratios and risks in considerable detail, but also to take account insurance and other forms of nonbank financial intermediation.

According to assessment conducted by Capraru (2010), in general, central banks communication policy in terms of financial stability have increased in the past years in Europe. His assessment is based on measuring the Sotomska-Krzysztofik and Szczepanska transparency index in the field of financial stability and the index was calculated for the end of 2010, on a sample of 36 central banks (ECB, EU-28 central banks, Norway, Switzerland, Iceland, Russia and 3 candidates to EU: Turkey, Macedonia and Croatia) ranging from 1 to 10 according to the transparency level, the score of 10 indicating the most transparent awarded by the Bank of England (10 p). Overall, the results show that most central banks in Europe (20) obtained a high score between 7-10 points. The researcher concludes that the main factors driving these positive trends were the process of European integration and the international financial crises experience.

The next question that follows is how central banks measure financial stability. There is no single answer to this question. In recent years the approach to development of such index shifted to a broader system-wide assessment of risks to the financial markets, institutions and infrastructure as the locus of concern moved from micro-prudential to macroprudential dimensions of financial stability. Recently, the analytical focus has further concentrated on the dynamics of behaviour, the potential build-up of unstable conditions as well as the so-called transmission mechanisms of shocks.

For example, some central banks calculate an aggregate financial strength index that combines six areas of financial soundness indicators, namely capital adequacy, profitability, liquidity, asset quality, interest rate risk and exchange rate risk. The issue of financial stability is organically linked with banking stability. Banking stability gets affected positively or negatively with the prevailing conditions in the financial market and the real economy; ultimately banking stability determines whether an economy is strong enough to withstand both the internal and external shocks. In the literature, a variety of methodologies for constructing Financial Stability Index or Banking Stability index have been developed. Many authors used selected quantitative indicators of the set of basic Financial Soundness Indicators complied by the International Monetary Fund. These indicators (40 indicators) are divided into two sets: core set and encouraged set. Core set includes statistics on the health and performance of deposit takers and consists of main indicators related to the banking sector (17 indicators) provided below.

Table 1. IMF Financial Soundness Indicators: The Core set

Core set	
Deposit takers	
Capital Adequacy (we measure Banks' capital cushion size to address expected or unexpected losses)	Regulatory capital to risk-weighted assets Tier 1 capital to risk-weighted assets Nonperforming loans net of provisions to capital Common Equity Tier 1 capital to risk-weighted assets Tier 1 capital to asset
Asset Quality	Nonperforming loans to total gross loans Loan concentration by economic activity Provisions to nonperforming loans
Earnings and Profitability	Return on assets Return on equity Interest margin to gross income Noninterest expenses to gross income Liquidity
Liquidity (Ratio of banks' readily available short- term resources that can be used to meet short-term obligations	Liquid assets to total assets (liquid asset ratio) for all DTs Liquid assets to short term liabilities for all DTs Liquidity Coverage Ratio for the DTs that have implemented Basel III liquidity standards Net Stable Funding Ratio for the DTs that have implemented Basel III liquidity standards
Sensitivity to Market Risk	Net open position in foreign exchange to capital
Real Estate Markets	
	Residential real estate prices

Source: IMF (2019)

The reader will notice that some of the deposit takers indicators consist in variables that contain indication on the financial stress of institutions, financial stress meaning the fear of failing to remain able to fulfil all contractual commitments.

The IMF has also stated publishing a global financial stability map which provides an assessment of the risks and the underlying conditions for the global financial system. Leading indicators in six broad areas are considered: monetary and financial conditions in leading industrial countries, risk appetite in global financial markets, macro-economic risks in G3 and OECD countries, emerging market risks credit risks and market risks.

European Central Bank's financial stability reports' statistical annex contains one section on financial market indicators, and one on financial institutions.

Other example includes: The Bank of Canada and the Nederlandsche Bank construct single aggregate measures of financial stability (albeit not published in their FSRs) which compare favourably in their ability to indicate crises. The Board of Governors of the Federal Reserve System does not publish a financial stability review, but it has an index of financial fragility, which has macroeconomic and microeconomic aspects. At the microeconomic level, financial fragility broadly means that elements on the liability and/or asset side of the balance sheet are highly sensitive to changes in interest rate, income, amortization rate, and other elements that influence the liquidity and

solvency of a balance sheet. In this case, not-unusual fluctuations in those variables create large financial difficulties.

The financial fragility index provides regulators with a means to detect financial fragility independently of the merit of an economic activity, of the profitability of business, of the default rate on loans, of the welfare created or destroyed by an economic activity, of the existence of a bubble or not, of the existence of fraud or not, of the expectation of an economic recession or not, or of the views of the future of economic units. [18]

HOW CENTRAL BANKS PROMOTE FINANCIAL STABILITY

In this section the author will addresses whether central banks have a natural role in ensuring financial stability, and if so, what do a central bank do to safeguard financial stability. **Central banks** are intendant national authorities and the most powerful economic institutions that are helping society to manage its collective financial affairs.

A classical way to look at what central banks are doing is to review their mandates and statures.

As a central bank, the primary objective of the European Central Bank (ECB) is to maintain price stability, but it also has a contributory role in financial stability, as indicated by the Treaty on the Functioning of the European Union. The ECB works to identify, assess and monitor risks to financial stability, because turbulence in the financial system may weaken the ECB's ability to maintain price stability. And since 2014, the ECB also has the power to take macroprudential policy measures aimed at addressing specific stability risks.

Article 127 (2) of the EC Treaty on the Functioning of the European states:

2. The basic tasks to be carried out through the ESCB shall be:

— to define and implement the monetary policy of the Community;

— to conduct foreign-exchange operations consistent with the provisions of Article 111 of this Treaty;

— to hold and manage the official foreign reserves of the Member States;

— to promote the smooth operation of payment systems.

5. The ESCB shall contribute to the smooth conduct of policies pursued by the competent authorities relating to the prudential supervision of credit institutions **and the stability of the financial system.**

The Treaty clearly outlines a contributory role for the ECB in maintaining financial stability given that financial stability is necessary for the credit channel of monetary transmission to function properly. As seen above, this implied mandate is confirmed, but also restricted in scope, by the ECB "contribution" clause in article 127(5) TFEU. However, it is not proposed to introduce a financial stability mandate of equal standing with price stability. [16]

Many researches have underlined that financial stability and price stability are functionally connected. As we saw during the last global financial crisis, financial instability can materially disturb the channels through which monetary policy influences prices. Thus, it can limit the ability of central banks to do their job.

Edward George, who was at the helm of the Bank of England during crises such as the collapse of Barings Bank made this point graphically when he said: "it is inconceivable that the monetary authorities could quietly pursue their stability-oriented monetary policy objectives if the financial system through which policy is carried on (…) were collapsing around their ears". [16]

According to the Bank of England Financial Stability Review (Bank of England, 2008), *"**The Bank of England has two core purposes — monetary stability and financial***

***stability**. The two are connected because serious disruption in the financial system can affect the implementation and effectiveness of monetary policy, while macroeconomic stability helps reduce risks to financial stability. The Bank's responsibility for contributing to the maintenance of the stability of the financial system as a whole derives from its responsibility for setting and implementing monetary policy, its role in respect of payment systems in the United Kingdom and its operational role as banker and supplier of liquidity to the banking system. The Bank aims to bring its expertise in economic analysis and its experience as a participant in financial markets to the assessment and mitigation of risks to the UK financial system including, as necessary, helping to manage and resolve financial crises".*

As Villar A. discusses many central banks have included financial stability in their mandate but not necessarily in the form of a quantitative goal and these authorizes have control over a large array of macroprudential tools. [19] But in some countries, decision-making powers and control over instruments remain diffused across institutions. In such cases, policy coordination implementation tilts towards favouring the central bank's role of" primus inter pares".

The truth is that today it is hard to separate the central bank ability to maintain monetary stability, the ability to maintain financial stability, or both they have been sometimes hard to separate. It is hard to delineate when financial stability gets so important that it affects monetary policy and vice versa. These days financial stability is about much more than just banks Things are not as simple as they used to be. For example, innovations like digital money, global value chains, online shopping and etc. add to the complexity of maintaining price stability.

According to Schembri [13], central banks can promote the stability of the financial system, by deploying a range of policy responses including:

- **keeping the focus of monetary policy on the right objective** – since the last financial he crisis, many central banks has kept its policy interest rate relatively low, by historical standards, to in order to overcome the recession and support economic growth and thereby achieve its primary goal of returning inflation to targeted per cent within a reasonable time frame. This reduction comes from previous successes, which have kept inflation low so allowed the monetary authorities to maintain the interest rates below the level proposed by historical experience [17]. However, we recognize that elevated household and or corporate debt could represent a risk to financial stability. This illustrates that targeting and reducing vulnerabilities by monetary policy tools, affects the entire economy and is thus a very blunt instrument to address financial stability.
- **encouraging prudence on the part of borrowers and lenders and enhancing market discipline through increased transparency.** Most central banks regularly provide communication through their financial stability reports or other periodic publication and analysis and in such manner, they inform lending institutions, households and businesses of their analysis and thereby raised their awareness of high vulnerabilities and financial risks in an effort to encourage them to exercise appropriate caution.
- **adopting macroprudential measures** – these measures primarily include capital buffers Introduced after the global financial crisis of 2007-09. Capital buffers aim to enable banks to absorb shocks and or losses while maintaining the provision of key services to the real economy, while automatic restrictions on distributions prevent the imprudent depletion of capital in times of stress. In the European framework, these buffers include the capital conservation buffer (CCoB), the countercyclical capital buffer (CCyB), buffers for global and other systemically important institutions (G-SIIs

and O-SIIs) and the systemic risk buffer (SyRB). The combination of all these buffers constitutes the combined buffer requirement (CBR).

- **strengthening regulation and supervision of the financial sector** - since the global financial crisis, the regulatory and supervisory framework has been further strengthened. More rigorous global standards have been developed and promote their implementation An example is the implementation of the Basel III regulatory reforms, which require banks to hold more and higher-quality capital and meet new liquidity and leverage requirements. Consequently, many banks that implementation of the Basel III are now in a better position to cope with unexpected downturns in economic activity.

Central banks as lender of last resort

In an acute financial crisis when standard sources of funding dry up, banks and increasingly other financial institutions turn to central banks to replace conventional lenders. Changed realities in financial markets, however, challenge central banks to reconsider the classical notion of LOLR. Although this role of central banks no longer can be taken as given, we agree with the classic Bagehot's doctrine that calls for helping out banks that may be illiquid, but not insolvent. In fact, this approach helped modern central banks to deal with the global financial crisis. By injecting large amounts of liquidity, central banks may have prevented an even deeper economic downturn. During the recent global financial crisis, Fed did allow Lehman Brothers to fail, however, this quickly turned into a demonstration of an opposite nature The Fed's decision with regard to Lehman was widely criticized, and it quickly became clear that central banks were not going to allow another major financial player to collapse.

The question we examine here is if the role of the central bank as a lender of last resort stand in conflict with monetary policy objectives? Financial crises typically go along with deflationary pressure. Therefore, lender of last resort activities tends to support both monetary and financial stability. As Hellwig (2015) argues the scope for lender of last resort activities is limited in in a fixed exchange rate regime or in a banking system whose liabilities are mostly denominated in foreign currency. The lender of last resort activities are generally supportive of macroeconomic stability but they may stand in conflict with the goal of maintaining a fixed currency peg.

FINANCIAL STABILITY AS MACROPRUDENTIAL POLICY OBJECTIVE

Regulation and oversight of financial institutions can reduce risks to individual firms. However, to mitigate systemic risks, many countries have turned to macroprudential polices that aim to ensure the safety of the financial system as a whole.

Policymakers have traditionally focused on reducing risks to individual financial institutions to (also known as macroprudential policies) to ensure that they are safe and able to honor their obligations. But the global financial crisis has exposed that keeping individual financial institutions sound is not enough as this allowed system-wide financial risks to grow unchecked. Since the crisis, many countries adopted a broader approach to safeguard the financial system as a whole are expanding their toolkits to explore a more systemic approach to financial regulation and supervision. This holistic approach is called macroprudential policy. Since the great financial crisis in 2008-09, central banks have started playing greater attention to macro-financial linkages than before and many have adopted a macroprudential orientation of their financial stability policy. They can use macroprudential policy to achieve this goal.

The macroprudential policy of central banks is relatively young and was born out of the financial crisis, but since then has been growing rapidly. While the central banks have

used the term "macroprudential prominently following the global financial crisis, the concept of "macroprudential policies" has been in use before.

The ultimate objective of macroprudential policy is to mitigate excessive systemic financial risks, resulting from external factors and market failures, to smoothen the financial cycle (time dimension) and make the financial system more resilient to shocks and limit contagion effects, and encourage a system-wide perspective in financial regulation to create the right set of incentives for market participants. These macroprudential policies typically operate through adjustments in capital and liquidity requirements and in permissible terms of lending, affecting the cost of intermediation and the availability of credit.

Central banks deploy a large set of prudential tools to improve the resilience of the financial system, which be used for both micro- and macroprudential purposes, depending on whether they are aimed at strengthening the stability of individual institutions or that of the system as a whole. A good example is the reserve requirements, that can be used for both monetary and macroprudential purposes. Central banks' ability to employ macroprudential instruments varies across jurisdictions. Most EU central banks have full control over macroprudential tools such as countercyclical capital buffers and capital requirements, margins and haircuts, sector-specific capital requirements for the banking sector and debt service-to income and loan-to-value ratios. In two cases, the central bank of Brazil and South Africa share the decision-making powers with the banking supervisor or another government body. In several jurisdictions, some instruments are simply unavailable. For instance, dynamic provisioning and sector-specific and countercyclical capital requirements are not available in Chile, Russia, Israel and etc. (BIS, 2017).

In Europe there is common framework for macroprudential policy which consists of a system of rules, practices and processes that direct and control the policy. Central Banks in Eurozone use a number of macroprudential instruments that provide them with greater control in respect of the emergence of systemic risks in the future

The role of the ECB goes beyond than just to identify, assess and communicate risks. The ECB was given some relevant competences after the crisis in 2007-09 that cover both individual banks and the banking system. Macroprudential policy has two goals, first, it aims to make the system more resilient to shocks.

In address its macroprudential measures ECB works together with other European and national authorities. At the European level, the ECB has a strong ally in the European Systemic Risk Board, (ESRB) established in 2010. The ESRB takes a broad view of the financial system and have a broad remit, covering banks, insurers, asset managers, shadow banks, financial market infrastructures and other financial institutions. It monitors and assesses systemic risk in all these areas of the financial system and where appropriate, it issues warnings and recommends action. responsible for the macroprudential oversight of the EU financial system and the prevention and mitigation of systemic risk. Other European authorities, such as the European Banking Authority, European Securities and Markets Authority, and European Insurance and Occupational Pensions Authority, also contribute to the ESBR's work. National authorities play a crucial role in macroprudential policy. Under the EU's legislative concept, macroprudential policy is also a national policy. The European perspective complements the national one. Unlike monetary policy, macroprudential policy can target specific sectors or countries. This in turn allows monetary policy to focus on price stability.

So how does macroprudential policy work in practice?

Macroprudential tools can be structural and cyclical. The first tools focus on the impact large, systemically important institutions have on the rest of the system when they

fail or become distressed. Structural macroprudential objectives motivate regulatory tools such as additional capital requirements for systemically important banks ("SIFI surcharges"), which aim to reduce the probability that a large institution fails, and resolution and recovery planning, which seeks to limit the damage in the event of failure. Other structural tools some countries deploy include limits on loan-to-value ratios (LTVs) or debt service–to–income ratios (DSTIs) for mortgage borrowers are examples of structural tools that have been applied to borrowers. These limits can be macroprudential when they are intended to not only protect an individual borrower from too much debt, but to protect home values in neighborhoods from falling sharply because many borrowers have trouble making their payments at the same time. For example, the Hong Kong Monetary sets the LTV ratios for borrowers based on the value of the property. Bank borrowers for properties with high values could get mortgages with LTV ratios ranging from 40 percent to 60 percent, while they could get mortgages with higher LTV ratios, up to 70 percent, for properties with low values.

The second set of macroprudential tools are cyclical focusing on aimed at increasing resilience in anticipation of an economic downturn to lessen the reduction in the supply of credit once the downturn materializes. The countercyclical capital buffer (CCyB) is an example of a cyclical policy. The CCyB works by requiring banks to increase their capital cushions during an economic expansion when systemic risks are rising, and then release them in an economic downturn to absorb losses. Capital buffers allow banks to continue to support the economy in downturns while also weathering losses. In doing that, the banks can be a source of strength for the economy, helping to absorb rather than amplify the economic shock caused by crisis. It is in banks' collective interest to continue to support viable, productive businesses, rather than seek to defend capital ratios and avoid using buffers by cutting their lending.

The ECB then has the power to top-up some of these measures. And while national authorities are the key players, it also makes sense to involve the ECB. This helps to keep an eye on any cross-border spill-overs and to alleviate any inaction bias that may still exist at national level. A good example of the important role that the ECB plays in macroprudential policies is the methodology it has developed for minimum additional capital to be held by regional systemic relevant banks. The methodology has reduced heterogeneity in the buffer calibration across the euro area.

All in all, since the global financial crisis, both advanced economies and emerging market economies have been using macroprudential measures more frequently, as illustrated in the charts below taken from ECB report on macroprudential policies measures as of October 1, 2020.

Individual structural buffers – Number of euro area banks or euro area countries	
Banks with individual structural buffers (G-SII buffer, O-SII buffer, SRB)	**115**
Banks with G-SII buffer	8
Banks with O-SII buffer (including those with G-SII buffer)	109
Banks with SRB	19
Countries that have activated the CCyB*	2

Individual structural buffers – Ranges	
Combined buffer requirement	**2.50% – 5.50%**
Average combined buffer requirement	3.08%
G-SII buffer	1.00% – 2.00%
O-SII buffer	0.06% – 2.00%
Average O-SII buffer (including G-SII buffer)	0.83%
SRB	1.00% – 2.50%
CCoB	2.50%
CCyB	0.00% – 1.00%

Chart 1. Macroprudential policy measures in the euro area as at 1 October 2020
Source: ECB website measures (https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin)

Notes: "The figures only include information on supervised banks (e.g. excluding O-SII buffer requirements for Cyprus-based investment firms). Small and medium-sized investment firms are exempted from the CCyB and/or the CCoB in Italy, Lithuania, Luxembourg, Malta and Slovakia. For Slovakia, the SRB is applied only to domestic exposures, meaning that the buffer applies in addition to the O-SII or G-SII buffer, whichever is greater. The CBR is calculated in accordance with Article 131 CRD IV but excludes mandatory or voluntary reciprocity of foreign macroprudential measures in accordance with Recommendation ESRB/2015/2. It consists of CET1 capital and is in addition to a minimum requirement of 8% total capital (4.5% CET1 + 1.5% AT1 + 2% T2). Pillar 2 measures are not included. The minimum combined buffer requirement at country level corresponds to a bank not subject to any individual bank-level structural buffer (G-SII, O-SII, SRB). Abbreviations: combined buffer requirement (CBR); global systemically important institution (G-SII); other systemically important institution (O-SII); systemic risk buffer (SRB); countercyclical capital buffer (CCyB); capital conservation buffer (CCoB); Capital Requirements Directive (CRD IV); Common Equity Tier 1 (CET1); Additional Tier 1 (AT1); and Tier 2 (T2). * Reflects only countries that have already activated a positive CCyB.

Capital and liquidity buffers have been designed with a view to allowing banks to withstand stressed situations like the current one. The European banking sector has built up a significant amount of these buffers. The ECB will allow banks to operate temporarily below the level of capital defined by the Pillar 2 Guidance (P2G), the capital conservation buffer (CCB) and the liquidity coverage ratio (LCR). The ECB considers that these temporary measures will be enhanced by the appropriate relaxation of the countercyclical capital buffer (CCyB) by the national macroprudential authorities.

The chart below shows the minimum and maximum CBR, as well as the banks affected by the maximum CBR. The minimum CBR (blue) is usually applicable to all banks in one country, taking into account the CCoB and the CCyB, the maximum CBR (yellow) relates to financial institutions that are required to apply an O-SII buffer, G-SII buffer or SRB, whichever is greater.

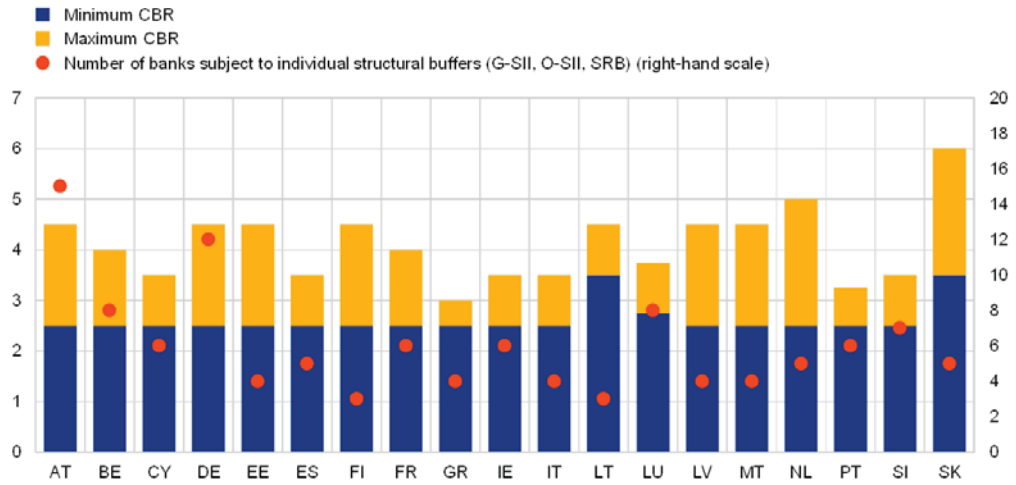


Chart 2. Overview of combined buffer requirements

(left-hand scale: percentage of total risk exposure; right-hand scale: total number; measures apply as of 1 October 2020)

Source: ECB website Macroprudential policy measures (https://www.ecb.europa.eu/pub/financial-stability/macroprudential-bulletin)

Notes: "The figures only include information on supervised banks (e.g. excluding O-SII buffer requirements for Cyprus-based investment firms). In some countries, certain financial institutions are designated as O-SIIs, but no additional buffer requirement applies at this time. Small and medium-sized investment firms are exempted from the CCyB and/or the CCoB in Italy, Lithuania, Luxembourg, Malta and Slovakia. For Slovakia, the SRB is applied only to domestic exposures, meaning that the buffer applies in addition to the O-SII or G-SII buffer, whichever is greater. The CBR is calculated in accordance with Article 131 CRD IV but excludes mandatory or voluntary reciprocity of foreign macroprudential measures in accordance with Recommendation ESRB/2015/2. It consists of CET1 capital and is in addition to a minimum requirement of 8% total capital (4.5% CET1 + 1.5% AT1 + 2% T2). Pillar 2 measures are not included. The minimum combined buffer requirement at country level corresponds to a bank not subject to any individual bank-level structural buffer (G-SII, O-SII, SRB). Abbreviations: combined buffer requirement (CBR); global systemically important institution (G-SII); other systemically important institution (O-SII); systemic risk buffer (SRB); countercyclical capital buffer (CCyB); capital conservation buffer (CCoB); Capital Requirements Directive (CRD IV); Common Equity Tier 1 (CET1); Additional Tier 1 (AT1); and Tier 2 (T2)"

In order to address the impact of the coronavirus (COVID-19) pandemic, the national competent authorities (NCAs) of six euro area countries have decided to revoke the implementation of previously announced Countercyclical capital buffers **CCyBs and to release already activated CCyBs. Currently, two euro area countries report a positive CCyB rate: Luxembourg, 0.25% as of 1 January 2020, which will be increased to 0.5% as of 1 January 2021, and Slovakia, 1% as of 1 August 2020. The NCAs of 12 euro area countries decided to maintain the CCyB rate at 0%.**

Case study: The countercyclical capital buffer (CCyB) in Germany was introduced 2016 and was activated by the Federal Financial Supervisory Authority for the first time on 1 July 2019 and increased to 0.25%. The banks had 12 months to implemented would have completed the process of building up the CCyB by 1 July 2020. This increase was due to an assessment by the German Financial Stability Committee that the long spell of favourable economic activity and low interest rates had given rise to cyclical systemic risks in the German financial system. Some of the underlying risks include: a potential underestimation of credit risk; second, an overestimation of the recoverability of the collateral used in real estate financing as a result of many years of rising real estate prices; and third, interest rate risk. The Bundesbank's analyses indicated that the banking system

should build up more capital in what was then a good macroeconomic setting in order to be more resilient to an unexpected economic downturn.

Due to the coronavirus pandemic, BaFin lowered the CCyB rate to 0% with effect from 1 April 2020 which created scope for maintaining the supply of loans needed by the real economy. In many other countries, too, the CCyB was released or its further build-up was discontinued. The announced buffer rates or buffers that had already been built up ranged from 0.25% (e.g. in Germany) to 2.5% (e.g. in Sweden).

Since the outbreak of COVID-19 pandemic, the European Central Bank has announced a number of measures to ensure that banks can continue to fulfil their role in financing households and corporates experiencing temporary difficulties. Overall, the banks in EU remained strong due to the early implemented macroprudential measures.

For example, in 2020 UK banks remained resilient and had high levels of capital, allowing them to absorb very big losses while continuing to lend to households and businesses. The Financial Policy Commission lowered the UK countercyclical capital buffer rate to 0% in March, meaning that banks have more capacity to lend.

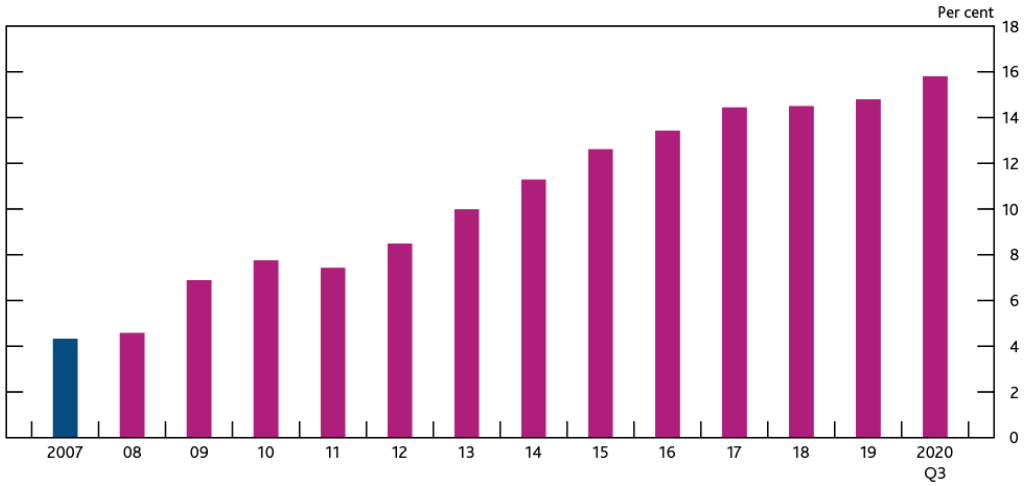


Chart 3. Aggregate CET1 capital ratio of major UK banks

Sources: Bank of England website.

(a) The CET1 capital ratio is defined as CET1 capital expressed as a percentage of risk-weighted assets. Major UK banks are Barclays, HSBC, Lloyds Banking Group, Nationwide, NatWest Group, Santander UK and Standard Chartered. From 2011, data are CET1 capital ratios as reported by banks. Prior to 2011, data are Bank estimates of banks' CET1 capital ratios.; (b) Capital figures are year-end, except 2020 Q3.

From a more general point of view, a flexible macroprudential framework is needed; one that allows to quickly respond to market developments. This will be all the more important in the future as macroprudential authorities should be ready to tackle new risks that may arise from the shift towards market-based finance. Key to this will be looking beyond the banking sector; keeping an eye on banks is no longer enough.

CENTRAL BANKS SUPERVISION ROLE IN PROMOTING FINANCIAL STABILITY

In this section we will address which supervisory structures are best suited to managing the risks arising from the financial sector. We will look at the importance of effective coordination across supervisors and central banks and will examine the integrated European Central Bank model and what benefits this set-up has brought.

The most direct way to affect financial stability is through prudential supervision. In fact, central banks are frequently directly involved in prudential supervision. Since November 2014, this has also been true for the European Central Bank (ECB), which has taken over broad responsibilities in banking supervision in the context of the Single Supervisory Mechanism (SSM). This setup was chosen because it could be implemented quickly under the existing legal constraints and because the ECB at the time was one of the few institutions capable of acting. However, it was recognized early on that this setup was not necessarily optimal, leading to a debate whether the combination of monetary policy and banking supervision within one institution is really desirable or whether a separation would be preferable in the longer term. In fact, this debate is not new. Nevertheless, it is far from being resolved, which is also reflected in the widely varying degree to which central banks are involved in banking supervision in different countries.

In the literature, a number of papers have analyzed the relationship between supervisory structure and macroeconomic outcomes, in particular inflation and financial stability. Overall, the empirical evidence is mixed and show that inflation rates are higher in countries in which the central bank is responsible for monetary policy and banking supervision. Supervising individual banks helps boost resilience. ECB Banking Supervision directly supervises the 118 biggest banking groups in the euro area – with over €20 trillion euros in total assets. Clearly, these banks – some in their own right, some as part of a group – are systemically relevant. Given their huge role in financing the euro area economy, their resilience is key to financial stability. The first step is for the supervisor to obtain a holistic view of each of these banks, not only assessing capital and liquidity risks, but also their internal controls and governance. And then the supervisor needs to act and push for improvements in all these elements if needed. But it is not enough to look at each bank in isolation. To identify and understand new risks and vulnerabilities, the second step is to take a broader view. As supervisors we have to stay closely attuned to the macroeconomic environment in which banks operate. European banking supervision has helped to maintain financial stability. It has done so by making banks safer and sounder. Euro area banks now hold more capital than ever before: their fully loaded CET1 ratio has increased by about 2.5 percentage points since 2014. Back then, it stood at 11.2%, now it stands at 13.8%. There is no doubt that banks are more resilient today than they were in the past; they are better able to withstand financial shocks and economic downturns. But, of course, capital is not the full story. Liquidity is also key, as a liquidity crisis in one bank can turn into a risk to the entire system.

Another key ingredient that are central to a supervisor's contribution to financial stability are the independence of the supervisors as they must be able to take their own decisions. They must be free from pressure from banks or other stakeholders – and they must be free from political trends. But Independent institutions need to be accountable. The ECB as a banking supervisor is no exception.

In the U.S., the Financial Stability Oversight Council (FSOC) was created in 2010 by the Dodd- Frank Wall Street Reform and Consumer Protection Act. The FSOC is led by the Secretary of the Treasury, and its members include the leaders of the financial regulatory agencies, including the Federal Reserve, Federal Deposit Insurance Corporation, Securities and Exchange Commission, Commodity Futures Trading Commission, and others. It is responsible for "identifying risks and responding to emerging threats to financial stability."

NATIONAL BANK OF MOLDOVA AND FINANCIAL STABILITY ISSUES

In this section the author will mainly address the use of monetary policy by the central bank in Moldova and its influence on the banking sector, managing risks and overall economic development.

The implementation of monetary policy in the Republic of Moldova is the task of the National Bank of Moldova. The subject Bank is a relatively young bank which was set up in 1991 as an autonomous public legal entity that has the executive rights in issuing money in the country, and is responsible for the execution of monetary and foreign exchange policies in the country, maintaining the stability of the currency, regulating payments abroad, and controlling the financial and banking system in the country.

In 1995 two important laws were adopted The Law of the National Bank of Moldova and the Law on Financial Institutions, as experts view these law as one of the most progressive laws on central banks and financial institutions in the CIS region. The subject Laws stipulate the independence of the NBM from the Parliament and also from the bodies of executive power which is very important for the formulation and implementation of an independent monetary, credit and foreign exchange policies. The highest management authority of the NBM is the Council of Administration and it has power to establish the monetary policy its main parameters and instruments for implementation. NBM is responsible both for monetary policy, and for the prudential regulation and supervision of the banking sector. There are additional regulatory bodies that are entrusted with the supervision of financial markets. However, given the relatively low importance and volume of operations on these markets, we can say that the Central Bank is the main supervisor of the financial sector.

Managing and executing the monetary policy is essential, unique and most important function of the National Bank of Moldova. The role of the Central banks varies from country to country in terms of its goals, objectives and principles of operation. In developed countries, where a developed capital market exists, banks are less dependent to the central bank, in terms of providing funds, on the other hand, in developing countries, as is the Republic of Moldova, banks are more dependent from the central bank, which has more dominant role in the conducting of the monetary policy.

In exercising its functions, the National Bank of Moldova uses a set of economic instruments and policies including 1) establishment of minimum required reserves, 2) refinancing rate which plays an important role in the demand for NBM's credits and as such it influences the reserves money and the money supply. This rate is largely influenced by the volume of credit auctions which drives the destitution of the NBM's credits among commercial banks. Recently the NBM started to use other instruments like the Lombard credit, REPO and operations with state securities, 3) financing of the state budget deficit that results into an increase of reserve money and an increase of money supply, so this is an inflationary factor, 4) state securities – open market operations performed by the NBM can take any form of securities purchase or selling or conclusion of state securities selling and repurchase agreements. Compared to the reserve's money, the open market operations are performed on a voluntary participation and as often as can, and 5) foreign exchange intervention.

The two monetary tools – required reserves and the refinancing rate show the best results in developing countries where the financial markets are not yet developed and where there is a high concentration of the banking sector. Yet, the central banks can face the dilemma to decrease the required reserve or to carry out credit emissions that could cause an inflation rise. In terms of the refinancing rate, if the Central Banks policy becomes more expansionary via the refining rate reduction this will lead to an increase of

the liquidity held by banks and of the liquidity available on the interbank market. Banks can increase the supply of credit to lower borrowing rates or providing liquidity on the interbank market at a lower rate which will lead will stimulate overall demand for goods and investment and will influence inflationary pressure. In this way NBM can achieve its aim through 5% inflation targeting.

Using the above-mentioned tools, the National Bank of Moldova throughout the past 15 years has helped Moldova to navigate the shocks of the international monetary system and now its effort is to bring the country into the euro area, as part of the Euro system, Since the last banking crisis in 2014-2015, political instability and government challenges, the National Bank of Moldova has shown resilience and adaptability.

In 1993 Moldova introduced its national currency - the Moldovan Leu and the currency has been relatively stable since 2016-17, after depreciating by 34% in 2014-2015. The maintaining of the price stability from the Central Bank has proved to be the correct and the best choice, especially for countries that are suffering from hyper-inflationary tensions and often loss of money value.

The main objective of the monetary policy of the National Bank of Moldova is the maintaining of price stability, which implies a reduction of the minimum level of inflation in the long run and ensuring stability of the financial system. According to the medium-term policy strategy of the NBM in order to ensure and maintain price stability over the medium term, the National Bank's target is to keep inflation at the level of 5.0 percent annually with a possible deviation of ± 1.5 percentage points, considered to be optimal for growth and development of Moldova's economy over the medium-term. The last quarter of 2019, the annual inflation rate continued to trend upward since the beginning of 2019, increasing from 6.3% in September 2019 to 7.5% in December 2019. This change was largely due to some upward dynamics of food prices due to less favorable weather conditions in the summer of 2019 for certain crops and a turnaround in regulated prices—as the effect of previous tariff cuts dissipated—and by the impact of robust aggregate demand on core inflation. Public debt declined and remains low, below 30 percent of GDP. Despite heightened political uncertainty, the leu remained relatively stable, and foreign exchange reserves remained adequate.

With regards to the financial sector, currently the Moldovan banking system was comprised of 11 commercial banks, the central banks and **nonbank financial institutions and markets are still small and underdeveloped.** The insurance sector is small at 3.5 percent of total financial sector assets and is growing only in line with GDP. Microfinance institutions and some small deposit-taking credit associations – regulated by the NCFM – are increasing in number but their reach and size is not growing IMF (2016).

During 2014 and early 2015, the Moldovan banking system was disrupted by a series of bank fraud of historic size, which evolved into a severe financial crisis in which the Central Bank's inaction came under scrutiny. In 2014, $1 billion disappeared from three Moldovan banks (Banca de Economii S.A. – BEM, JSCB Banca Sociala– BS and JSCB Unibank – UB), that accounted for a 25% of the country's banking sector and these bans remained without license of activity, and the National Bank of Moldova (NBM) established regime of special surveillance over 3 other banks – JSCB Moldova Agroindbank, JSCB Moldindconbank and JSCB Victoriabank. The Liquidation of the three banks, a significant increase of the base rate, and increasing reserve requirements had great impact on the Republic of Moldova economy and private sector. The BM tightened aggressively monetary policy and in less than a year, the NBM increased the monetary policy rate in several stages, from 3.5 percent to 19.5 percent in lei and the reserve

requirements from 14 percent to 35 percent. The private sector had to bear this cost of crisis very obvious, faced with high credit rates and limited credit availability.

Some analysts blamed the Central Bank for the failure of the three financial institutions and the financial losses resulting from their default. Their arguments are that Central Bank would be morally authorized to act immediately after at least one prudential indicator for the banking sector has risen above (or fallen below) its maximum (or minimum) admissible value. However, the Central Bank defended itself by stating that is followed existing prudential rules and regulation very closely and that it undertook all possible efforts to minimize the losses to the financial sector as a whole.

After the 2014-15 banking crisis, macroeconomic stabilization in Moldova has been supported by an IMF programme as in November 2016, IMF approved a US$ 179 million three-year arrangement for Moldova focusing on stabilizing the banking sector, restoring shareholding transparency and corporate governance in all banks, promoting key legislative reforms such as Basel-III regulation, bank recovery and resolution legislation, but also strengthening the deposit guarantee fund and financial market infrastructure.

In 2018 came into effect a Law on banks' activity, which modernized the regulation and supervision standards in the banking sector. The law provided improvements to the corporate governance framework of the banks and their obligation to hold adequate share capital in relation to the assumed risks. The law will contribute to the harmonisation process of the national banking legislation with international principles and standards. In July 2018, the new Basel III regulations came into force (based on the European CRD IV / CRR framework). The new regulations set the size of capital buffers, which if necessary, will diminish the impact of systemic crises on banks' capital.

In 2018, with the banking supervision priorities and commitments assumed towards the development partners in strengthening the transparency of the shareholders' structure for the banks, significant changes, related to the acquisition of shares in the capital of certain banks by several reputable international groups, were made in 2018. As a result, more than 70% of bank assets are being managed by international groups with a sound reputation.

The Moldovan National Bank requires banking institutions to submit monthly reports containing financial and statistical data required for the construction of a number of prudential indicators that the authority then follows in order to assess the financial health of the banking sector. Aside from the general data that it collects, the Central Bank also requires banks to nominally identify entities towards which the bank has large exposures, as well as the ownership structure of the bank. However, off-shore entities are allowed to own shares in banks and the Central Bank has little means to monitor and identify the final beneficiaries of companies registered in off-shore locations. When the Central Bank, as a result of its supervisory activities, detects irregularities in the operations of a financial institution, the literature has documented a number of general intervention options available to it. These general intervention methods are outlined in Online Annex 1 which also provides additional bibliographic information.

In theory, the Central Bank would be morally authorized to act immediately after at least one prudential indicator has risen above (or fallen below) its maximum (or minimum) admissible value. In the case of the Moldovan Central Bank, its failure to swiftly intervene to block fraudulent operations, to take over control and, finally, to bail-out the affected institutions came under scrutiny. Some analysts blamed the Central Bank for the failure of the three financial institutions and the financial losses resulting from their default. However, the Central Bank defended itself by stating that is followed existing prudential rules and regulation very closely and that it undertook all possible efforts to minimize the

losses to the financial sector as a whole. In this paper, we investigate whether this is indeed the case, and whether through its postponement of intervention the Central Bank achieved its stated objective of stability and minimization of financial losses

In addition, much needed are reforms of the financial sector to enforce shareholder transparency, enhance access to finance, mitigate systemic risks and bring in international investments.

The recent global outbreak of the coronavirus disease (COVID-19) has caused significant disruptions to Moldova's economy. Moldova's economic outlook has deteriorated sharply due to the COVID-19 pandemic. Real GDP has fallen and public finances have been under significant pressure from declining tax revenues and emergency health and social spending. These developments coupled with lower remittances inflows, and spillovers from global financial channels have created urgent balance of payments needs. The full impact of the crisis remains highly uncertain. In April 2020, IMF approved a US$235 Million in Emergency Assistance to Moldova to address the pandemic and funds are make available to the authorities to meet the urgent balance of payment needs stemming from the COVID-19 pandemic, help catalyze developmental partner support, and address imminent health system needs IMF (2020).

Despite successful stabilization efforts and significant progress made on banking sector supervision, weak oversight of the non-bank financial sector, gaps in Moldova's AML/CFT framework, and lack of progress on asset recovery are recurring sources of concern.

CONCLUSIONS

This paper draws on the recent research and international experience to assess the roles of central banks may play with respect to fostering financial stability. The above discussion suggests that monetary policy should support macroprudential policy conducted by central banks in preventing the build-up of asset and credit booms. The use of macroprudential tools to mitigate financial stability risks appears to be an additional tool for central banks. However, the practice shows that there can be overlap between the micro- and macroprudential tools, but the timing and rationale for the application of a particular policy instrument may differ depending on the objective. The available central banks financial stability reviews suggest that macroprudential tools can increase the resilience of the financial system through both the buildup of buffers that absorb shocks and a reduction in structural vulnerabilities.

The author of this paper believes that coordinating macroprudential measures with monetary policy is particularly important. At the same time, coordination cannot go too far because price stability, the main objective of monetary policy, is not within the remit of macroprudential frameworks. So, finding the right balance between the use of monetary and macroprudential mechanism can help central banks deal with more ambiguous goals,

As more responsibilities are allocated to the central bank, the incentives for political capture and misuse by governments increase. Overburdening monetary policy may eventually diminish and compromise the independence and credibility of a central bank, thereby reducing its effectiveness in maintaining price stability and contributing to crisis management.' (Orphanides, 2013).

BIBLIOGRAPHY

1. Allen, W., Wood G., 2006. Defining and achieving financial stability, *Journal of Financial Stability* 2 (2), p. 152.
2. Bank of England. 2020. Financial stability Report. Retrieved from https://www.bankofengland.co.uk/financial-stability-report/2020/december-2020
3. Board of Governors of the Federal Reserve System. 2020. Financial Stability Report. Retrieved from: https://www.federalreserve.gov/publications/financial-stability-report.htm.
4. Bank of International Settlements Papers No 94, 2017 Macroprudential frameworks, implementation and relationship with other policies Monetary and Economic Department https://www.bis.org/publ/bppdf/bispap94.pdf
5. Capraru, B., 2010. Financial stability and central bank transparency in Europe. *Faculty of Economics and Business Administration "Al. I. Cuza* University of Iasi Iasi, Romania
6. European Systemic Risk Board, 2014. Handbook on Operationalising Macroprudential Policy in The Banking Sector.
7. European Systemic Risk Board, 2014. Flagship Report on Macroprudential Policy in The Banking Sector.
8. Hellwig, M., 2015. Financial Stability and Monetary Policy. Max Planck Institute for Research on Collective Goods.
9. Hofimann, C., 2018. Reconsidering Central Bank Lending of Last Resort European Business Organization Law Review volume 19, pages883–922(2018)
10. International Monetary Fund, 2019 Financial soundness indicators
11. International Monetary Fund, 2016. Republic of Moldova: Financial System Stability Assessment
12. Orphanidesa, A., and Wielandb, V., 2013. Complexity and Monetary Policy, *International Journal of Central Banking, p.167-202*
13. Schembri, L., 2016. "Connecting the Dots: Elevated Household Debt and the Risk to Financial Stability." *Speech before the Guelph Chamber of Commerce*
14. Schnabel, I. 2016. "Wat role for central banks in safeguarding financial stability?"
15. Schinasi, G., 2004. Safeguarding financial stability, theory and practice. *International Monetary Fund.*
16. Psaroudakis, G., 2018. The Scope for Financial Stability Considerations in the Fulfilment of the Mandate of the ECB/Eurosystem, Journal *of Financial Regulation*, Volume 4, Issue 1, Pages 119–156
17. Taylor, J., 2009 The financial crisis and the policy responses: an empirical analysis of what went wrong. *National Bureau of Economic Research*, Working paper series, Cambridge,
18. Tymoigne, E., 2011. Measuring Macroprudential Risk: Financial Fragility Indexes. *Levy Economics Institute of Bard College Working Paper,* No. 654
19. Villar, A., 2016. Macroprudential frameworks: objectives, decisions and policy interactions. *Bank of International Settlements Working Paper*, No 94

THE IMPACT ON THE ECONOMY OF USING OF THE ELECTRONIC SIGNATURE

INCIDENȚA UTILIZĂRII SEMNĂTURII ELECTRONICE ASUPRA ECONOMIEI

Budurin-Furculiţă Cristina
Profesor de discipline economice, grad didactic superior
Colegiul Național de Comerț al ASEM
e-mail: budurin.furculita.cristina@gmail.com

Iovu-Carauș Marina
Profesor de discipline economice, grad didactic superior
Colegiul Național de Comerț al ASEM
e-mail: iovucarausmarina@gmail.com

Abstract
Modern life became easier thanks to the contribution of technology, which facilitated access to communication and informational exchange without borders. The digitization of the working processes at the level of public authorities, economic agents, and individuals is directly conditioned by the use of technology, and in this case by electronic signature. Traditional methods of signing and authenticating various documents have been easily replaced by technological innovations aimed at streamlining and facilitating work.
In the Republic of Moldova, the legal framework regulates the usage of three types of electronic signatures: simple electronic signature, unqualified advanced electronic signature and, qualified advanced electronic signature. There is an increase in both the number of closed contracts and public-key certificates. The increased security of the electronic signature allows the signed documents to ensure that they can no longer be modified or altered in any way.

Keywords: *digital signalture, financial institutions, financial services, legal procedure, securitization, technological innovation, technological change, technological impact.*

JEL Clasification: *G200, G210, K400, O320, O330*

INTRODUCERE

Internetul este o componentă indispensabilă a societăţii contemporane iar impactul acestuia asupra proceselor economice, comportamentelor sociale şi atitudinii morale a persoanelor, se află într-o continuă ascensiune, catalizată de răspândirea tot mai trepidantă a interacţiunii om–platforme sociale, precum şi de digitalizarea vieții cotidiene, în general. Denumită generic internet, reţeaua de computere extinsă la nivel global reprezintă un suport tehnologic comod pentru o nouă formă de comunicare virtuală. Indiferent care dintre atributele nominative le va prelua efectul tehnologic al internetului – ”electronic”, “virtual”, “cyber”, “on-line”, sau extinderea terminologiei pe procesele sociale cum ar fi: grupuri virtuale, interacţiuni virtuale, comunicare mediată de computer, comerţ electronic, guvernământ on-line, semnătură electronică (e-signature), etc., acesta condiționează virtualizarea societății. În acest context, oportunitățile digitalizării au devenit tot mai accentuate, mai competitive, mai conectate la mediul extern şi inevitabil – mai calitative. Totodată impactul internetului asupra mediului de afaceri este un fenomen complex, a cărui valenţă este greu de cuantificat, şi determină evoluții imprevizibile. Specificul de ajustare la acest fenomen ține de inteligenţa şi capacitatea de adaptare a fiecărei economii,

de abilitatea selectării modelelor de business pentru a ajunge mai uşor la potenţialii clienţi şi pliază pentru un mediu social-virtual cât mai real. Consecinţele utilizării internetului pe scară largă are un efect asupra întregii societăţi, prin ralierea la tehnologia informatică, care oferă acces cognitiv, tehnic şi financiar aproape instantaneu, antrenând un număr în continuă creştere de utilizatori.

CONSIDERAŢII GENERALE

Viaţa modernă a devenit mai uşoară datorită contribuţiei imense a utilizării tehnologiilor, care au facilitat accesul la comunicare şi schimb de informaţii fără nici o barieră. Digitalizarea proceselor de lucru la nivelul autorităţilor publice, agenţilor economici şi a persoanelor fizice este direct condiţionată de utilizarea acestor tehnologii, şi în speţă a semnăturii electronice. Metodele tradiţionale pentru semnarea şi autentificarea diverselor tipuri de documente au fost înlocuite rapid de inovaţii tehnologice menite să eficientizeze şi să înlesnească munca. Poate una dintre cele mai utile este semnătura electronica, introdusă în SUA de mai bine de 10 ani, care a devenit un suport pentru orice antreprenor care nu vrea să îşi piardă timpul stând la cozi sau lovindu-se de birocraţia complicată în interacţiunea cu instituţiile statului.

În Republica Moldova, noţiunea de semnătură electronică a fost introdusă prin Legea nr.264/2004 cu privire la documentul electronic şi semnătura digitală, iar ulterior, în vederea creării cadrului comunitar pentru semnăturile electronice, a fost aprobată Legea nr.91/2014 privind semnătura electronică şi documentul electronic. Utilizarea semnăturii electronice ca metodă de identificare şi autentificare atât pentru persoanele fizice, cât şi pentru persoanele fizice în interesul persoanelor juridice reprezentată o soluţie optimă pentru nivelul de dezvoltare tehnic şi juridic al R. Moldova.

Semnătura electronică reprezintă date în formă electronică, care sunt ataşate sau logic asociate cu alte date în formă electronică şi care sunt utilizate ca metodă de autentificare. Prin asociere, semnătura electronică reprezintă un eşantion de date ce demonstrează că unui document i s-a ataşat o semnătură. Totodată, în cazul în care se cere ca documentul să fie perfectat sau prezentat pe suport de hârtie, semnat cu semnătura olografă sau şi autentificat cu ştampilă, documentul electronic se consideră a fi corespunzător acestei cerinţe [1].

În Republica Moldova, cadrul normativ reglementează trei tipuri de semnături electronice [1]:

Semnătura electronică simplă este utilizată ca metodă de autentificare, fără a face trimitere exclusiv la semnatar şi nu se bazează pe certificate electronice. Semnăturile simple utilizează orice date în format electronic, ataşate sau logic asociate la alte date electronice. Documentul semnat cu semnătura electronica simplă este asimilat, după efectele sale, cu documentul analog pe suport de hârtie, semnat cu semnătură olografă, doar în cazurile stabilite expres de actele normative sau de acordul părţilor, privind aplicarea semnăturilor electronice.

Semnătura electronică avansată necalificată este o semnătură electronică ce face trimitere exclusiv la semnatar şi permite identificarea acestuia. Ea este creată prin mijloace controlate exclusiv de semnatar, este dependentă de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată.

Semnătura electronică avansată calificată este o semnătură electronică care îndeplineşte toate cerinţele semnăturii electronice avansate necalificată şi se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de certificar, acreditat în domeniul aplicării semnăturii electronice avansate calificate. Semnătura este creată prin intermediul dispozitivului securizat de creare a semnăturii electronice şi se verifică

securizat cu ajutorul dispozitivului de verificare a semnăturii electronice şi/sau al produsului asociat semnăturii electronice, care dispun de confirmarea corespunderii cu cerinţele prevăzute de prezenta lege.

Autenticitatea semnăturilor electronice este determinată de măsurile de securitate pe care le deține fiecare tip în speță (tab.1).

Tabelul 1. Parametrii specifici categoriilor de semnături electronice

	Tipuri de semnături electronice		
	Simplă	***Avansată necalificată***	***Avansată calificată***
Se utilizează ca metodă de autentificare	*	*	*
Face trimitere exclusiv la destinatar		*	*
Permite identificarea semnatarului		*	*
Este creată prin mijloace controlate exclusiv de semnatar		*	*
Este legată de datele la care se raportează, astfel încât orice modificare ulterioară a acestor date poate fi detectată		*	*
Se bazează pe un certificat calificat al cheii publice emis de un prestator de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate			*
Este creată prin intermediul dispozitivului securizat de creare a semnăturii electronice şi se verifică securizat cu ajutorul dispozitivului de verificare a semnăturii electronice			*

Sursa: https://www.atic.md/files/Ghid-Semn%C4%83tura-Electronic%C4%83-Final.pdf , pag 5

Astfel, instituţiile publice şi-au eficientizat activitatea, accelerând întregul proces de preluare şi prelucrare a datelor. Beneficiile acestei tehnologizări sunt proiectate către instituţiile publice şi cele private, întrucât utilizarea semnăturii digitale în serviciile publice electronice a redus timpul de aşteptare la ghişee şi riscurile asociate cu erorile de îndeplinire a formularelor. La momentul actual, companiile private, precum şi entităţile publice care deţin un certificat digital, pot beneficia de serviciile publice electronice în vederea transmiterii, în mod electronic, a informaţiei atât către cele mai importante instituţii de stat (Serviciul Vamal, Serviciul Fiscal de Stat, Casa Naţională de Asigurări Sociale, Casa Naţională de Asigurări în Medicină, Agenţia Achiziţii Publice, Trezoreria de Stat, Camera de Licenţiere, Serviciul Stare Civilă, Banca Naţională a Moldovei), cât şi către companii private (Î.M. Biroul de Credit). Furnizorii ce permit obţinerea semnăturii electronice în conformitate cu Legea Nr. 91 din 29.05.2014 sunt:

- Î.S. „Fiscservinform”
- Î.S. „Centru de telecomunicaţii speciale”
- S.A. „Orange”
- S.A. Moldcell
- Centrul Resurselor Informaţionale de Stat „REGISTRU”

Semnătura electronică se aplică împreună cu marcajul temporal, adică cu indicarea timpului semnării şi nu poate fi aplicată retroactiv. Totodată, semnarea retroactivă, validitatea documentului şi condiţiile aferente pot fi negociate de părţi, conform regulilor generale în materie civilă. Termenul de valabilitate a cheii private şi certificatului cheii publice utilizate la crearea semnăturii electronice avansate calificate este de 2 ani.

Semnătura electronică înscrie un model de semnare și verificare a documentului digital astfel încât acesta se conectează la identitatea electronică a semnatarului (fig.1).

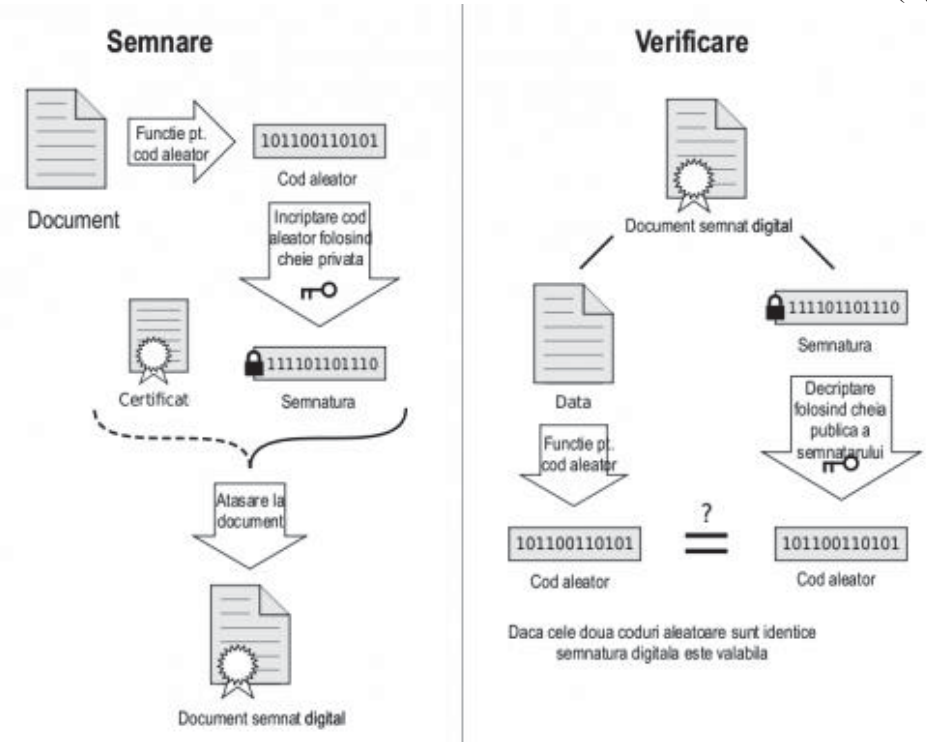


Figura 1. Modul de semnare și verificare a documentului digital semnat electronic

Sursa: https://www.atic.md/files/Ghid-Semn%C4%83tura-Electronic%C4%83-Final.pdf , pag 10

Actualmente, în R. Moldova există peste 70 de servicii electronice publice prestate prin intermediul Portalului serviciilor publice, și paginilor web oficiale ale instituțiilor publice. La moment, semnătura electronică este utilizată, în mare parte, în raporturile dintre persoanele fizice și juridice de drept privat cu persoanele juridice de drept public, în special la depunerea declarațiilor și raporturilor fiscale, în alte cazuri fiind dată în continuare prioritate semnăturii olografe. De menționat, că tehnologia infrastructurii cheilor publice permite realizarea pe baza acesteia a mai multor tipuri de servicii, menite să acopere majoritatea cererilor utilizatorilor. Astfel, există posibilitatea creării și utilizării, inclusiv de către sistemele automatizate a sigiliilor electronice, care se atribuie direct unei persoane juridice sau unui sistem informațional distinct. Deși numărul prestatorilor de servicii de certificare a scăzut, ca urmare a consolidării centrelor de date în sectorul public, numărul persoanelor care solicită prestarea acestor servicii este în continuă creștere. Astfel, conform datelor prezentate de prestatori de servicii de certificare se înscrie o majorare atât a numărului de contracte încheiate cât și a certificatelor de chei publice (tab. 2).

Tabelul 2. Date statistice cu referire la numărul de contracte și chei publice înregistrate în R. Moldova

Anul de referință	*Numărul de contracte încheiate*	*Certificate a cheilor publice*
2016	23 391	32 361
2017	30 240	69 745
2018	23 457	150 565
2019	34 976	160 327

Sursa: date adaptate în baza informațiilor publicate de Centru de Tehnologii Informaționale în Finanțe

Avantajele pe care le oferă semnăturile electronice sunt vădite și plauzibile, ceea ce permit cu ajutorul unui singur click să asigurăm:

- confidențialitatea datelor;
- siguranța și ușurința în utilizare;
- fluidizarea circuitului documentelor;
- o mai bună comunicare între instituții prin transmiterea documentelor semnate în format electronic;
- garanția autenticității semnăturilor pentru eliminarea oricăror dubii cu privire la eventualele substituiri de persoane sau falsuri;
- eliminarea necesității de a tipări documentele doar pentru a fi semnate;
- reducerea costurilor;
- semnatarul nu poate nega în fața justiției faptul că el este expeditorul documentului.

CONCLUZII

Securitatea sporită a semnăturii electronice permit ca documentele semnate să asigure garanția că nu mai pot fi modificate sau alterate în vreun fel, în mod intenționat sau din greșeală. Fiecare semnătura este protejata, astfel încât ești notificat atunci când apare vreo schimbare în documentul respectiv. In plus, poți beneficia și de un istoric al tuturor modificărilor efectuate, ceea ce asigură o siguranță amplificată. Semnătura electronică este protejată și împotriva falsificării, ceea ce înseamnă mai multă securitate pentru documentele importante.

Necesitatea utilizării acestui instrument de lucru a crescut exponențial în ultima perioadă, precum și volumul de documente semnate și transmise electronic. Astfel, încrederea și viitorul comerțului electronic în condiții ridicate de securitate depinde de evoluția semnăturii electronice.

BIBLIOGRAFIE

1. Legea nr. 91/2014 privind semnătura electronică şi documentul electronic
2. https://semnatura.md
3. https://stisc.gov.md/ro/semnatura-electronica
4. https://www.ctif.gov.md/ro
5. https://raportare.gov.md/page/semnatura-electronica
6. https://monitorul.fisc.md/
7. https://statistica.gov.md/
8. http://ict.md/files/Ghid-Semn%C4%83tura-Electronic%C4%83-Final.pdf
9. https://www.atic.md/files/Ghid-Semn%C4%83tura-Electronic%C4%83-Final.pdf

SPECIFICITY OF SOCIO-ECONOMIC DEVELOPMENT OF CEE COUNTRIES UNDER CONDITIONS OF ECONOMIC INTEGRATION

Dilan Neli
PHd student, assistant
State University of Moldova
e-mail : dilan.nelly@yahoo.com

Abstract
The relevance of the problem is due to the need to develop strategies for the international development of the Central and Eastern Europe Countries (CEE), due to its current priorities, specific features and needs of the socio- economic development of the economic region. The experience gained by the developing countries of Central and Eastern Europe proves the diversity of national models of participation in economic integration processes, as well as to the ambiguous results of their implementation. The specifics and ambiguous consequences of the CEE countries development within the EU are of particular interest to developing countries located in close proximity to the borders of this integration association.

Keywords: *CEE countries, integration processes, the socio-economic dynamics, promotion of international development, labor productivity, unemployment, poverty.*

JEL Classification: *P4*

INTRODUCTION

Regional integration forms not only economic relations, but also many economic problems that can no longer be resolved by individual countries. As a result of the fact that the nature of the distribution of the additional gross product produced by the economies of the countries involved in the integration process favors, the accumulation of capital rather than the growth of consumption, the gap between the economically developed countries and the EU "periphery" states widens. Integration associations are increasingly influencing on the dynamics of the development of member countries, the groupings and on the global economy as a whole.

The toughening of competition in the world labor market creates problems in industrialized countries, which sometimes close production, transferring it to developing countries with a low labor price. And new jobs are created at new facilities of multinational companies (TNCs) where in general the working conditions leave much to be desired, despite its increasing productivity. With the growth of opportunities for improving the material situation of the world's population, inequality of access to them is the main obstacle to the transformation of economic growth into full-fledged sustainable economic development. Thus, under the influence of global competition, the social climate in even developed countries worsens, and the treat of unemployment increases.

PAPER BODY

The development of countries of such world region as Central and Eastern Europe (CEE), at the present stage, is characterized by the presence of many heterogeneous problems in the socio-economic and labor spheres (low in comparison with the average European level of labor productivity), overcoming of which becomes very important for the countries of this region in the view of their strategic course towards rapprochement in terms of the level of economic development with Western European states, adopted in order to deepen European integration. Within this region, there is great variability in living

standards and economic development. On the territory of the European Union there has not been formed yet a single place with equal social conditions and opportunities for all groups of the population. This fact is a significant obstacle to the development of the EU as a whole country and of member states individually.

Despite the successful creation of a single domestic market and other events, the European Union is still far from becoming a truly single and homogeneous economic space in which member states move forward at the same speed and participate on an equal footing in the implementation of integration programs, although such an integration philosophy was originally laid the foundation for the creation of the Union.

On the whole, in terms of labor productivity, the countries of Central and Eastern Europe are inferior to developed Western European states, which, given the internationalization of economic ties across the European Union and the whole of Europe, and the industrial and investment expansion of the West to the East of Europe, exacerbates the gap in the level of nations well-being and contributes to the concentration created in Eastern Europe, the surplus value is not in the hands of the local population involved in its creation, but in the form of capital of funds owners from the Western part of it. Although, in general, the countries of Central and Eastern Europe stand out among the remaining regions of this part of the world and the world as a whole with relatively high rates of economic growth [1].

On the background of a general tendency toward the decrease in the unemployment rate, its surge was noted in 2009, when a ubiquitous rapid growth of the indicator began, the rate of which continued to increase in 2010 and slightly decreased only in 2011-2013. As a result of the crisis, the position of young people at the labor market has also worsened significantly. The growth rate of youth unemployment is 5 times higher than among the adult population, which is associated with the difficulties in moving from training to a specialty to work due to a lack of experience in conducting it, as well as the difference between the acquired skills and the employers' requirements.

Facing such challenges, limited by declining state budgets, national governments, while pursuing active employment policies, are not able to implement large-scale long-term employment programs and are forced to rely on part-time and temporary employment.

Intensification of technological modernization of national production and stimulation of labor productivity growth is a priority in promoting socio-economic development, focusing on an active employment policy that European governments calls for, by the international community will not give the best effect in terms of improving the welfare of the population and long-term employment in most countries of Central and Eastern Europe. A more effective means of increasing the level of population's income in the general case will be to facilitate the emergence of new industries with labor productivity higher than the national average in the country.

The revealed contradiction of the pan-European policy in the field of socio-economic development and the actual needs to promote such development in the countries of Central and Eastern Europe is due to the fact that often the current policy objectives of the national and supranational levels are determined solely on the basis of the generalized dynamics of statistical indicators of economic development, without taking into account regional specifics existing relations between them. Meanwhile, an analysis of these relationships allows us to identify the causes of the decline in the level of population incomes and economic growth rates, and not only to discover the consequences of their manifestation.

Table 1. Absolute indicators of migration in the world regions

	2002	2007	2012	2017
Eurozone	6731514	4671862	1929664	3318998
European Union	7257129	6281070	2939221	4320989
CEE	-804567	-993491	-553383	-243005
Japan	164199	277580	358133	250000
The USA	5206538	5033689	4500000	4500000

Source: https://www.worldbank.org/

However, it is too early to talk about a coordinated social policy on the territory of the Union, although it should be noted that the European Commission takes many measures to coordinate the measures of the EU member states in the field of social sphere. Currently, migration problems are relevant especially after the EU has expanded eastward (Table 1). According to statistics, the number of migrants illegally arriving in the EU ranges from 4.5 to 8 million people, and their number is growing by 350-500 thousand every year.

The countries development of such region of the world as Central and Eastern Europe (CEE), at the present stage, is characterized by the presence of many heterogeneous problems in the socio-economic and labor spheres (low in comparison with the average European level of labor productivity), overcoming of which becomes very important for the countries of this region in the light of their strategic course towards rapprochement in terms of the level of economic development with Western European states, adopted in order to deepen pan-European integration. Within this region, there is great variability in living standards and economic development.

Due to the efforts of the EU, it was possible to achieve a noticeable unity of its members in a common understanding of the so-called pan-European values, in pursuing a coordinated foreign policy, in creating a common market for goods, services and capital, in expanding mutual trade and economic relations. The countries of Central and Eastern Europe differed from each other in their economic potential even at a time when they were all socialist states. Czechoslovakia had a higher level of development when Hungary had somewhat lower.

With the process of rapprochement of the CEE states within the European Union, tendencies of their differentiation have emerged, which determine the current heterogeneity of the economic condition of the countries of this region.

Conventionally, two directions of differentiation can be distinguished:

- minimal reduction of differences between Central and Eastern Europe, integrating within the framework of the European Union, from Western;
- differentiation within the East European space, expressed in significant differences between integrating countries.

The position of the East European countries in comparison with their western neighbors remains multilevel. Almost 30 years after the start of socio-economic transformations, the CEE countries not only lag behind the average European level of GDP per capita, but also differ (also very significantly) among themselves. Romania, Bulgaria and Croatia are very different in this indicator from the Czech Republic, Poland and Slovenia.

According to Eurostat, the total GDP of the transforming CEE countries amounted to 8.5% of the EU's GDP for 2017. The largest contribution to the total EU GDP from CEE countries was made by Poland 3%, Czech Republic 1.3%, Romania 1.2%, Hungary 0.8%, which in general makes up two thirds of the total GDP of CEE. The remaining economies

of this region are marked by shares in the total EU GDP: Slovakia 0.6%, Slovenia, Bulgaria, Croatia and Lithuania 0.3% each, Latvia and Estonia 0.2% each.

With regard to mass migration of labor from CEE countries to the western EU countries, its possible consequences were considered very uncertain.

Table 2. Dynamics of labor migration from CEE countries, thousand, people

	2002	*2007*	*2012*	*2017*	*Population for 2018, million*
Bulgaria	-85500	-83742	-24472	-24001	7024216
Czech republic	47402	250889	59997	59997	10625695
Estonia	-18406	-15151	-10516	-4999	1320884
Hungary	61589	25150	29999	29999	9768785
Lithuania	-99104	-150930	-146217	-25000	2789533
Latvia	-72490	-86594	-83325	-50000	1926542
Poland	-183471	-178456	-73997	-50002	37978548
Romania	-468204	-774651	-299997	-150000	19473936
Slovakia	1199	-8855	11346	4999	5447011
Slovenia	14998	39348	16571	6002	2067372
Eurozona	6731514	4671862	1929664	3318998	341783171
Croatia	-2580	-10499	-32772	-40000	4089400

Source: compiled by the author based on data from the World Bank http://www.worldbank.org

Short-term forecasts determined labor migration from east to west of Europe in the amount of 300-350 thousand people. in the early years of expansion. According to long-term forecasts, the total volume of labor migration was estimated at around 3 million people, that is, only 1.2% of the working population of the Eurozone in 2020, but this forecast is far from the truth if we rely on data from the World Bank [5]. Already the first years of CEE membership have shown that the percentage of labor in the EU-15 markets are steadily increasing, especially after a restraining three-year transition period, indicated by some Western European countries: Britain, Austria and Ireland.

The maximum outflow of labor (a little less than 775 thousand people) was noted in Romania in 2007, the year the country joined the EU. In subsequent years, emigration from Romania decreased, but keeps the country in the position of a leader by this indicator in the region (Table 2). A significant outflow of the population is also observed in the Baltic countries, especially in Lithuania and Latvia, if we take the analysis of the total population of these countries as a basis (Table 2). This situation is not observed in all countries of the region. The Czech Republic, Hungary, Slovenia and Slovakia became attractive for labor migration from European transforming countries. In Poland, there is a gradually decreasing outflow of labor resources, if in 2002 more than 183 thousand people emigrated. for the year, then in 2017 this indicator dropped to 50 thousand people (Table 2).

However, the volume of labor migration from CEE is insufficient to significantly affect of the structure and levels of wages in the EU labor markets. In most countries of the region, labor resources are declining due to aging, but also due to migration outflows. Over time, a growing number of retirees and shrinking labor resources will lead to lower economic growth and increased budget deficits.

Of major concern in European recipient countries is migration from third countries. At the present stage, the population of the European Union is growing due to the influx from third countries, on average by 1 million people in year.

Differentiation is also noted in terms of unemployment rates. But in this case, the unemployment rate in CEE countries is lower than the EU average. According to Eurostat,

as of June 2019 the EU unemployment rate was 6.3%, in Germany 3.1%. This is the lowest figure since June 2008. In the transforming CEE countries, unemployment in the Czech Republic reaches 2.2%, in Hungary, Poland and Romania more than 3%, in the Baltic countries about 6%, in Croatia 7% [3]. Whereas in the Eurozone this indicator is higher not only in comparison with the CEE countries, but also in the EU as a whole, reaching 7.5%. However, this is the lowest unemployment rate in the Eurozone since May 2008. Eurostat notes that youth unemployment is stronger: in the EU - 14.2%, and in the Eurozone 15.4% [3].

All CEE countries, without exception, suffered from the global financial economic crisis in 2008, which was far from the same for them and strengthened their further differentiation. The crisis had a negative impact on the reproductive processes of CEE countries. The main reason for the slowdown in real production during the crisis was the lack of investment capital. This was reflected in a decrease in the added value of all three sectors of the economy, but the losses were uneven across countries. In general, the crisis caused an increase in the divergence of the economic development of the EU countries.

The process of differentiation continued during the period of post-crisis recovery, which took place at different speeds in individual countries. In 2017, almost all CEE countries exceeded the pre-crisis level in terms of GDP (Table 3.). Poland was the only country that did not experience a recession in 2009 and has shown steady economic growth over recent years [2]. Obviously, Poland during this period was ahead of other states in the region in achieving a higher level of economic development due to the relatively solid growth rate of its GDP.

Table 3. GDP growth dynamics in CEE and the Eurozone (%)

	2004	*2005*	*2008*	*2009*	*2012*	*2013*	*2017*	*2018*
Czech republic	4,9	6,5	2,7	-4,8	-0,8	-0,5	4,4	2,9
Hungary	5,1	4,4	0,9	-6,6	-1,6	2,1	4,1	4,9
Poland	5,1	3,5	4,2	2,8	1,6	1,4	4,8	5,1
Slovenia	4,4	4	3,3	-7,8	-2,7	-1,1	4,9	4,5
Slovakia	5,3	6,8	5,6	-5,4	1,7	1,5	3,2	4,1
Romania	10,4	4,7	9,3	-5,5	2,1	3,5	7	4,1
Bulgaria	6,4	7,1	6	-3,6	0	0,5	3,8	3,1
Croatia	3,9	4,1	2	-7,3	-2,3	-0,5	2,9	2,6
Latvia	8,3	10,7	-3,5	-14,4	4	2,4	4,6	4,8
Lithuania	6,6	7,7	2,6	-14,8	3,8	3,5	4,1	3,5
Estonia	6,3	9,4	-5,4	-14,7	4,3	1,9	4,9	3,9
Eurozona	2,3	1,7	0,5	-4,5	-0,9	-0,2	2,4	1,9

Source: compiled by the author based on data from http://www.worldbank.org

The different dynamics of economic growth mainly depends on internal savings, due to which there is an expanded reproduction in the country. Consequently, the level of economic development of CEE countries is largely determined by the value of the investment rate, which affects the subsequent economic and social dynamics. In the short term, the further differentiation of countries will largely depend not only on their rate of internal accumulation and inflow of foreign funds, but also on the progress of development accumulated by each of them.

Despite the relative economic activity in the region, convergence between Western and Central Europe will take longer than anticipated. This is because in the longer term,

the growth potential (the most acceptable production growth expected in the economy) in most countries of Central and Eastern Europe is still significantly lower than before the global financial crisis of 2008 (Table 3).

In anticipation of the next planning period 2021–2027 the European Commission has prepared a new appropriation program called Cohesion and Values. It is planned to change the system of funds distribution between EU countries. It is supposed to apply an extensive system of criteria, taking into account, in particular, the unemployment rate among young people, the state of education, environmental protection, migration, innovation, and the fight against corruption.

CONCLUSIONS

So, purely quantitative data indicate that according to various important indicators, the process of differentiation of CEE countries is constantly ongoing. Some states temporarily overtake others, then slow down their growth, while others steadily accelerate economic development. Moreover, a more favorable starting position does not always guarantee further success. Practice shows that countries with large production potential, as a rule, achieve better results. This can be said about the Czech Republic and Slovenia, but not about Hungary, in which there was a degradation of agriculture and partly industry.

Between them, differentiation is increasing due to different adaptability to pan-European economic conditions and lack of competitiveness. The modern scenario allows the existence of concepts as “concentric circles” or “Europe of different speeds,” that is, each country will choose the degree of acceleration for further integration. Differentiation of CEE countries will continue in the future, not only due to different levels of their development, but also due to the characteristics of cultures, mentalities, traditions, social relations.

The long process of integration of the countries of Central and Eastern Europe into the European Union is far from over. It takes place in a difficult international environment, amid instability in Europe and a premonition of a new wave of global crisis.

BIBLIOGRAPHY

1. Евроинтеграция: влияние на экономическое развитие Центральной и Восточной Европы. Доклады Института Европы. № 303. М., 2014.
2. Marzenna Anna Weresa. Poland. Competitiveness report 2016 the role of economic policy and institutions. Copyright by the Warsaw School of Economics, Warsaw 2016
3. Eurostat electronic database http://ec.europa.eu/eurostat
4. World Bank Group http://www.worldbank.org
5. http://dealerpride.ru/vnzh/the-countries-of-the-european-union-for-a-year-the-economy

RETHINKING THE CONCEPT OF NATIONAL EXTERNAL ECONOMIC SECURITY

К ВОПРОСУ ПОСТРОЕНИЯ КОНЦЕПТА НАЦИОНАЛЬНОЙ ВНЕШНЕЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Киртоагэ Роман
Аспирант, Академия Экономических Знаний Молдовы
e-mail: chirtoagar@gmail.com

Abstract
In the paper is examined the concept of national external economic security based on the rethinking of the categories of general external economic security and factor of external medium. As an object of study of the scientific discipline are examined exogen shocks for national economy, and as a protected value – the capacity of national economy to satisfy material necessities of society, namely, maximally possible long-term economic growth, national internal economic cohesion and national economic sovereignty. Examining the factor of external medium is positing a notion of the geographical zone of national external economic interests.

Keywords: *external economic security, concept, economic growth, national internal economic cohesion, national economic sovereignty, the zone of priority external economic interest.*

JEL Classification*: P4*

ВВЕДЕНИЕ

В настоящее время задача построения адекватного концепта национальной внешнеэкономической безопасности (далее НВЭБ), способного стать прочным базисом для эффективной теоретической и практической деятельности, сохраняет свою актуальность. Анализ литературы в данной области свидетельствует о том, что в настоящее время проблематика НВЭБ занимает периферийное положение в поле зрения исследователей национальной экономической безопасности (далее, ВЭБ) и не имеет общепринятой трактовки в научной среде.

Так, Фокин, один из ведущих авторов, специализирующихся в рассматриваемой тематике, выделяет три подхода в отношении концепта НВЭБ: сателлитный, автономный и ситуативный [7]. В первом случае считается, что предмет исследования данной дисциплины фактически уже изучается в рамках экономической науки, как две важные категории – конкурентоспособность на международных рынках и устойчивость перед внешними шоками, а также, как ряд отдельных междисциплинарных проблем – энергетической безопасности, миграции и т.д. Такой подход доминирует в западной научной среде в русле ее отношения к теории экономической безопасности в целом и поддерживается рядом авторов постсоветского пространства [5; 4; 1]. Необходимо отметить, что многие элементы проблематики НВЭБ изучаются в рамках международной политэкономии, научной дисциплины близкой к секьюритологии (security studies) [16], внимание которой фокусируется на интересах, преследуемых государством в ходе международного экономического взаимодействия – максимизации национального агрегированного дохода, политической власти, социальной стабильности и экономического роста [17]. В рамках второго подхода, поддерживаемого большинством авторов постсоветских школ, НВЭБ рассматривается как отдельная научная категория, с собственными специфическими угрозами и вызовами, деятельность по обеспечению

безопасности от которых относится к компетенции государства. Третий подход, предлагаемый самим Фокиным, сочетает первые два, суть его отражена в предлагаемой дефиниции ВНЭБ: внешнеэкономическая безопасность представляет собой конкурентоспособность национальной экономики, которая обеспечивает ее защиту от внешних угроз и вызовов, и, таким образом, ее устойчивое развитие. Более широкое определение НВЭБ, в русле большинства работ стран постсоветского пространства, предлагает Шаламов: устойчивость национальной экономической системы к экзогенным шокам экономического или политического характера, выраженная в ее способности к нейтрализации потенциальных источников этих шоков и минимизации нанесенного ими ущерба [8]. То есть, данная дефиниция, по сути, отражает взгляд на концепцию НВЭБ как на частное проявление общей теории НЭБ, специфика которого выражается в существовании внешнего контекста, в первую очередь, как источника внешних деструктивных воздействий – угроз и вызовов.

Принимая в качестве базового второй подход (по Фокину), как строящийся на наиболее прочном теоретическом фундаменте, логично сделать вывод, что концепт НВЭБ основывается на базовых элементах общей теории национальной экономической безопасности и, следовательно, разделяет ее основные проблемы – застой в развитии концепта [6] и слабую практическую применимость.

Таким образом, целью настоящей статью является формулирование основных параметров концепта НВЭБ, которые могли бы устранить указанные ограничения, при сохранении в качестве фундамента теории национальной экономической безопасности. В ходе исследования для достижения поставленной цели используется метод научного анализа.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Представляется, что основная причина существующих трудностей кроется в сложной междисциплинарной природе теории НЭБ, которая соединяет элементы политологии и экономики и требует особо методологически выверенного подхода [14]. Исходя из недостатков актуального общего подхода, на наш взгляд, недостаточно учитывающего возможности экономической науки, считаем необходимым выработку иных принципов структурирования знаний в этой области. По нашему мнению, ключевой задачей, в данной связи, является идентификация системы оценки безопасности ценностей, способной соединить элементы обеих наук, в частности, могла бы отражать понятия из политологии в экономических категориях, которые стали бы органичной частью материи, в целом являющейся экономической. Такие категории как «безопасность», «угроза», «риск» и т.д. должны быть сформулированы в рамках простого и связного концепта, который позволил бы удобное и надежное оперирование ими, в том числе, в рамках практической деятельности.

В русле этой логики, попытаемся выстроить общую архитектуру модели оценки состояния безопасности ценности, которая могла бы лечь в основу анализа, как на уровне теории, так и в практической деятельности (см. рис.1).

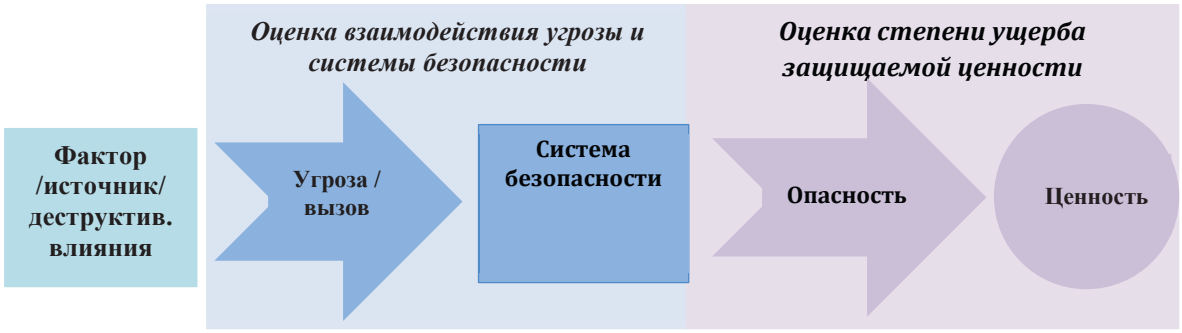


Рисунок 1. Общая модель оценки состояния безопасности ценности

Источник: разработка автора

Так, анализ состояния безопасности защищаемой ценности включает, на наш взгляд, исследование следующих компонентов и связи между ними: защищаемая ценность – ЗЦ , деструктивное влияние – ДВ, система безопасности – СБ.

Соответственно, вывод относительно безопасности/небезопасности защищаемой ценности может быть сделан в зависимости от соотношения между уровнем деструктивного влияния и эффективностью системы безопасности:

$$Безопасность_{ЗЦ} = СБ - ДВ, \quad (1)$$

В результате, могут складываться следующие ситуации:

1) ДВ > СБ. В данном случае сила деструктивного влияния превосходит защитные возможности системы безопасности (то есть, в ней существуют **уязвимости**) и это влияние переходит со стадии **угрозы / вызова** в фазу **опасности**.

2) ДВ < или = СБ. В данном случае, соответственно, система безопасности в состоянии сдержать деструктивное влияние и предотвратить наступление негативных эффектов для защищаемой ценности.

3) Какой-то из параметров не известен, соответственно, нельзя сделать вывод о перспективах перехода деструктивного влияния из формы угрозы / вызова в опасность, то есть, имеет место ситуация **неопределенности** и существуют **риски** такого перехода.

Изложенная модель предоставляет рамку, в которой можно рассматривать базовые параметры теории НЭБ.

Центральную роль в рамках концепта безопасности занимает понятие защищаемой ценности (называемой в западной науке *референтом* безопасности), то есть, любого предмета, феномена, и т.д., который представляет важность и, соответственно, определяет интерес в недопущении негативного изменения его качественных / количественных характеристик. Следовательно, ответ на вопрос, какая ценность защищается в ходе деятельности по обеспечению НЭБ является фундаментальным, предоставляющим основу для построения всего концепта.

Пожалуй, наиболее маститый из немногих западных ученых, рассматривающих данный вопрос, Барри Бузан, полагает, что референтом НЭБ является отсутствие ситуации национального банкротства или неспособности удовлетворения базовых потребностей населения [12]. Представители пост-советских школ рассматривают в этой роли: национальную экономику, независимость, стабильность и прогресс (Л. Абалкин), экономику, национальные интересы, жизненные стандарты и военную безопасность (В. Сенчагов), национальные экономические интересы, независимость и устойчивость к внешнему и внутреннему негативному влиянию (С. Степашин), экономику, продуктивные

силы общества и устойчивое социально-экономическое развитие (С. Глазьев), прогресс, рост жизненных стандартов и военную безопасность (И. Богданов), национальную экономику, прогресс, рост жизненных стандартов и военную безопасность (Е. Олейников) и др.

Представляется, что ответ на указанный вопрос можно получить, опираясь на концепт континуума безопасности-развития, в соответствии с которым всю продуктивную деятельность общества можно разделить на две категории, реализующие, соответственно, императивы безопасности и развития [подробнее, 3]. В этом смысле, в основе императива развития находится экономическая система общества, рассматриваемая в широком смысле, в условиях автаркии, как совокупность материальных благ, произведенных обществом и, одновременно, ее способность произвести эти блага. Понимание аккумулированных материальных благ и производственных возможностей, как двух различных категорий с приматом последней, существует еще из периода меркантилизма, а Ф. Лист в XIX веке отмечал, что «сила создания богатства намного важнее, чем сама экономика» [List, 1856]. Основная задача этой системы состоит в удовлетворении материальных потребностей общества – повышении жизненных стандартов его членов, научно-технического развитии, улучшении возможностей обеспечения безопасности и т.д. Ответ экономики на эти потребности – рост. Соответственно, в рамках предлагаемого подхода, понятие НЭБ тесно связано с феноменом качественного и количественного развития материальной базы общества в широком смысле, включающего все элементы, способствующие экономическому росту – от здоровья населения до безопасности инфраструктуры.

Таким образом, защищаемой ценностью в деятельности по обеспечению НЭБ является способность экономической системы национального государства обеспечивать его материальные потребности. Исходя из специфики ее взаимодействия с императивом обеспечения безопасности, можно выделить три измерения данной ценности, которые могут рассматриваться как национальные интересы с сфере НЭБ: максимально возможный долговременный экономический рост, внутренняя экономическая связанность государства и национальный экономический суверенитет.

Исходя из изложенного, **национальная экономическая безопасность – это защищенное состояние национальной экономической системы от деструктивного влияния на ее способность удовлетворения материальных потребностей гражданина, нации и государства, выраженное в обеспечении максимального долговременного экономического роста, внутренней экономической связанности государства и национального экономического суверенитета.**

Таким образом, основным параметром императива развития является **долговременный экономический рост**, кратковременные же колебания (стабильность экономической системы), рассматриваемые через призму влияния на ритмы долговременного роста, представляют его составную часть. В литературе такой взгляд близко коррелируется с мнением А. Илларионова: «под экономической безопасностью государства понимается такая комбинация экономических, политических и юридических условий, которая обеспечивает устойчивое производство на душу населения в долговременной перспективе, наиболее эффективным способом» [2].

Такой подход позволяет разрешать проблемы НЭБ через использование системы знаний и научного инструментария теории экономического роста.

Современная наука рассматривает феномен экономического роста в условиях автаркии, с позиций неоклассической теории, исходя из эволюции стилизованных фактов, экзогенной теории и неоклассической функции, Y = f(K,AL) [27; 28; 29]. Модели, основанные на этой функции, объясняют базовые макроэкономические закономерности, установленные в рамках стилизованных фактов Н. Калдора. Параметр А, т.н. остаток Солоу, рассматривается исходя из уточненных стилизованных фактов, на основе эндогенных теорий экономического роста, выявляющих в качестве детерминантов долговременного экономического роста институциональные и поведенческие факторы.

Шараев, на основе современных исследований, компилирует основные дереминанты, включая неохваченные теорией эндогенного роста, в т. ч., демократия, коррупция, социальное неравенство, климатические условия, политическая нестабильность и т.д. [9]. Он выделяет следующие направления развития эндогенных теорий: (1) производство инноваций как результат деятельности специализированного сектора национальной экономики (авторы – Ромер, Гроссман, Хелпман); (2) рост человеческого капитала как результат деятельности, ориентированной на развитие человека – образование и perfecționare (Лукас, Мэнкью, Ромер, Вайл), а также обучение на практике (Ромер, Ребело, Барро); (3) социальный капитал; (4) международный капитал и распространение технологий (Гроссман, Хелпман, Барро, Салла-и-Мартин, Лукас, Вентура); (5) влияние политики на экономический рост; (6) модели прогресса и населения (Кремер, Хансен, Прескотт, Галор); (7) влияние социального неравенства на экономический рост (Бенабоу, Алесина, Родрик, Болтон).

В рамках такого подхода становятся измеряемыми негативные эффекты деструктивных воздействий (в т.ч. неэкономического характера) на национальную экономическую систему, что дает дисциплине НЭБ необходимую практическую ясность. Сам долговременный экономический рост может быть выражен в динамике ВВП на душу населения. Соответственно, тяжесть негативного воздействия может быть измерена через отклонение реального ВВП от потенциального ($Y - Y^*$), выраженного в процентных пунктах ВВП или реальном выражении (см. рис.2).

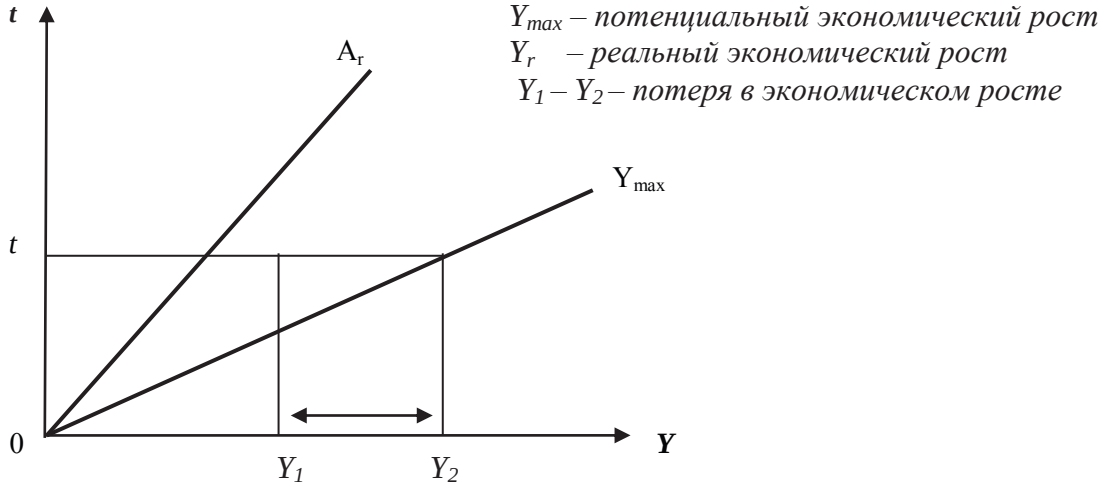


Рисунок 2. Негативное воздействие на долговременный экономический рост
Источник: разработка автора

Экономическая связанность государства означает в первую очередь наличие у членов определенного общества экономических мотивов сохранения необходимого уровня политического единства, как на уровне отдельных

территориальных общин, так и социальных групп. В первом случае, в условиях автаркии, речь идет о недопущении складывания самодостаточных региональных экономических систем либо создания других предпосылок для т.н. экономического сепаратизма. Связанность общества на уровне социальных групп тесно связана с оптимальным распределением продукта, созданного обществом и касается проблемы социальной справедливости. Перед обществом стоит задача занятия сбалансированной позиции между материальным стимулированием вклада наиболее способных членов общества в экономический рост и максимизации жизненных стандартов населения в целом. В этом смысле, государства могут использовать разные конфигурации соответствующих политик, ориентированных приоритетно на стимулирование роста или обеспечение социального равенства.

В качестве критериев оценки в этом случае могут быть использованы системы индикаторов, ориентированных на измерение степени социального неравенства, по типу индикатора Джинни.

Под **национальным экономическим суверенитетом** понимается способность государства самостоятельно осуществлять контроль над собственной экономической системой, без вмешательства иных сил (в закрытой экономике они будут иметь внутренний характер, как группы частных интересов, организованная преступности и т.д.). В данном случае, суверенитет представляет гарантию, что экономика будет использована в интересах гражданина и нации, особенно, в ситуации расхождения интересов национального государства и иных центров силы.

Вторым компонентом модели оценки безопасности защищаемой ценности является **деструктивное влияние**, обладающее потенциалом уничтожить либо снизить уровень полезности защищаемой ценности. Выделяют следующие формы такого влияния: угроза и вызов, а также, опасность, в случае преодоления им системы безопасности. В экономической теории близким аналогом синтагмы «деструктивное влияние» является научная категория **негативного шока** для экономики.

Защита национальных ценностей обеспечивается **системой безопасности**, определенной Концепцией национальной безопасности Республики Молдова как «ансамбль концептов, стратегий, политик, средств, регламентирований и административных структур государства, а также, ансамбль общественных институтов, комплекс человеческих и материальных ресурсов, организаций, политик, инфраструктуры и т.д.», предназначенных для предотвращения трансформации угрозы в опасность и наступления нежелательных эффектов для целостности защищаемой ценности. Система НЭБ, соответственно, ориентирована на идентификацию, оценку и предотвращение / снижение деструктивного влияния на долговременный экономический рост, внутреннюю экономическую связанность и национальный экономический суверенитет.

В теории экономической безопасности категория **риск** остается противоречивым понятием, который в значительной степени обусловил снижение интереса западных школ к практической применимости концепта НЭБ. Так, феномен развития подразумевает постоянный процесс изменения, трансформации, который неизбежно создает риски для стабильности существующей системы. То есть, экономический рост в рыночной экономике основан на т.н. феномене «креативного разрушения» [25], который может быть интерпретирован как потеря ее менее эффективной части в пользу другой, более конкурентоспособной и продуктивной. Другими словами, значительная часть шоков для экономики не просто представляет собой естественный результат процесса роста, а являются обязательным условием

этого роста. Бузан указывает, что «нормальное состояние актёров в рыночной экономике предполагает условия риска, агрессивной конкуренции и неопределенности» [11]. Следовательно, логично сделать вывод, что в условиях рыночной экономики не может ставится задача абсолютной экономической безопасности, которая априори не может быть достигнута. Представляется, что в этом случае можно использовать следующий контраргумент: НЭБ представляет собой не полное отсутствие угроз и рисков, а ситуацию, при которой угрозы не трансформируются в опасность. То есть, система НЭБ должна быть ориентирована не столько на устранение всех рисков, а скорее, на их мониторинг, контроль и управление, с целью недопущения наступления негативных эффектов для защищаемых ценностей.

Исходя из вышеизложенного, можно сделать вывод, что **предмет дисциплины НЭБ составляет всестороннее исследование негативных шоков для национальной экономической системы, их причин, природы и влияния на ее способность обеспечивать удовлетворение материальных потребностей гражданина, нации и государства, а также, изучение методов защиты и противодействия этим шокам.**

Специфика концепта НВЭБ в общей теории НЭБ заключается в существовании фактора внешней среды, с которой взаимодействует национальная экономическая система и которая обуславливает иную динамику ее функционирования, а также генерирует специфическое деструктивное влияние на защищаемые ценности. Таким образом, для построения концепта национальной внешнеэкономической безопасности, имея концепт НЭБ в качестве его основы, необходимо дать ответ на два вопроса: что представляет собой внешняя среда и как она влияет на способность экономической системы государства удовлетворять материальные потребности общества.

В литературе по международной экономической безопасности указывается на два уровня международного контекста: глобальный и региональный. Если сущность понятия глобальная экономическая система понятна и не вызывает серьезных расхождений взглядов в научной среде, региональное измерение, на наш взгляд, требует уточнения в части понятия международного региона. Для большинства стран именно региональный контекст является наиболее актуальным, в этом контексте, представляется верным утверждение авторов теории регионального комплекса безопасности, что международные отношения в целом должны рассматриваться в первую очередь с позиций международных регионов [13]. Под ними поднимется группа государств, чьи интересы в области безопасности настолько тесно переплетены, что не могут быть вычленены и рассмотрены по отдельности [13]. Считаем, что та же логика может быть применена и для региональных экономических систем.

В то же время, рассматривая понятие международного региона с позиций экономических интересов конкретного национального государства, следует отметить целесообразность включения в него других стран, прежде всего, в контексте реализации своего императива развития. В русле такой интерпретации, более правильным названием экономического региона с позиций интересов национального государства была бы зона его приоритетных внешнеэкономических интересов (далее, зона ПВИ). Таким образом, зона ПВИ государства включает наиболее важные для него страны с точки зрения реализации задач по максимизации своего долговременного экономического роста, обеспечению внутренней экономической связанности и национального экономического суверенитета. В соответствии с

гравитационной моделью, эта зона будет иметь в основе фактор географической близости, вместе с тем может включать и отдаленные страны без активного экономического взаимодействия, которые, однако, обладают инструментами экономического влияния на данное государство через международные экономические организации либо значимых экономических партнеров. Важной проблемой в этом контексте является выявление критериев разграничения, которые бы позволяли включить страну – экономического партнера в зону ПВИ. Решение этой задачи еще предстоит, однако общий подход мог бы основываться на анализе ее процентной доле в экспорте, финансовых и информационных потоках, ином внешнеэкономическом взаимодействии национального государства, способствующем долговременному экономическому росту.

Участие национального государства в международных экономических отношениях существенным образом влияет на процесс обеспечения его экономической безопасности.

Так, открытие национальной экономики для взаимодействия с зарубежьем и ее интеграции в более крупную экономическую систему, с доступом к новым рынкам труда, земли, капитала и полезным знаниям, позволяет преодолеть ограничения автаркии и содержат дополнительные возможности по обеспечению долговременного роста. Экономические теория и практика свидетельствуют об общей позитивной корреляции на мировом уровне между интенсификацией международных экономических связей и экономическим ростом. Среди основных позитивных динамических эффектов участия в международных экономических отношениях исторически рассматривались преодоление барьеров, накладываемых внутренним рынком и рост эффективности через улучшение производительности труда [26], откладывание снижение нормы прибыли [21], открытие новых рынков как условие для успеха инноваций [24; 25] и т.д. В настоящее время, все больше внимания уделяется международной торговле (и, особенно, экспортному сектору) как переменной, находящейся в основе этого феномена, позитивный эффект объясняется через лучшее распределение ресурсов (исходит из конкурентных преимуществ), более широкое использование производственных возможностей (исходит из эффекта масштаба), большую склонность к внедрению технологических улучшений (как ответ на более интенсивную конкуренцию) и большую занятость [10]. В то же время, международная торговля способствует распространению полезных знаний, открытые экономики пользуются более широким к ним доступом, что поощряет креативность, инновации и использование эффекта масштаба [23]. Участие в международном обмене способствует росту и через поощрение накопления физического и человеческого капитала, а также, рост производства для фиксированных уровней капитала [15]. Также, была установлена сильная позитивная корреляция между ритмами экономического роста и долей инвестиций в ВВП, а также, между долей инвестиций в ВВП и корреляцией международной торговли и ВВП [19]. Еще одним позитивным фактором является импорт капитальных товаров, как способ внедрения современных технологий [22; 18].

Открытие экономики для взаимодействия с внешним миром обуславливает появление новых переменных с неоднородными эффектами. В процессе ребалансировки экономики в результате ее включения в более обширную систему, эти изменения касаются, как правило, всех групп детерминант экономического роста через призму открытости экономики перед международными потоками трудовых и природных ресурсов, капитала, полезных знаний и технологий; влияния кредитных циклов других государств; географического расположения по отношению к важным

внешним центрам факторов производства и рынкам; международной политической конъюнктуры; социально-культурных факторов. Вместе с тем, участие в международном экономическом обмене неизбежно порождает конкуренцию с другими актёрами и может приводить к нелояльной конкуренции и политическим конфликтам.

Участие государства в международном экономическом взаимодействии придает новое качество и задаче обеспечения других национальных интересов в области НЭБ – внутренней экономической связанности и экономического суверенитета.

Так, экономический сепаратизм проявляется в завязывании экономики региона страны больше на внешнюю среду, чем на национальную экономику, либо на внешних партнеров, отличных от приоритетных для национального государства в целом. На социально-экономическом же уровне, пониженные стандарты жизни населения и воспринимаемой социальной справедливости в сравнении с другими странами неизбежно будет приводить к неудовлетворённости населения и росту угроз, связанных с внутренней социально-политической дестабилизацией. То есть, значительное опережающее развитие соседних стран в этой области представляет стратегический вызов для безопасности государства. В этом смысле, конкуренция между государствами (в т.ч., за привлечение талантов, инвестиций и т.д.) на нынешнем этапе все чаще принимает форму соревнования в различных аспектах уровня развития в сравнении с другими странами региона.

Обеспечение национального экономического суверенитета в условиях участия в международных отношениях принимает особое значение и состоит в контроле национального государства над своей экономической системой, без вмешательства со стороны внешних сил (других государств, международных актёров, иностранных компаний и т.д.) Международные экономические системы можно рассматривать как систему элементов трех категорий: производственных комплексов, рынков потребления, а также транспортной, финансовой и иной инфраструктуры, их соединяющей, при этом часть данной системы находится за пределами национального государства, вне его юрисдикции и пределов национального суверенитета. В данной ситуации, соответственно, задача полного обеспечения национального суверенитета априори не может быть достигнута без нарушения суверенитета других участников международной экономической системы и можно говорить о максимально возможном суверенитете.

Исходя из вышеизложенного, можно сформулировать следующее определение НВЭБ: **национальная внешнеэкономическая безопасность – это защищенное состояние экономической системы национального государства от внешнего деструктивного влияния на ее способность удовлетворять материальные потребности гражданина, нации и государства, выраженное в максимизации долговременного экономического роста, обеспечении национальных внутренней экономической связанности и экономического суверенитета.**

Таким образом, **предметом исследования** научной дисциплины национальной внешнеэкономической безопасности является выявление, изучение и пресечение внешних деструктивных воздействий на национальную экономическую систему.

ВЫВОДЫ

Исходя из вышеизложенного, можно сформулировать следующие основные выводы:

1) концепт НВЭБ строится на базовых элементах общей теории национальной экономической безопасности и, следовательно, разделяет ее основные проблемы;

2) разрешение этих проблем видится в концептуальной конструкции, которая бы верно сочетала его политологические и экономические компоненты, где архитектура общей модели оценки безопасности выражалась бы в терминах теории безопасности, а ее наполнение было бы преимущественно экономическим;

3) в рамках предлагаемого подхода, НЭБ – это защищенное состояние национальной экономической системы от деструктивного влияния на ее способность удовлетворения материальных потребностей гражданина, нации и государства, выраженное в обеспечении максимального долговременного экономического роста, внутренней экономической связанности государства и национального экономического суверенитета;

4) предмет дисциплины НЭБ составляет всестороннее исследование негативных шоков для национальной экономической системы, их причин, природы и влияния на ее способность обеспечивать удовлетворение материальных потребностей гражданина, нации и государства, а также, изучение методов защиты и противодействия этим шокам;

5) специфика концепта НВЭБ в общей теории НЭБ заключается в существовании фактора внешней среды, который предлагается трактовать в первую очередь как международного региона, определяемого с позиций экономических интересов конкретного национального государства как зона его приоритетных внешнеэкономических интересов;

6) в русле излагаемых идей, НВЭБ – это защищенное состояние экономической системы национального государства от внешнего деструктивного влияния на ее способность удовлетворять материальные потребности гражданина, нации и государства, выраженное в максимизации долговременного экономического роста, обеспечении национальных внутренней экономической связанности и экономического суверенитета;

7) предметом исследования научной дисциплины НВЭБ является выявление, изучение и пресечение внешних деструктивных воздействий на национальную экономическую систему.

БИБЛИОГРАФИЯ

1. Белоус, А. Г. (2001). Глобализация и безопасность развития: монография / А. Г. Белорус, Д. Г. Лукьяненко. – Киев: КНЭУ. – 733 с.
2. Илларионов, А. И. (1998). „Критерии экономической безопасности.” // *Вопросы экономики*, № 10; 35-58.
3. Киртоагэ, Р.Н. (2019) Взгляд на концепт национальной безопасности через призму связки „безопасность-развитие”. *Труд. Профсоюзы. Общество.* № 2 (64); 84-90.
4. Марченкова, Л.М., Ильюхина, И.Б. (2015). Проблемы внешнеэкономической безопасности России в условиях глобализации мировой экономики. *Евразийский юридический журнал,* №6 (85).

5. Савон, И.В., Мамонтова, Ю.П. (2016). Состояние внешнеэкономической безопасности России и направления ее обеспечения в современных условиях. *Ростовский научный журнал,* № 12, 130 – 145.
6. Феофилова, Т.Ю. (2009) Проблемы теории экономической безопасности. *Проблемы современной экономики,* №5, 103 – 106.
7. Фокин, Н.И. (2016). Внешнеэкономическая безопасность: понятия, опыт, проблемы. Научно – практический семинар „Экономическая безопасность АТР и будущее России". *Информационно – аналитический бюллетень ИИАЭ ДВО РАН,* № 18, 10-20.
8. Шаламов, А. В. (2007). Внешнеэкономическая безопасность национальной экономики в условиях глобализации// *Глобальные и региональные проблемы современности: истоки и перспективы: материалы научной конференции молодых ученых*, Екатеринбург, Вып. 2.: Изд-во Урал. ун-та, 122-125.
9. Шараев, Ю.В. (2006). Теория экономического роста. Москва: ГУ ВШЭ.
10. Afonso, O. (2001). The Impact of International Trade on Economic Growth. FEP Working Papers, Porto University, 2001. Доступно на http://wps.fep.up.pt/wps/wp106.pdf.
11. Buzan, B. (1983). People, States and Fear: The National Security Problem in International Relations. Brighton, Sussex: Wheatsheaf Books.
12. Buzan, B., Wæver, O., Wilde, J. (1998). Security: A New Framework for Analysis. Boulder: Lynne Rienner Publishers.
13. Buzan, B., Wæver, O. (2003). Regions and Powers: The Structure of International Security. Cambridge University Press.
14. Chirtoagă, R. (2017). Impactul factorului amplasării geografice asupra creșterii economice a țărilor Europei de Est după dizolvarea sistemului sovietic. Revista / Journal „Economica", nr.4 (102), 41-51.
15. Frankel, J., Romer, D. (1999). Does Trade Cause Growth? In: *American Economic Review*, vol. 89, no 3, June, 379-399.
16. Kirshner, J. (1997). The microfoundations of economic sanctions. In: *Security Studies*, No. 6, 1997, 32–64.
17. Krasner, S. D. (1976). State Power and The Structure of International Trade. In: *World Politics*, Volume 28, Issue 3, April, 317-347.
18. Lee, J. (1995). Capital goods imports and long-run growth. In: *Journal of Development Economics*, vol. 48, 91-110.
19. Levine, R., Renelt, D. (1992). A Sensitivity Analysis of Cross-Country Growth Regressions. In: *The American Economic Review*, Vol. 82, No. 4. (Sep.), 942-963.
20. List, F. (1909). The National System of Political Economy. London, New-York, Bombay, and Calcutta: Longmans, Green, and Co. Доступно на https://oll.libertyfund.org/titles/list-the-national-system-of-political-economy.
21. Ricardo, D. (1817). The principles of political economy and taxation. Oxford University Press, February 2015.
22. Rodrik, D. (1994). Getting interventions right: how South Korea and Taiwan grew rich. NBER Working Paper no. 4964, December. Доступно на https://www.nber.org/papers/ w4964.pdf.
23. Romer, P. (1990) Romer P. Endogenous Technical Change // Journal of Political Economy. 1990. Vol. 98. N 5. 71—102.
24. Schumpeter, J. (1912). The Theory of Economic Development – Translated by R. Opie, 1934, Cambridge, 2008.

25. Schumpeter, J. (1942). Capitalism, Socialism, and Democracy. New York: Harper & Bros, 1994.
26. Smith, A. (1776). An inquiry into the nature and causes of the wealth of nations. Oxford University Press, 1976.
27. Solow, R. (1956). A contribution to the theory of economic growth. In: *Quarterly Journal of Economics*, 70, February, 65-94.
28. Solow, R. (1957). Technical progress and aggregate production function, In: *Review of Economic Studies*, vol. 39, 312-320.
29. Swan, T. W. (1956) Economic Growth and Capital Accumulation. In: *Economic Record*, 32, 334-361.

Economic Security at the Business Level

THE CONCEPT OF REORGANIZATION OF THE AGRICULTURAL EDUCATION AND RESEARCH SYSTEM IN THE REPUBLIC OF MOLDOVA ON THE DEVELOPMENT OF OCCUPATIONAL AND QUALIFICATION STANDARDS FOR SPECIALTIES IN THE FIELD OF AGROBUSINESS

CONCEPTUL DE REORGANIZARE A SISTEMULUI DE EDUCAȚIE ȘI CERCETARE CU PROFIL AGRAR DIN REPUBLICA MOLDOVA SUB ASPECTUL ELABORĂRII STANDARDELOR OCUPAȚIONALE ȘI DE CALIFICARE PENTRU SPECIALITĂȚILE DIN DOMENIUL AGROBUSINESSULUI

Cimpoieș Dragoș
Doctor habilitat în economie, profesor universitar
Universitatea Agrară de Stat din Moldova
e-mail: dcimpoies@gmail.com

Racul Anatol
Doctor în științe economice, conferențiar universitar
Universitatea Agrară de Stat din Moldova
e-mail: anatol.racul@gmail.com

Reșitca Rodica
Șef Serviciu știință, educație și extensiune rurală MADRM
e-mail: rodica.reshitca@madrm.gov.md

Abstract
Scopul lucrării constă în evaluarea adecvată a performanței academice a cercetătorilor din cadrul organizațiilor din sfera științei și inovării cu profil agronomic prin intermediul metodologiei neparametrice de analiză a anvelopării datelor. În rezultatul determinării ratingului performanței academice în opțiunea revenirii variabilei la scară este posibil de a determina resursele de îmbunătățire a activității personalului institutelor de cercetare cu profil agronomic prin calcularea funcției distanță pentru fiecare factor cauzal. Este prezentată implementarea aplicației soft de evaluare neparametrică care dă posibilitate de a face o analiză comparativă a performanței academice la toate nivelurile ierarhice a institutelor cu profil agrar în Republica Moldova.

Cuvinte cheie: *performanță academică, DEA, institute de cercetare, sectorul agrar*

Clasificator JEL: *A20, A23, I23*

INTRODUCERE

Întreprinderile din sectorul agrar al Republicii Moldova reprezintă sursa de bază în promovarea industriei alimentare și creează trendul de bază în creșterea economiei agricole pentru asigurarea sustenabilității pilonului unu a politicii comunitare agricole în dezvoltarea spațiului rural. Resursa primordială care asigură stabilitatea dezvoltării economice este echilibrul între componentele de bază a spațiului rural prin promovarea aspectelor sociale, procesarea produselor agricole cu un grad înalt de valoare adăugată și comercializarea logistic definită a rezultatelor activității sectorului agrar prin crearea unui personal educat atât în afaceri, cât și în agricultură. Aceasta impune ca studenții în managementul afacerilor agricole, angajați în companiile specializate în inginerie, sisteme

biologice, biotehnologie, tehnologie agroalimentară, știință alimentară, marketing alimentar și personalul de conducere să fie dotați cu cunoștințe adecvate obiectivelor impuse de realizarea integrării în Uniunea Europeană [3].

Sectorul agricol este din ce în ce mai mult o sursă de materii prime pentru sectoarele din afara sistemului alimentar tradițional și a textilelor. Produsele agricole sunt utilizate pentru producerea de biocombustibili, produse industriale, cum ar fi polimeri și substanțe chimice și fibre sintetice obținute pe bază de biotehnologie, precum și produse farmaceutice / de sănătate, cum ar fi alimente funcționale, hormoni de creștere și transplanturi de organe și crearea de noi provocări strategice și competitive pentru firmele din sectorul agroalimentar și aceasta va avea implicații profunde pentru acestea structura și operațiunile lanțurilor de aprovizionare din industrie.

Organizațiile agricole sunt din ce în ce mai flexibile și mai complexe, mai descentralizate și totuși depind de acțiunea colectivă și coeziune. Acest lucru reprezintă provocări pentru managerii care proiectează sisteme de stimulare și instituții interne care sunt fundamentul structurii, strategiei și guvernării intra-firme. În acelasi timp, schimbările tehnologice și apariția noilor provocări globale, impun tensiunile de localizare și vor stimula schimbările în relațiile socio-economice, remodelarea economiilor de amploare și de scară, creșterea riscurilor, vor introduce interdependențe noi și noi, vor naște pentru noii rivali și potențiali parteneri și modelează mai multe forme de organizare hibride. Acest lucru va complica coordonarea între firme pentru managerii agroalimentari și factorii de decizie a spațiului rural.

Provocările mileniului sub aspect ecologic, trendul schimbărilor climaterice și limitarea resurselor naturale cu o penurie de specialiști în domeniul agrobusinessului impune o restructurare a spațiului rural prin definirea criteriilor de optimizare a performanței economice a fermierilor. Acest concept ar putea declanșa o reevaluare imprevizibilă, radicală a sistemului alimentar și modifică ratingul de poziționare strategică pentru firmele agro-comerciale. Înțelegerea și anticiparea dinamicii modelului macroeconomic agro-comercial global va fi din ce în ce mai critic. Aceste provocări împreună cu progresele în abordarea teoretică, instrumentele de diagnostic și tehnicile empirice pentru abordarea lor, vor permite savanților din domeniul agrobusinessului o ofertă vastă de probleme, abordări și motive pentru a îmbunătăți și a extinde ancheta într-un sistem alimentar global complex și tot mai important. Ele ne vor oferi, de asemenea, noi oportunități de a ajuta studenții, managerii și factorii de decizie prin intermediul programelor de predare și dezvoltare a agrobusinesslui. Economia care este ghidată pe baza conceptelor echilibrului componentelor spațiului rural necesită implicarea specialiștilor din managementul în agribusinessului și administrării rurale pentru a asigura soluțiile optimale în promovarea economiei de piață [5].

Analiza economică a proceselor complexe care definesc evoluția spațiului rural impune o abordare aplicativă a informației primare din teritoriu. Unitățile economie agricole au specificul utilizării în calitate de obiectiv componentele sectorului vegetal și zootehnic care impun tehnologii agricole în care funcția scop nu este numai profitul sau indicatorii economici de performanță pe piață dar și componenta socială a vieții rurale precum și abordările ecologice indispensabile activității economice, care include întrebările referitoare la îmbinarea armonioasă a fluxurilor de resurse și a rezultatelor activității agricole și care are ca scop elucidarea profilului intelectual, social și a cunoștințelor de specialitate în domeniul managementului în agrobusiness și administrarea rurală este o replică a criteriilor de dezvoltare durabilă în sectorul agrar al Republicii Moldova. Primordial informația primară în chestionar se referă la caracteristicile întreprinderilor agricole, capacitatea de a presta activitatea în domeniul agrar cu o evaluare a performanței

încadrării în economia de piață autohtonă și datele cu caracter social a personalului inclus în activitatea economică. O radiografie complexă a informațiilor incluse în cadrul chestionarului referitoare la aspectul demografic presupune gruparea respondenților conform criteriilor de angajare în unitățile economice agricole pe specialități și după prestarea preponderentă a serviciilor în spațiul rural. Evident că profilul educațional a specialiștilor care a apărut odată cu semnarea acordului de integrare în Uniunea Europeană (management, marketing ș.a.) poate fi echivalat cu profilurile antecedente obținerii independenței a Republicii Moldova și formează o structură amplă a personalului încadrat în activitatea economică. Sunt indicate în chestionar și posibilitățile de reprofilare a specialiștilor cu un șablon profesional moral depășit prin încadrarea în structurile educaționale a Agenției Naționale pentru ocuparea forței de muncă, posibilitatea studiului aprofundat în cadrul Instituțiilor de învățământ profesional tehnic (ȘP, colegii, centre excelență) sau prin subdiviziunile care asigură extensiunea universităților cu profil agronomic. În chestionarul utilizat pentru obținerea informației primare din unitățile economice cu profil agrar sunt indicate suporturile educaționale pentru reprofilare și reciclare a personalului Universității Tehnice din Moldova și a Universității Agrare de Stat din Moldova. Un compartiment aparte în colectarea informației îl are definirea raportului între cunoștințele cu aspect fundamental în comparație cu efortul educațional pentru cunoștințele de specialitate și numărul de ore de studiu necesare pentru componenta de orientare socio-umanistă. Datele primare colectate arată o afinitate statistic veritabilă față de componenta fundamentală în studiu și toți respondenții atestă că aceste cunoștințe sunt de lungă durată și formează profilul intelectual a specialistului ca factor de decizie. Însă cunoștințele aplicative reprezintă un atu pentru persoanele care sunt orientate să susțină un interviu de angajare la lucru și pe termen scurt acest compartiment al planului de învățământ este solicitat preferențial de studenți. Prezentarea în cadrul chestionarului a disciplinelor solicitate de factorii de decizie în unitățile economice agricole cu scara nominală Likert presupune o abordare econometrică a funcției logistice pentru evaluarea probabilității maximale de solicitare a cunoștințelor în domeniu [9].

METODOLOGIA CERCETĂRII

Cercetarea în Managementul agrobusiness-ului presupune o abordare teoretică a conceptului educațional care are la bază modelarea econometrică a proceselor economice în instituțiile de învățământ superior și cercetare cu profil agrar din Republica Moldova. Elaborarea chestionarului referitor la datele primare în sectorul agrar impune necesitatea definirii criteriilor de optimizare a procesului educațional în baza unor indicatori economici și a obiectivelor învațământului agrar. În rezultatul cercetării a fost definită funcția distanță în calitate de măsură invariantă a performanței academice care reflectă amplu componenta economică a procesului educațional în sectorul agrar și aspectul social ca obiectiv major a instituțiilor de învățământ superior și cercetare în domeniu. Metodologia evaluării funcției distanță care se bazează pe programarea liniară a datelor primare care reflectă componenta aplicativă a managementului în agrobusiness din unitățile economice presupune analiza anvelopării datelor conform scării multinominale Likert. Definirea funcției distanță dă posibilitate de a calcula ratingul componentelor disciplinelor în cadrul programelor analitice și permite evaluarea performanței academice alocative și tehnice. În baza rezultatelor obținute din prelucrarea datelor primare a chestionarului unităților economice a fost structurat profilul ocupațional a specialiștilor în business și administrare care stă la baza elaborării noului plan de învățământ pentru specialitatea economică „Management în agrobusiness și administrare rurală”. În cadrul metodologiei neparametrice de evaluare a ratingului componentelor profilului ocupațional

instrumentarul statistic de analiză a componentelor principale reprezintă un rezultat substanțial care dă posibilitate de a evalua vectorii proprii a setului primar de date conform chestionarului elaborat și are ca obiectiv diminuarea numărului variabilelor exogene. În așa mod abordarea aplicativă a funcției distanță dă posibilitate de a atribui un rating numeric disciplinelor și lecțiilor practice cu o pondere majoră în solicitarea pe piața muncii în business și administrare. Profilul educațional ce ține de management în agrobusiness presupune o viziune integrată a sectorului agrar prin includerea componentei agroalimentare, care se definește de la cercetarea și furnizarea de resurse, până la producție, prelucrare și distribuție la magazinele de vânzare cu amănuntul și deservirea consumatorilor [2].

Argumentarea metodologică a criteriului de evaluare a performanței academice a studenților specialității ”Management în agrobusiness și dezvoltare rurală” are la bază măsura radială a eficienței în care inputurile $x = (x_1, x_2, \dots, x_M)$ generează factori rezultativi y care se includ în modelul econometric în calitate de coeficienți a productivității parțiale.

$$\xi_i = \frac{x_i}{y}, 1 \le i \le M. \quad (1)$$

În așa mod funcția exponențială de performanță academică reprezintă frontiera eficientă în cadrul procesului educațional:

$$y^k = f^k(y^k\xi), \quad 1 \le i \le K. \quad (2)$$

Măsura invariantă care dă posibilitate de a evalua ratingul componentelor disciplinelor în cadrul programelor analitice este alcătuită din performanța academică alocativă (reprezintă raportul între efortul mediu de studiu la outputul optimal corespunzător) și tehnică (care arată cu cât trebuie să majorăm valoarea outputului față de resursele educaționale utilizate).

$$Eff = \left\{\xi = (\xi_1, \xi_2, \dots, \xi_M) | \xi_i = \min_k \min_\mu \frac{\mu x_i^0}{f^k(\mu x_i^0)}, 1 \le k \le K\right\} \quad (3)$$

Contribuția metodologică a cercetării constă în definirea măsurii radiale a performanței academice și permite argumentarea ratingului cunoștințelor obținute în sistemul de învățământ superior în calitate de formator a aptitudinilor manageriale cu o pondere majoră în solicitarea pe piața forței de muncă în business și administrare. În urma analizei ofertelor educaționale din universitățile mai multor țări a fost determinată o specialitate nouă ”Management în agrobusiness și dezvoltare rurală”. În rezultatul evaluării activității sistemului de educație-cercetare cu profil agrar din Republica Moldova a fost definită abordarea econometrică pentru implementarea unei măsuri invariante de tipul de activitate în sectorul umanist al învățământului și științei care permite fundamentarea teoretică a suporturilor educaționale pentru studiu. Isocuanta graficului tehnologic definită prin intermediul unor transformări radiale ale inputurilor și outputurilor dă posibilitate de a evalua componentele ofertei educaționale din universitățile cu profil agrar în baza analizei anvelopării datelor conform scării multinominale Likert.

$$Isoq\ GR = \{(x, y) \in GR \text{ și } (\delta x, \delta^{-1} y) \notin GR \text{ pentru orice } 0 < \delta < 1\} \quad (4)$$

Elaborarea planului de învățământ pentru noua specialitate economică „Management în agrobusiness și dezvoltarea rurală" presupune utilizarea analizei componentelor principale pentru datele primare obținute în rezultatul chestionării unităților economice cu profil agrar și indicarea vectorilor proprii a disciplinelor și lecțiilor practice cu o pondere majoră în solicitarea pe piața forței de muncă în business și administrare. Valoarea teoretică și aplicativă a cercetării constă în fundamentarea ratingului cunoștințelor obținute în sistemul de învățământ superior agrar și în conformitate cu isocuanta graficului tehnologic definește componentele capacitative din sistemul de aptitudini manageriale cu o solicitare majoră de către agenții economici [6].

REZULTATE ȘI DISCUȚII

Obiectivul cercetării constă în elaborarea planului de învățământ pentru noua specialitate economică cu profil agrar "Management în agrobusiness și dezvoltare rurală" pentru instituțiile de învățământ superior. Abordarea teoretică pentru definirea noțiunii de disciplină de studii în cadrul Managementului afacerilor agricole presupune elucidarea componentelor de bază a spațiului rural și evaluarea contribuției aspectului economic a sectorului agrar prin metode parametrice pentru fundamentarea conținutului cunoștințelor necesare studenților din domeniul de formare profesională 0413 Business și administrare la specialitatea „Management în agrobusiness și administrarea rurală". Economia agrară reprezintă un domeniu în care implementarea legilor teoriei economice prin optimizarea tehnologiei producției și a distribuției produselor agroalimentare presupune definirea corelațiilor între componentele spațiului rural care reprezintă obiectul de studiu la specialitatea nominalizată și criteriile de evaluare a performanței economice prin intermediul indicatorilor de eficiență, productivitate și competitivitate. Cunoștințele necesare specialiștilor în sectorul agrar impune o aplicare a performanței într-o varietate largă de domenii aplicative cu o suprapunere considerabilă în economia convențională. Economia agrară presupune contribuții substanțiale de resurse informaționale, abordări logice și fundamentarea teoretică în dezvoltarea durabilă a spațiului rural, economia de mediu, economia industrială și agroalimentară cu aspecte metodologice în promovarea politicii agricole comunitare de vecinătate cu Uniunea Europeană. În perioada clasică a abordării economice managementul în agrobusiness și administrarea rurală a fost definit ca studiu a alocării resurselor și asigurarea echilibrelor macroeconomice în spațiul rural. Evoluția progresului tehnic, utilizarea metodelor chimice în optimizarea tehnologiilor agricole și promovarea principiilor democratice în organizarea socială a dezvoltării durabile în sectorul agrar au ca rezultat o clasă nouă de angajați în domeniu care asigură competitivitatea unităților economice agricole pe piața autohtonă prin intermediul tehnicilor de inginerie financiară și promovează exportul produselor agroalimentare prin optimizarea structurii organizatorice a producției agricole.

Conform abordărilor teoretice, a savantului decernat cu premiul Nobel pentru economie din 1979 Theodore Schultz, dezvoltarea durabilă a spațiului rural Euroatlantic este esențial asigurată prin implementarea în practica agricolă a metodologiei optimizate a managementului în agrobusiness. Prin consecință a fost definită structural și funcțional care poate fi profilul intelectual a specialiștilor ce asigură implementarea abordărilor conceptuale și realizarea practică a domeniilor aplicative. Componenta cunoștințelor care se referă la abordarea matematică a modelelor econometrice în economia rurală a fost definită la nivelul studiilor de bacalaureat, iar cunoștințele în sfera tehnologiilor informaționale presupune performanță în limbajele de programare de nivel înalt cu implementarea sistemelor informaționale și digitalizarea agriculturii. Planul de învățământ propus se încadrează logic la compartimentul nominalizat cu profilul educațional în

Washington State University la specializarea Agricultural and Food Business Economics pentru anul de studii 2018 atât referitor la volumul de ore rezervat și numărul de credite atribuite cursului. Metodele cantitative și calitative de analiză a datelor primare în activitatea agenților economici presupune dotarea cu pachete de programe aplicative care sunt oferite gratis pe perioada studiului disciplinei de către Biblioteca Republicană Științifică Agricolă [8].

Profilul educațional în agrobusiness presupune o viziune integrată a sectorului agrar prin includerea componentei agroalimentare, care se definește de la cercetarea și furnizarea de resurse, până la producție, prelucrare și distribuție la magazinele de vânzare cu amănuntul și deservirea consumatorilor. Elaborarea planului de învățământ Management în agrobusiness și administrarea rurală are ca scop elucidarea structurii cunoștințelor în domeniu prin abordarea economiei marketingului și managementului cooperatist, proiectarea și dezvoltarea instituțiilor de piață de credit, proiectarea organizațională, structura pieței și analiza performanței, gestionarea și proiectarea lanțului de aprovizionare, optimizarea eficienței operaționale, dezvoltarea datelor și analizei pentru managementul financiar, managementul strategic și educația în domeniul agroindustrial.

Cercetarea în Managementul agrobusinessului și administrării rurale impune necesitatea definirii noțiunilor de bază a componentelor naturale, ecologice și sociale a spațiului rural sub aspectul penuriei resurselor pentru a asigura o dezvoltare durabilă. Cunoștințele referitoare resursele naturale și biologice, disponibilitatea de terenuri agricole și produse minerale utilizate în tehnologiile rurale reprezintă limitele modelului economic marginal pentru o dezvoltare exponențială. Calitatea acestor resurse naturale în Republica Moldova diferă foarte mult de la o regiune la alta. Unele terenuri sunt incapabile să crească ceva în starea lor naturală, iar altele sunt extrem de fertile. În ultimii ani, societatea a devenit conștientă și de deficiența din ce în ce mai mare de apă potabilă, în timp ce resursele naturale legate de energie au reprezentat resurse critice deficitare în ultimele decenii. În plus față de resursele naturale, resursele limită includ și resurse biologice, cum ar fi animale, animale sălbatice și diferite soiuri genetice de culturi [4].

Resursele umane reprezintă o limită în restructurarea spațiului rural pentru a asigura soluții optimale în procedurile tehnologice și promovarea pe piață a producției agroalimentare. Fermierii asigură o gestiune sustenabilă a resurselor naturale și include tot spectrul de performanță în sectorul agrar de la agricultura de subzistență până la tehnologiile intensive în spațiul rural. Forța de muncă fiind o componentă de bază în economia de piață limitează oferta prin abordări specifice a Managementului în agrobusiness și administrarea rurală atât sub aspect financiar cât și prin promovarea politicilor comunitare agricole. Muncitorii în sectorul agrar furnizează forța de muncă pentru producerea de culturi agricole și animale. Forța de muncă este considerată scăzută chiar și atunci când forța de muncă din țară nu este angajată pe deplin. Muncitorii agricoli furnizează servicii ca răspuns la rata salariilor în curs. Este posibil ca agenții economici să nu poată angaja toate serviciile de muncă pe care le doresc la salariul pe care doresc să îl plătească. Managementul reprezintă o altă formă de resurse umane care oferă servicii antreprenoriale și care pot implica formarea unei noi firme, renovarea ei sau extinderea unei firme existente prin asumarea riscurilor financiare și supravegherea utilizării resurselor existente ale firmei, astfel încât obiectivele acesteia să poată fi îndeplinite. Fără Managementul de antreprenoriat, agribusiness-urile la scară largă ar înceta să funcționeze eficient.

Managementul în agrobusiness și administrarea rurală are ca obiectiv promovarea deciziilor în cadrul unităților economice agricole și de procesare agroalimentară. Această abordare conceptuală include patru sectoare în care specialiștii manageri au contribuții

semnificative la elucidarea și susținerea deciziilor operaționale, financiare și strategice în firmele din sectorul agroalimentar. Managerii în agribusiness și administrarea rurală sunt dotați cu cunoștințe pentru crearea metodologiei și instrumente robuste care asigură eficiența economică a proceselor tehnologice în sectorul agroalimentar.

Conform ofertei educaționale a Michigan State University în cadrul oficiului Departament of Agricultural, Food and Resource Econoimcs repartizarea creditelor transferabile și orelor de studiu pentru disciplinele de specialitate care se referă la „Bazele managementului", „Managementul producției animaliere", „Managementul producției horticole" și „Economia dezvoltării rurale" se poate afirma că cunoștințele de specialitate reflectă obiectiv necesitățile de organizare și planificare a producției agricole conform cerințelor standardului de acreditare a învățământului superior Bachelor of Science Degree a Statelor Unite ale Americii. Analiza comparativă a planului de învățământ propus cu standardul susmenționat arată o rezervare a resurselor de ore și credite mai favorabilă pentru oferta educațională a managerilor în agribusiness și administrarea rurală din Universitatea Agrară de Stat din Moldova. Transformarea mărfurilor agricole în produse alimentare necesită în mod obișnuit conversia unor cantități mari de materiale cu valoare mai mică în produse și transport mai valoroase (de inputuri agricole și de produse alimentare) pe distanțe considerabile. Pentru a rezolva această provocare economică, managerii trebuie să fie capabili să evalueze atât costurile alternative de producție în cadrul unei singure facilități de producție, cât și eficiența totală a costurilor localizării mai multor instalații într-o regiune. O provocare similară există în ceea ce privește proiectarea celui mai eficient sistem de producție și transport pentru a oferi contribuții la operațiunile de producție agricolă. Eficiența operațională sporită are ca rezultat un nivel mai ridicat de performanță pentru firmele din sectorul agroalimentar care îmbunătățește bunăstarea socială prin costuri alimentare mai mici și produse alimentare de calitate superioară. Abordarea tehnologică a proceselor economice s-a concentrat pe sinteza funcțiilor de costuri din surse de informații inginerești, biologice și alte informații utile, din date de contabilitate s-au pe baza relațiilor de intrare-ieșire la nivel de proces. Deși o instalație individuală de fabricare a alimentelor ar putea obține o eficiență internă excepțională, performanța economică generală a acelei unități poate fi afectată semnificativ de costurile obținerii de contribuții agricole și de distribuirea producției fabricii. În calitate de subunități firmele de producție agricolă pot avea mai multe procese tehnologice de producție și managerii în agribusiness și administrarea rurală trebuie să fie capabili de a optimiza sistemul [1].

O contribuție substanțială în structura planului de studii a managementului în agribusiness și administrarea rurală o are universitatea Wageningen din Olanda care propune un raport de repartizare optimală a creditelor și orelor de studii între disciplinele fundamentale și de specialitate. În cadrul planului de studiu propus pentru anul doi de studiu din totalul șaizeci de credite transferabile disciplinele de specialitate reprezintă 56% iar disciplinele fundamentale numai 13%, ce corelează cu oferta educațională a universității din Olanda. Tehnicile de evaluare a funcției de producție în cadrul unităților economice agricole cu definirea aferentă a indicatorilor economici de productivitate, eficiență și competitivitate care reflectă performanța promovării pe piață reprezintă o cotă parte semnificativă a disciplinelor în cadrul planului de studiu Management în agribusiness și administrarea rurală. Modelarea econometrică permite abordări manageriale pentru a minimaliza costurile combinate de asamblare și prelucrare a mărfurilor agricole. În esență, o extensie a modelului de transport liniar pe baza programării liniare include numărul de locații și locațiile ca variabile interne și a permis economiile la scară. Această abordare de bază a fost extinsă pentru a reflecta mai exact circumstanțele produselor agricole

alternative și dinamica reală a pieței. În cadrul Uniunii Europene tehnicile care au ca obiectiv studiul eficienței operaționale în sectorul agro-comercial sunt favorizate prin subvenționare de către factorii de decizie. Această creștere marcantă a productivității academice a fost rezultatul comun al forțelor care interacționează, cum ar fi schimbarea nevoilor de societate, avansuri în teorie și capacități de calcul și infuzia de finanțări federale care vizează marketingul agricol [7].

Programele educaționale în sfera agrobusinessului au creat un capital uman care contribuie substantial la creșterea productivității și eficienței sectorului agroalimentar a Republicii Moldova. Ofertă de studiu a universităților agrare în Uniunea Europeană au în calitate de punct forte specializarea Managementul în agribusiness și administrarea rurală cu o repartizare a accentului educational în în favoarea disciplinilor de specialitate (cota parte 70%) cu un suport substantial a disciplinilor fundamentale (cota parte 13%). Universitatea Agrară de Stat din Moldova cu oferta educațională a specializărilor economice propune Managementul în agribusiness și administrarea rurală cu o repartizare similară a creditelor transferabile și orelor de studiu. Disciplinile care se referă la managementul resurselor naturale și schimbări climaterice (S.03.O.20) și managementul riscurilor (F.03.O.21) sunt un criteriu de organizare ierarhică a cunoștințelor aplicative în organizarea și planificarea producției agricole. Importanța aplicativă a cunoștințelor în agribusiness este vizibil evidențiată pentru producătorii agricoli care formează oferta excesivă a unor produse agroalimentare și nu se încadrează în criteriile de optimizare a bursei agricole autohtone. Capacitățile de gestionare a informației online de pe piața produselor agricole determină performanța managementului unității economice și respectiv profitul care rezultă din decizii optimale sau pierderile nejustificate care se bazează pe lipsă de informație sau modele economice depășite moral și etnic.

CONCLUZII

A fost propusă spre implementare în instituțiile de învățământ superior cu profil agrar în Republica Moldova o nouă specialitate „Management în agrobusiness și dezvoltarea rurală" care conform anchetării agenților economci în spațiul rural reprezintă o pondere majoră a specialiștilor în business și administrare solicitați pe piața forței de mincă. Valoarea teoretică și aplicativă a cercetării constă în elaborarea metodologiei neparametrice de evaluare a funcției distanță care stă la baza calculării ratingului componentelor educaționale a planului de învățământ pentru specialitățile economice. Aplicarea metodei de analiză a anvelopării datelor pentru optimizarea ofertelor educaționale din universitățile cu profil agrar reprezintă aportul teoretic și aplicativ al cercetării pentru fundamentarea ratingului cunoștințelor obținute în sisteml de învățământ superior. Pentru realizarea acestor obiective a fost creat grupul de lucru pentru elaborarea profilului ocupațional, aprobat de către Comitetul Sectorial pentru Formare Profesională din Agricultură și Industria Alimentară, (CS AgroindVET), Hotărârea nr.12 din 10.06.2020. În baza rezultatelor Comisiei, CS AgroindVET a evaluat dosarul (notă de argument, profil, chestionare, aviz); aprobat profilul ocupațional „Manager în agrobusiness, Nivel 7 CNCRM" care a fost recomandat pentru elaborarea Standardului Ocupațional (Hotărârea nr.14 din 10.07.2020). Spre final, a fost propusă includerea în Clasificatorul Ocupațiilor din Republica Moldova actualizat a ocupației Manager în agrobusiness în grupa de bază 1311 Conducători de organizații din agricultură și silvicultură.

BIBLIOGRAFIE

1. Cimpoieș, D., Reșitca, R. Analiza comparativă a performanței academice în universitățile cu profil agronomic din România și Republica Moldova. In: Conferința științifică internațională „Paradigme moderne în dezvoltarea economiei naționale și mondiale". USM, Chișinău, 2020.
2. Coelli T. (2005). An introdoction to efficiency and productivity analysis. Second edition. New York: Springer Science Business Media, Inc.
3. Duguleană L., Duguleană C. (2015). Data Envelopment Analysis for the efficiency of Academic Departments. In: Bulletin of the Transilvania University of Braşov, Series V, Economic Sciences, vol. 8 (57), no. 2, 453-468.
4. Lissitsa A., Coelli T., Rao P. (2005). Agricultural Economics Education in Ukrainian Agricultural Universities: an efficiency analysis using Data envelopment analysis. In: The XI International Congress of European Association of Agricultural Economists. 1-17.
5. Prudnikova N. (2016). Topicality of Linguistic Competence and Performance Teaching at Higher Educational Institutions of the Russian Federation (on the Example of RANEPA). In: International journal of english linguistics. vol. 6, no. 2, 99-104.
6. Reșitca, R., Cimpoieș, D., Racul, A. Evaluation of the academic performance in the agricultural education and research institutions in the Republic of Moldova. In: Life sciences for sustainable development. Cluj-Napoca 2020. p 86-94.
7. Salah R. (2011). Assessment of academic departments efficiency using data envelopment analysis. Islamic University-Gaza (GAZA STRIP). In: Journal of industrial engineering and management. vol. 4, no. 2, 301-325.
8. Schultz T. Economic Growth and Agriculture. Ed. McGraw Hill. 1968. p.152.
9. Sîrbu A., Cimpoieș D. (2015). Asigurarea economiei agrare a Republicii Moldova cu cadre performante prin dezvoltarea învățământului superior agronomic. In: Culegeri de lucrări științifice a Universității Agrare de Stat din Moldova, vol. 43, 69-75.

THE ISSUE OF BANK SECURITY ON OPTIMIZING THE BUSINESS MODEL WITHIN THE BANK

PROBLEMATICA SECURITĂȚII BANCARE ASUPRA OPTIMIZĂRII MODELULUI DE AFACERI ÎN CADRUL BĂNCII

Gîrlea Mihail
Doctor în științe economice, conferențiar universitar
Universitatea de Stat a Moldovei
e-mail: mihaigirlea1982@gmail.com

Ștefaniuc Olga
Doctor în științe economice, conferențiar universitar
Universitatea de Stat a Moldovei
e-mail: olga.stefaniuc@mail.ru

Abstract
Since the inception of the financial crisis of 2007-2009, the banking sector in Europe has been undergoing fundamental changes. Following the major fallouts of large banking groups – in particular those with excessively risky business models combined with the trillions incurred in losses and subsequent taxpayer-funded government bailouts to keep the European banking sector afloat – a wave of re-regulation was undertaken to bring back eroded market confidence and to safeguard financial stability. This led to major restructuring and waves of deleveraging with fundamental implications for the future of the European banking sector and financial intermediation.
While the economic crisis has triggered policy responses to stimulate lending to the real economy while assuring the stability of the banking sector that provides breathing space in the short run, deep restructuring of many banking systems will be needed in the medium-term. In this changing context of evolving market structures and regulations, the banks' business models analysis can provide market participants, depositors, creditors, regulators and supervisors with a useful tool to better understand the nature of risk attached to each bank business model and its contribution to systemic risk throughout the economic cycle.

Keywords: *bank security, banking sector, systemic risk, financial stability, macroprudential tools, bank business model.*

JEL Classification: *E58, G01,G21*

INTRODUCERE

Secolul al XXI-lea reprezintă o perioadă caracterizată de schimbări continue în domeniul relaţiilor internaţionale, printre care diversificarea actorilor relaţiilor internaţionale, modificarea raporturilor dintre aceştia, schimbări la nivel de interese naţionale, precum şi modificări substanţiale în conjuncturile regionale de securitate, care, în ultimă instanţă, contribuie în mod nemijlocit la adoptarea de către actorii internaţionali a unui anumit comportament în raport cu ceilalţi. Factorii enumeraţi, precum şi o serie de alţi factori au contribuit la diversificarea condiţiilor de conducere a relaţiilor internaţionale şi de stabilire a raporturilor dintre actori, mai cu seamă în aspecte ce vizează subiecte de securitate. În contextul celor enunţate, merită a fi menţionat faptul că, în noile condiţii conturate pe arena internaţională, atenţia cercetătorilor a atras conceptul de securitate economică.

În acest sens, conceptul de securitate a cunoscut noi abordări, de această dată pe mai multe dimensiuni, cu recunoaşterea noilor tipuri de ameninţări în faţa cărora este plasată comunitatea internaţională per ansamblu, dar şi statele naţionale.

Într-o lume globalizată securitatea internaţională, dar şi cea naţională sunt reperele fundamentale prin care se manifestă principalele schimbări atât la nivel global, cât şi la nivelul fiecărui stat şi, respectiv, al fiecărei persoane. În această formulă, prezenţa unei economii performante şi competitive, stabile din punct de vedere macro-economic şi financiar, precum şi dinamice, reprezintă un factor important al politicii de securitate. Însăşi conceptul de securitate este definit cel mai des ca lipsa ameninţărilor, adică se interpretează drept o situaţie legată de starea fizică fie a unui sistem sau a unei naţiuni, sau a unui individ, unde lipseşte orice fel de ameninţare din partea factorilor exogeni si endogeni. Securitatea este abordata atât ca lipsa totală a unor ameninţări, cât şi ca păstrarea acestora la un nivel care nu poate influenţa securitatea propriu-zisă. [1]

Dicţionarul explicativ a limbii române dă o interpretare generală, cea mai cunoscută, de altfel, şi exactă pentru toată lumea, a definiţiei securităţii – „faptul de a fi la adăpost de orice pericol; sentiment de încredere şi linişte pe care îl dă cuiva absenţa oricărui pericol; protecţie, apărare”. [1]

Despre securitatea economică se vorbeşte destul de mult. Dar în urma analizei în domeniu putem observa că nu există o definiţie clară a conceptului de securitate economică, cu atât mai puţin una general acceptată. De exemplu, savantul rus Sencheacov B. propune definirea securităţii economice drept o stare a economiei şi a instituţiilor puterii de stat prin care se asigură protecţia garantată a intereselor naţionale, dezvoltarea social orientată a ţării în ansamblu, un potenţial suficient de apărare chiar şi în condiţii nefavorabile de dezvoltare a proceselor interne şi externe. Securitatea economică este interpretată ca o stare a sistemului sau o stare în care se află acest sistem. Astfel, securitatea economica a statului este definită ca o stare a economiei naţionale care permite asigurarea suveranităţii şi creşterii economice, ridicarea nivelului de trai al populaţiei în condiţiile intensificării relaţiilor economice internaţionale. De asemenea, securitatea economică este identificată cu capacitatea sistemului economic naţional de a asigura satisfacerea efectivă a nevoilor sociale atât la nivel naţional, cât şi la nivel internaţional. Cercetătorul român Pigui T. defineşte că, securitatea economică ar trebui înţeleasă ca fiind: un factor esenţial al securităţii naţionale şi anume acela care asigură resursele şi echilibrul dinamic al celorlalte componente ale acestui sistem (securitatea naţională); una dintre dimensiunile securităţii naţionale, regionale şi planetare, deziderat al fiecărui individ, comunitate umană, stat naţional etc.; obiectiv prioritar al guvernelor, al organizaţiilor regionale şi internaţionale care au ca menire asigurarea şi garantarea securităţii umane globale; stare a economiei naţionale văzută ca sursă şi fundament al eradicării sărăciei, foametei, inegalităţilor sociale şi economice atât între indivizi, cât şi diferite regiuni ale unor ţări. Iar savantul român Pop N. cataloghează securitatea economică drept un bun public. În una din prezentările sale, dr. Pop N. menţionează că, „pornim la drum de la definiţia şi obiectul ştiinţei economiei – gestionarea resurselor rare – şi menirea acestei gestiuni în societate în sensul ei cel mai larg: securitatea economică. Aceasta din urmă este cel mai convenabil exemplu clasic de bun public definit prin non-rivalitate în consum şi non-excludere pentru a-l produce. Statul nu poate fi decât arbitrul, toţi cetăţenii lui având acces la acest bun, toţi agenţii economici având şansa de a contribui la producerea lui.” [1]

Astfel securitatea economică reprezintă o parte componentă indispensabilă a securităţii naţionale. Astfel, acţiunile autorităţilor administraţiei publice centrale vor fi orientate spre crearea unor condiţii interne şi externe care să asigure independenţa economiei naţionale, o creştere economică durabilă, satisfacerea necesităţilor statului şi ale cetăţenilor, combaterea sărăciei, competitivitatea pe pieţele externe. În scopul consolidării sistemului financiar-bancar naţional, autorităţile relevante vor întreprinde, de asemenea, măsuri de sporire a rezistenţei sistemului dat faţă de crizele financiare şi economice

externe.

În acest sens, studierea şi abordarea conceptului de securitate economică a devenit o prioritate pentru statele naţionale, precum şi un domeniu de interes sporit pentru comunitatea de cercetători. Republica Moldova nu reprezintă o excepţie, mai cu seamă în condiţiile în care unul dintre cei doi vecini ai statului se confruntă cu un conflict militar în condiţii deosebite şi care comportă repercusiuni la nivel regional, dar şi internaţional.

Studierea şi fundamentarea conceptului de securitate economică nu este nici pe departe unul uşor, cu atât mai complicată este studierea fenomenului de securitate a unor state mici, care, aflându-se în fază de tranziţie la economia de piaţă încă nu şi-au trasat suficient de clar interesele economice interne şi externe. În Republica Moldova, ca şi în alte state în tranziţie, este bine dezvoltată crima organizată şi corupţia, organele publice nu sunt suficient de puternice sau sunt implicate direct în fărădelegile interne, şi din această cauză nu inspiră o încredere socială în capacitatea statului de a garanta respectarea "regulilor de joc". Drept urmare, în majoritatea acestor state o parte a activităţii economice trece în sectorul tenebru sau chiar criminal al sistemului economic Astfel, conform unui studiu economia neobservată a Republicii Moldova a atins dimensiuni de 30% din volumul economiei formale, aceste sectoare prin existenţa lor creează dificultăţi suplimentare în analiza fenomenului de securitate economică. Aceasta este doar una dintre cauzele care explică de ce barierele în calea înţelegerii importanţei securităţii economice sunt dublu dificile, atunci când obiectul securităţii este nu pur şi simplu un stat mic, ci şi un stat slab, debusolat şi dispersat în opinii. Iar în urma ultimelor evenimente atât pe plan mondial cât şi naţional tindem să credem că domeniul prioritar din cadrul sistemului de clasificare a securităţii naţionale este cel economicofinanciar. [1]

Pandemia Covid-19 a indus o criză economică globală profundă. Deși până acum băncile și-au arătat rezistența, parțial datorită reformelor majore de după criza din 2007-2009, criza le va pune sub stres. Mai mult, modelul bancar tradițional era deja contestat înainte de Covid de trei tendințe: *rate ale dobânzii persistent scăzute*, *reglementări sporite* și *concurență sporită din partea băncilor shadow* și *a operatorilor digitali*. Această coloană introduce cel de-al doilea raport din seria Viitorul băncilor de la IESE Business School și CEPR, care oferă o perspectivă asupra modului în care criza actuală și aceste tendințe vor forma viitorul sectorului bancar.

Lumea este martora unei crize economice mari şi sincronizate. Previziunile pentru 2020 sugerează o scădere a PIB-ului global de 6%, cu un număr record de țări în creștere la rate negative (OECD 2020). [2] Economiile avansate vor suferi o scădere mult mai mare a PIB-ului, de o dimensiune nemaivăzută de la Marea Depresiune. Fără îndoială, băncile vor fi supuse stresului, deoarece vor apărea insolvențe pe scară largă în rândul firmelor și ar putea urma un val de falimente în rândul gospodăriilor. În plus, în timp ce băncile au intrat în criză mai bine capitalizate și mai lichide, dimensiunea crizei le va tensiona probabil într-un grad mai mare decât cel prevăzut în multe teste de stres efectuate până acum (Banca Centrală Europeană 2020).[3]

La rîndul său şi Republica Moldova sa confruntat cu o serie de probleme economice în ultimii ani, inclusiv fuga de capital, deprecierea în unele perioade a monedei naționale. Unul dintre pașii care vizează realizarea, ratele de creștere stabile ale economiei naționale pe termen lung, este elaborarea proiectului strategiei securității naționale a Republicii Moldova.

PREZENTAREA PROBLEMEI ŞI FORMULAREA IPOTEZELOR

Securitatea reprezintă o stare atașată de esența unei bănci, o stare în care cele mai mici pericole ar trebui să poată fi anticipate. Odată cu dezvoltarea sistemului bancar,

securitatea și, implicit, politica de securitate s-a impus categoric în întreg sistemul bancar. În acest articol am încercat să ne expunem pe unele viziuni de îmbunătățire a tratării politicii de securitate a unei instituții bancare, incluzând și etapele necesare în vederea dezvoltării unei politici de securitate.

Problematica modelului de business al băncilor comerciale este una vastă, dat fiind complexitatea activităţii bancare, precum şi contextul economico-financiar actual, definit pentru băncile comerciale din Republica Moldova printre alţi factori care au influenţat criza economico-financiară mondială actuală, concomitent cu un proces de integrare bancară europeană. Din această perspectivă, sistemele complexe par uneori prea haotice pentru a mai putea recunoaşte în ele un tipar, fiind chiar dificil de a construi şabloane universal valabile, de a determina anumiţi factori şi de a stabili gradul de influenţă a acestor factori asupra sistemelor.

METODOLOGIA

Metodele de sistematizare și generalizare a conceptelor teoretice din acest domeniu au fost utilizate ca bază metodologică pentru investigarea posibilității de creștere a nivelului de securitate economică a sectorului bancar. Sinteza experienței străine a fost utilizată pentru a identifica cele mai prioritare, eficiente și utilizate pe scară largă metode în procesul de asigurare a securitatea economică a sectorului bancar.

PREMISELE LUCRĂRII

Crizele financiare au efecte negative de mare amploare asupra economiilor naţionale din ţările unde se produc; mai mult ca atât, datorită interdependenţelor crescânde, cauzate de procesul de globalizare, au chiar tendinţa de a contamina şi alte economii, afectând astfel securitatea financiară la nivel global. Din aceste considerente, eforturile autorităţilor naţionale de supraveghere bancară au fost suplimentate într-un mod tot mai pronunţat, în ultimii ani, de acţiuni de îmbunătăţire a cadrului de reglementare a activităţii bancare la nivel internaţional.

În cadrul dezvoltării relaţiilor de piaţă şi formării structurilor comerciale rolul principal îl deţin băncile comerciale. Anume ele acumulează fluxuri financiare mari şi sunt capabile să influenţeze activ asupra dezvoltării economiei naţionale. Băncile adesea sunt privite ca elita mediului de afaceri. Însă în acelaşi timp ele sunt supuse celui mai mare pericol, deoarece acolo unde sunt mulţi bani, întotdeauna se vor găsi persoane, care să dorească să „pună mâna pe ele”.

Ar fi greşit de afirmat, că problema securităţii băncii este „*durerea de cap*” doar a proprietarilor şi colaboratorilor ei, ci este şi problema clienţilor. Problemele băncilor ating interesele păturilor largi ale populaţiei şi sunt capabile în anumite condiţii chiar să influenţeze situaţia din ţară.

Crimele comise faţă de bancă şi lucrătorii bancari sunt din cele mai periculoase şi grele. Şi dacă timpurile când atentatele la viaţa bancherilor din diferite ţări nu erau considerate ca ieşite din comun, aceasta încă nu înseamnă lipsa oricărui pericol.

La momentul de faţă pericolul care ameninţă băncile este mult mai sofisticat, cu utilizarea celor mai proaspete inovaţii ale ştiinţei şi tehnicii. De aceea, trebuie de clarificat care este pericolul pentru bancă şi care sunt sursele lui, precum şi complexul de măsuri care trebuiesc întreprinse.

După cum cunoaștem, sectorul financiar, inclusiv infrastructura bancară mereu este cointeresată de către infractori cu scopul de a manipula datele cu caracter personal. Securitatea este definită drept protecția împotriva amenințărilor de securitate și este denumită „circumstanță, condiție sau eveniment cu potențialul de a provoca dificultăți economice pentru datele sau resursele de rețea sub formă de distrugere, dezvăluire,

modificare a datelor, refuz de serviciu. În prezent, în legătură cu evoluția tehnologică aspectul securității banacare a manifestat o evoluție continuă. În dependență de nivelul securității banca păstrează următoarele caracteristici reputația și competitivitatea. [4]

În cadrul acestei cercetări putem menționa că asigurarea durabilității fiecărei instituții de credit individuale este legată de stabilitatea sistemului economic național, iar durabilitatea sistemului economic este legată de stabilitatea băncilor din sectorul bancar. Firește, cu cât scara unei instituții de credit este mai mică, cu atât rezultatele activităților sale au un impact mai redus asupra stabilității unui nivel superior. Pe de altă parte, impactul durabilității sistemului economic național asupra activităților instituțiilor de credit la scară mică este mai mare decât cel al băncilor mai mari.

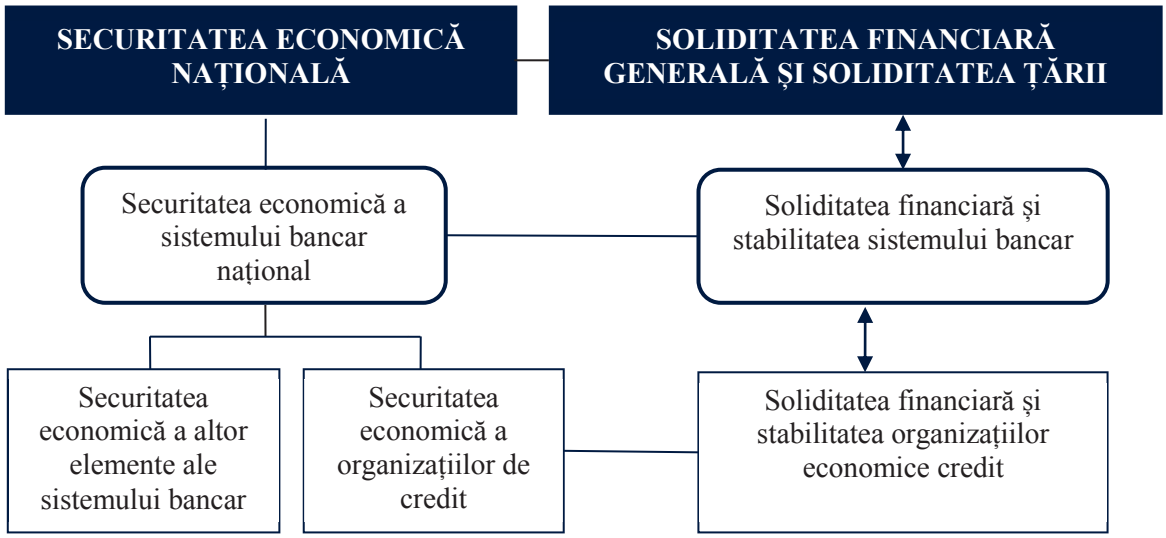


Figura 1. Raportul dintre securitatea economică și sustenabilitatea financiară la diferite niveluri

Sursa: [5]

Un principiu similar al determinării stabilității sistemului bancar al țării a fost descris de J. Keynes, care a descris relația și corelația stabilității instituțiilor financiare cu activitățile sectorului real. Extinzând acest principiu, autorii sugerează includerea în acesta a securității economice a statului.

În același timp, modelele de avertizare timpurie caracteristice sectorului bancar sunt de o importanță capitală. Întrucât băncile comerciale primesc finanțare pe piețele financiare internaționale și sunt orientate spre activitate internațională, de aceea depind în mare măsură de evenimentele internaționale, în timp ce factorii regionali joacă doar un rol secundar.

Cu toate acestea, efectele secundare regionale devin un factor determinant semnificativ al stabilității sistemului bancar, în special pentru băncile regionale mici. Autorii cred că un indicator continuu și promițător al stabilității sectorului bancar poate servi la identificarea indicatorilor macroprudențiali de avertizare timpurie și a efectelor secundare internaționale și regionale. Astfel BNM prin elaborarea Legii privind redresarea și rezoluția băncilor, [6] reglementează prevenirea crizelor bancare și asigură rezoluția ordonată a băncilor în curs de a intra în dificultate, minimizând totodată impactul acestora asupra economiei reale și a finanțelor publice. Această lege transpune standardul internațional în domeniul „Atributele-cheie pentru regimuri eficiente de rezoluție”, aprobat în noiembrie 2011 de Consiliul pentru Stabilitate Financiară, precum și Directiva 2014/59/UE privind redresarea și rezoluția instituțiilor bancare.

Indicatorul ar trebui să includă nu numai principalele instituții importante din punct de vedere sistemic, ci și băncile mici, care sunt deosebit de importante pentru creditarea regională. Indicatorul de stabilitate este destinat să ofere un instrument de analiză macroprudențială pentru supraveghetorii bancari și factorii de decizie politică. [14] Poate fi alcătuit din trei componente: *probabilitatea de nerambursare*, *spreadul creditului* și *indicele bursier pentru sectorul bancar*.

Probabilitatea de nerambursare se bazează pe modelul de risc pentru băncile mici; pentru organizațiile financiare mari, se pot utiliza ratingurile de stabilitate financiară ale Moody's Bank.

Este posibil să se formeze o estimare a profilului riscului de control ca referință pentru atribuirea ponderilor componentelor indicatorului. Acest lucru subliniază necesitatea monitorizării indicatorilor macroprudențiali în supravegherea bancară și sprijină autoritățile de reglementare care dezvoltă reglementări cerințe care includ ciclul de afaceri.

O altă posibilitate de îmbunătățire a securității economice a sistemului bancar este utilizarea instrumentelor macroprudențiale care sunt mai flexibile și care pot fi vizate în anumite puncte din sistemul financiar care creează distorsiuni. În special, Banca Națională a Moldovei poate utiliza rapoarte de adecvare a capitalului, rate de pierdere de împrumut și rate de împrumut pentru active pentru a descuraja speculațiile de pe piețele în care se formează un balon potențial.

De asemenea, este posibil să crească nivelul de securitate prin reducerea riscului sistemic prin îmbunătățirea sistemelor de decontare a plăților și prin crearea de stimulente pentru anumite tranzacții cu instrumente derivate care pot fi rezolvate.

O altă modalitate este de a dezvolta proceduri menite să mențină stabilitatea instituțiilor importante din **punct de vedere sistemic**. În conformitate cu art.63 alin. (7) din Legea privind activitatea băncilor nr.202 din 06.10.2017, Banca Națională Moldovei (BNM), în calitate de autoritate competentă, identifică băncile care sunt societăți de importanță sistemică (în continuare O-SII). Ulterior, băncile identificate vor face obiectul cerinței de menținere a amortizorului de capital aferent O-SII.[7] În elaborarea metodologiei de identificare a societăților de tip O-SII din Republica Moldova, BNM s-a condus de prevederile Ghidului Autorității Bancare Europene privind criteriile de stabilire a condițiilor de aplicare a art.131 alineatul (3) din Directiva 2013/36/EU (CRD IV) în ceea ce privește evaluarea altor instituții de importanță sistemică.[10]

Ar fi posibil să se utilizeze proceduri de autorizare similare cu cele ale Corporației Federale de Asigurare a Depozitelor, astfel încât instituțiile importante din punct de vedere sistemic să nu poată deveni prea mari pentru a fi în situație de criză. [8] Creșterea nivelului de securitate economică a sistemului bancar este posibilă prin dezvoltarea procedurilor de intervenție pentru a evita denaturări semnificative ale cursului de schimb real, a cărui modificare poate fi prea costisitoare și poate afecta stabilitatea sistemului financiar.

Scopul principal al băncii centrale în contextul instabilității geopolitice este descurajarea daunelor și limitarea impactului asupra economiei reale. Primul imperativ este să asigurăm liniștea pe piețele financiare. Panica pieței creează echivalentul unui atac financiar, întrerupând fluxul de împrumuturi. Acest lucru crește daunele din sistemul bancar și este unul dintre principalele canale de transmisie prin care criza afectează economia reală. Prin urmare, este necesar să se reducă incertitudinea, să se asigure buna funcționare a piețelor de credit pe termen scurt și să se prevină prăbușirea instituțiilor de credit din cauza constrângerilor de lichiditate.

O altă măsură neconvențională este intervenția directă pe piețele financiare: achiziționarea directă de instrumente financiare pentru a influența curba randamentului sau

pentru a stimula o piață de credit importantă din punct de vedere sistemic. Dacă este necesar, flexibilitatea poate fi utilizată ca instrument suplimentar. Este posibil să se reducă cerințele de garanție și să se ofere o gamă mai largă de instrumente: să se organizeze swapuri inter-valutare cu băncile centrale străine pentru a furniza lichidități, exprimate în valută străină.

Un punct important este *lichidarea datoriilor la împrumuturi*. Împrumuturile restante sunt o povară pentru bilanțurile băncilor și înrăutățesc profitabilitatea băncilor, provocând pierderi de venituri. De asemenea, acestea blochează o parte din capitalul băncilor, reducând astfel capacitatea băncilor de a acorda noi împrumuturi. Asigurarea securității economice a sistemului bancar necesită progrese în curățarea bilanțurilor băncilor și restabilirea unor buffere de capital suficiente. Este necesar să se realizeze o restructurare reală a împrumutului sau răscumpărarea activelor neutilizate, care ar trebui să fie susținute de cadrul legal actual pentru a asigura povara datoriei și răscumpărarea activelor.

Multe țări lucrează pentru a îmbunătăți cadrul insolvenței și funcționarea sistemului judiciar pentru a asigura o restructurare mai rapidă a datoriilor. De exemplu, Grecia a introdus licitații electronice pentru a vinde garanții. O altă modalitate este deciziile de restructurare extrajudiciară, bazate pe cooperarea voluntară a băncilor și a debitorilor. Dacă restructurarea împrumuturilor eșuează, băncile ar putea lua în considerare eliminarea activelor depreciate. Împrumuturile restante pot fi tranzacționate pe piețe secundare specializate, eventual ca produse securitizate.

Pentru a face față moștenirii împrumuturilor cu probleme, unele țări au înființat companii de administrare a activelor (AMC), cunoscute și sub numele de „bănci rele", astfel încât băncile să le poată transfera portofolii de datorii neperformante. Sprijinul pentru vânzarea unor astfel de datorii poate fi organizat și de sectorul bancar însuși (prin garanții guvernamentale, de exemplu, utilizând schema Atlante din Italia). Rolul autorităților naționale de supraveghere și al autorităților de reglementare este fundamental atunci când vine vorba de soluționarea problemei.

Astfel de organisme verifică în mod regulat calitatea activelor bancare, controlează rambursarea datoriilor și impun rezerve adecvate pentru pierderi la împrumuturi și tampoane de capital.

În plus, pare oportun să se dezvolte surse alternative de finanțare pentru companii. Pentru a îmbunătăți accesul la finanțare prin surse nebancare, ar trebui întreprinse diverse acțiuni pentru dezvoltarea piețelor de capital: piețele de valori și obligațiunile, fondurile de capital privat și de capital de risc și abordările moderne ale securitizării. De asemenea, este important să se implementeze măsuri specifice pentru a sprijini dezvoltarea piețelor regionale de capital.

Securitatea bancară presupune sistemul de protecţie a informaţiilor bancare şi a mijloacelor financiare aflate în gestiunea băncii.

Existența unui sistem de securitate sănătos în bancă este cauzat de următoarele:

- ✓ majoritatea resurselor financiare ale băncii sunt împrumutate, păstrarea integrităţii lor presupune păstrarea stabilităţii băncii;
- ✓ un sistem de securitate slab favorizează fraudele bancare, informaţia despre fraude comise în cadrul băncii va submina autoritatea băncii pe piaţă precum şi în faţa clienţilor săi;
- ✓ existenţa unui sistem de securitate condiţionează posibilitatea băncii de a majora şi diversifica serviciile. Un sistem de securitate slab în schimb generează cheltuieli suplimentare pentru bancă pentru finanţarea fraudei sau îmbunătăţirea sistemului de securitate existent.

ROLUL ȘI IMPORTANȚA MODELULUI DE BUSINESS ÎN ACTIVITATEA BANCARĂ

Analiza sistemelor bancare naţionale din ţările dezvoltate evidenţiază că acestea sunt foarte diferite, fiind constituite dintr-o mare varietate de instituţii, cu precădere în cadrul spaţial financiar european. În acest context, s-a formulat întrebarea dacă procesul de globalizare financiară, care se traduce prin emergenţa progresivă a unei industrii bancare mondiale, nu va favoriza o tendinţă de uniformizare a sistemelor bancare, pe baza unui model dominat de bancă. [9].

Pentru instituțiile financiare și bănci, *instrumentele de securitate* sunt o parte esențială a activității lor, nu numai în ceea ce privește păstrarea în siguranță a conturilor clienților lor, ci și în ceea ce privește conformitatea internă. Aceste organizații au responsabilitatea de a proteja atât banii, cât și informațiile clienților lor. În consecință, este vital să aibă instrumentele și tehnologia la locul lor pentru a proteja aceste active critice.

Pe măsură ce tehnologia continuă să se dezvolte în ritm, în 2020 vom vedea că mai multe bănci încep să adopte *inteligența artificială (AI)* asociată cu *machine learning* (ML – învățarea automată) pentru a oferi clienților lor caracteristici de securitate îmbunătățite. În plus, pe măsură ce concepțiile greșite și miturile despre *securitatea cloud* sunt disipate, adoptarea tehnologiei cloud va crește, de asemenea. Acum, în 2020, ce va însemna adoptarea sporită a acestor tehnologii în rândul instituțiilor financiare pentru securitate în industria bancară în anul următor?

Prin utilizarea sporită a *inteligenței artificiale (AI)* și a învățării automate (ML – *machine learning)* în următorii ani, băncile vor putea ajuta clienții să își păstreze conturile mai sigure prin detectarea oricăror anomalii și activități frauduloase mult mai rapide decât s-a putut anterior. Frumusețea utilizării AI și ML în acest mod constă în capacitatea lor de a înțelege ceea ce este „normal” pentru fiecare cont sau card prin recunoașterea tiparelor bazate pe tranzacții și comportamente anterioare.

De exemplu, dacă 99% din tranzacțiile pentru un cont au loc de luni până vineri, o tranzacție care are loc în weekend va fi văzută ca fiind anormală și marcată ca atare. Odată cu accelerarea AI a detectării oricăror abateri de la tiparele normale, băncile vor putea răspunde mai rapid atunci când își vor informa clienții dacă conturile lor par să fi avut o activitate neobișnuită. Întrucât întreprinderile pierd în prezent o medie de 7% din cheltuielile lor anuale din cauza fraudelor și în 2017, înregistrând un record de 16,7 milioane de victime ale fraudelor de identitate, utilizarea AI și ML ar trebui să vadă această cifră redusă. [11]

Desigur, tranzacțiile anormale nu sunt întotdeauna fraude. Adesea, sunt doar ieșite din comun, necesitând mai multe investigații, iar semnalizarea acestora către afaceri ar permite acest lucru. Aceste noi tehnologii vor asigura întreprinderilor posibilitatea de a face față discrepanțelor din conturile lor imediat, mai degrabă decât să afle despre ele luni în jos, când este mai greu să obțineți o imagine clară a evenimentelor în momentul în care a avut loc tranzacția.

Deși este puțin probabil să se întâmple în 2020, în viitor, putem ajunge la un punct în care detectarea fraudelor se poate face în timp real, pentru a opri tranzacțiile frauduloase pe urmele lor. În aceste cazuri, am putut vedea contul blocat sau blocarea cardului pentru a împiedica finalizarea tranzacției.

AI și ML vor fi, de asemenea, esențiale pentru *securitatea cibernetică* și menținerea conformității cu reglementările, ambele fiind subiecte fierbinți pentru sectorul serviciilor financiare și vor continua să se deplaseze în 2020 și nu numai. Vom vedea că mai multe bănci folosesc ML pentru a codifica platformele pentru a identifica tiparele utilizatorilor și

a detecta comportamentul anomal al rețelei, care devine din ce în ce mai esențial, deoarece atacurile cibernetice sunt adesea deghizate cu date sau cod discret. [11]

În mod istoric, *adoptarea cloud-ului* a fost lentă în rândul instituțiilor financiare, în parte din cauza concepțiilor greșite despre securitate. Cu toate acestea, băncile încep să-și dea seama că *serviciile de cloud computing* nu prezintă un risc de securitate mai mare decât tehnologia actuală, deoarece furnizorii de cloud public au investit timp, bani și eforturi pentru a îndeplini standardele de securitate.

În cele din urmă, *furnizorii de cloud* au servicii de securitate comodizate, deci în loc de băncile care au nevoie să-și construiască propriile capacități de criptare, de exemplu, experți din industrie, cum ar fi *AWS cloud*, le-au făcut posibilă implementarea serviciilor de securitate printr-un clic dintr-un buton direct din cutie. Acest lucru oferă băncilor o modalitate mult mai rapidă și mai ușoară de a fi sigure decât implementarea sau adaptarea caracteristicilor de securitate în propriile medii. Acest lucru va ajuta băncile să se asigure că stochează informațiile despre clienți într-un mod sigur și conform, respectând reglementările bancare pe scară mai largă. [11]

Biometria a fost utilizată pentru a face accesul la conturi și a face plățile mai sigure de câțiva ani, dar numai pentru cei cu anumite dispozitive și cu anumite bănci. Cu toate acestea, se anticipează că până la finele anului 2020, aproape toate dispozitivele inteligente , inclusiv telefoanele mobile , tabletele și dispozitivele portabile , vor avea o anumită formă de activare a securității biometrice, astfel încât această funcționalitate va deveni în curând mai disponibilă pe scară largă. În consecință, mai mulți oameni vor putea efectua plăți prin amprente digitale și recunoașterea facială și, până în 2023, se estimează că vor fi peste 2,6 miliarde de utilizatori de plăți biometrice.

Deși autentificarea biometrică în prezent tinde să fie disponibilă doar consumatorilor, 2020 ar putea fi anul în care clienții corporativi au acces la aceeași funcționalitate. Pe măsură ce funcționalitatea biometrică se extinde în arena cardului corporativ, procesul de plăți comerciale nu numai că va deveni mai sigur, ci și mai ușor. De asemenea, am putea vedea portofele mobile care se amintesc de atributele personale ale individului pentru a efectua plăți sigure pe aceste carduri, fie că sunt autentificate prin amprentă digitală sau prin recunoaștere facială.

Deși amenințările privind securitatea cibernetică, cum ar fi malware-ul (*softwturi de eliminare și protecție împotriva fraudelor*) și riscul de fraudă, nu vor dispărea niciodată, în 2020, vom vedea băncile adoptând măsuri noi și mai sofisticate pentru a preveni aceste cazuri și a îmbunătăți securitatea în sectorul financiar. Cheia acestui lucru va fi adoptarea sporită a tehnologiilor inteligenței artificiale (AI) și a învățării automate (ML), care vor ajuta băncile să detecteze mai repede anomaliile și, poate, într-o zi, să le oprească să se producă cu totul. Eficiența acestor tehnologii este deja realizată de băncile corporative, utilizarea de către Visa a AI a redus ratele globale de fraudă la mai puțin de 0,1%. Pe măsură ce mai multe bănci recunosc impactul semnificativ pe care AI și ML îl pot avea nu numai asupra securității, ci și asupra organizațiilor lor în următorii ani de dezvoltare a acestui domeniu, este probabil să vedem mai multe companii care apelează la fintechs pentru sprijin. Pe o piață atât de competitivă, acesta va fi un pas vital pentru a învăța cum să folosim cel mai bine aceste tehnologii pentru a îmbunătăți securitatea și a menține conformitatea pentru a păstra clienții și a atrage noi. Aceste tehnologii vor oferi, de asemenea, băncilor avantajul de a deveni mai agile și mai inovatoare, ajutându-le astfel să-și păstreze clienții existenți și să atragă alții noi. [11]

În zilele noastre, există multe noutăți pentru instituțiile financiare – și clienții lor – de luat în considerare. Dar într-un moment în care încrederea consumatorilor în activități

bancare se află într-un moment critic, atât de multe dintre aceste influențe menționate anterior se află în afara controlului direct al unui lider bancar / de securitate.

Totodată este de menționat faptul că încă de la finele anului 2017, băncile din Republica Moldova sunt obligate să implementeze, la cererea societății SWIFT, Programul de Securitate a clienților (Customer Security Programme - CSP) care vizează îmbunătățirea partajării informațiilor în întreaga comunicate bancară. Măsura a fost luată de SWIFT, ca urmare a creșterii "numărului amenințărilor și atacurilor cibernetice la nivel mondial", notează, cu referire la Banca Națională a Moldovei (BNM) [12].

În special e vorba o serie de tentative, dar și fraude de la o serie de bănci din lume, inclusiv și de la bănci centrale. Cel mai celebru caz a fost în 2016, când hackerii au reușit să scoată din Banca Centrală din Bangladesh 81 milioane dolari, urma cărora se pierde în cazinourile din Filipine.

Cercetătorii susțin că viramentele frauduloase au trecut printr-o piratare informatică sofisticată a rețelei bancare SWIFT (Society for Worldwide Interbank Financial Telecommunication) care leagă între ele miile de bănci din întreaga lume.

Și în cazul furtului miliardului, cele trei bănci implicate au creat datorii false față de terțe părți. Astfel în noiembrie 2014, reprezentanții acestor trei bănci au trimis la SWIFT mesaje false cu privire la punerea în aplicare a anumitor operațiuni, inducând în eroare organele de supraveghere, inclusiv Banca Națională.

În consecință în anul 2017 societatea SWIFT a lansat Programul de Securitate a clienților (Customer Security Programme – CSP) care vizează îmbunătățirea partajării informațiilor în întreaga comunitate SWIFT, îmbunătățirea instrumentelor SWIFT pentru clienți și asigurarea unui cadru de control al securității clienților. Băncile din Republica Moldova urmau să implementeze acest program conform cerințelor stabilite de către societatea SWIFT.

Prima etapă – efectuarea unei autoevaluări până la finele anului 2017 și identificarea nivelului de conformare la cerințele de securitate SWIFT – a fost finalizată cu succes. Constatarea a fost făcută în cadrul comunicării dintre băncile licențiate și Banca Națională a Moldovei, dar și într-o scrisoare parvenită de la SWIFT", se arată într-un răspuns pentru Mold-Street a autorității bancare.

Cu toate acestea, va trebui în continuare efectuată o activitate semnificativă care să conducă la îmbunătățiri suplimentare în materie de securitate și la creșterea transparenței în cadrul comunității financiare.

Unele bănci din Republica Moldova sunt extrem de inovative la acest capitol și au avansat mult în acest sens. De exemplu Moldindconbank a ales soluția FMA de la compania Allevo pentru oglindirea tranzacțiilor SWIFT între platformele de producție și de backup, asigurând integritatea și consistența datelor, precum și continuitatea operațională.

„Am ales soluția FMA pentru a fi pregătiți să facem față cu brio posibilelor evenimente neplanificate. Grație acestei soluții vom ști exact care sunt pașii care trebuie parcurși și cât timp este necesar pentru ca activitățile noastre să revină la normal, fără impact asupra datelor", spune Mihai Ursu, Director al Departamentului Tehnologii Informaționale din cadrul Moldindconbank.

Or, gestionarea riscurilor și asigurarea continuității operaționale 24/7 în orice condiții sunt două aspecte extrem de importante pentru toate băncile. [13]

De notat că Banca Națională a Moldovei are conexiune directă cu centrul global de procesare SWIFT amplasat în Olanda și nu apelează la serviciile companiilor de intermediere pentru primirea/transmiterea mesajelor SWIFT.Și băncile comerciale din Republica Moldova, de asemenea, au o conexiune directă, cu excepția uneia mici, care se

conectează la sistemul SWIFT prin SWIFT Service Bureau al companiei ProFIX din Ucraina. [13]

CONCLUZII

Rezumând cele menționate mai sus, putem concluziona că sistemele bancare sunt elemente importante al securității economice, permițând formularea și implementarea politicilor monetare și de supraveghere, promovarea creării unui mediu economic și financiar solid și exercitarea responsabilității funcționale, pentru asigurarea unui sistem financiar fiabil și stabil.

Securitatea se bazează, înainte de toate, pe o stabilitatea economică, dar şi pe o stabilitate politică. Astfel, putem afirma că un sistem viabil de securitate va putea fi clădit doar dacă sunt consolidate aceste două componente. Certitudinea, încrederea şi liniştea îşi au originea nu doar în absenţa pericolelor, ci chiar în ţinerea acestora sub control.

În ultima perioadă, sectorul bancar operează într-un mediu caracterizat de instabilitate și incertitudine, iar pierderile pot genera tulburări severe activităților bancare. Reputația și stabilitatea instituțiilor bancare depind de capacitatea acestora de a face față tulburărilor și provocărilor, fie că sunt de natură infracțională (spălare a banilor, finanțare a terorismului, corupție sau fraudă), fie că este vorba de impactul globalizării sau a crizelor economice. De aici, putem afirma importanța studierii securității bancare și a fenomenelor care o poate impacta, într-un fel sau altul.

De asemenea, în acest studio am reflectat și câteva cazuri intens mediatizate și discutate de securitatea sistemelor informatice. Securitatea sistemelor informatice**,** tratează problema securității în instituțiile bancare. Securitatea reprezintă o stare atașată de esența unei bănci, o stare în care cele mai mici pericole ar trebui să poată fi anticipate. Odată cu dezvoltarea sistemului bancar, securitatea și, implicit, politica de securitate s-a impus categoric în întreg sistemul bancar. De asemenea, am încercat să subliniez importanța înlăturării factorilor sau a proceselor ce pot avea un impact negativ asupra serviciilor oferite, a imaginii instituției, a politicilor, a dezvoltării administrative și organizaționale.

În încheiere putem menționa că securitatea bancară este un domeniu complex format din mai multe ramuri și activități. Datorită evoluțiilor din domeniul tehnologiei, instituțiile bancare au devenit mult mai vulnerabile. Fie că este vorba de un angajat bancar, fie că este vorba de un client, securitatea bancară sau a operațiunilor, precum și confidențialitatea datelor sunt prioritare.

BIBLIOGRAFIE

1. Perciun R. *Managementul stabilității financiare sistemice în contextul asigurării securității economice a Republicii Moldova*. Teza de doctor habilitat în științe economice. CZU: 336.1, Chișinău, 2017.
2. Raport iese business school şi cepr pentru lumea post-covid: este necesară o restructurare profundă a multor sisteme bancare, pe termen mediu"[Online] Published: 22 iunie 2020, Avialable at: https://www.bursa.ro/raport-iese-business-school-si-cepr-pentru-lumea-post-covid-este-necesara-o-restructurare-profunda-a-multor-sisteme-bancare-pe-termen-mediu-25568936 [Accesat 10.11.2020]
3. Provocări de supraveghere ale pandemiei și nu numai [Online] Published: 3 noiembrie 2020, Avialable at: https://www.bankingsupervision.europa.eu/banking/tasks/stresstests/html/index.ro.html [Accesat 10.11.2020]
4. Shadi A. Online Banking Security Measures and Data Protection, Jordan University of Science and Technology, 2017, 312 p. [Online] Published: 17 oct 2017, Avialable at:

https://ru.scribd.com/document/361814047/Online-Banking-Security-Measures-and-Data-Protection [Accesat 10.11.2020]
5. Dremov D., Penkin A. Possibilities of increasing the economic security level of the Russian banking system in conditions of geopolitical instability Aumento el nivel de seguridad económica del sistema bancario ruso en condiciones de inestabilidad geopolítica. [Online] Published: 30 mai 2018, Avialable at: https://www.revistaespacios.com/a18v39n36/a18v39n36p20.pdf [Accesat 10.11.2020]
6. Legea privind redresarea şi rezoluţia băncilor nr. 232 din 03.10.2016
7. Metodologia de identificare a societăților de importanță sistemică (societățile de tip O-SII) din Republica Moldova, aprobată prin HCE al BNM nr. 192 din 31.07.2018
8. Corporația Federală pentru Asigurarea Depozitelor (FDIC) Avialable at: https://www.fdic.gov/ [Accesat 10.11.2020]
9. Gîrlea M., Modelul de business bancar: tendinţe actuale USM. Revista ştiinţifică „Studia UniversitatisMoldaviae", 2017, nr.2(102) Seria "științe exacte și economice" ISSN 1857-2073 ISSN online 2345-1033 p.102-107
10. Ghidul privind procedurile și metodologiile comune pentru procesul de supraveghere și evaluare (SREP), elaborat și aprobat de Autoritatea Bancară Europeană (EBA/GL/2014/13 din 19.12.2014), [Online] Avialable at: https://www.bankingsupervision.europa.eu/banking/srep/srep_2019/html/methodology.en.html#toc28 [Accesat 07.11.2020]
11. Gareth J., Banking security in 2020: what to expect. [Online] Published: 30 january 2020, Avialable at: https://www.techradar.com/news/banking-security-in-2020-what-to-expect [Accesat 10.11.2020]
12. Regulament privind cerințe minime pentru Sistemele Informaționale și de Comunicare ale băncilor, aprobat prin HCE al BNM nr.47 din 14 martie 2018
13. Băncile din Republica Moldova, obligate să implementeze noi măsuri de Securitate. [Online] Published: 9 aprile 2018, Avialable at: https://radiochisinau.md/bancile-din-republica-moldova-obligate-sa-implementeze-noi-masuri-de-securitate---65863.html [Accesat 10.11.2020]
14. Metodologia de supraveghere și evaluare a activității băncilor, aprobată de către Banca Naţională a Moldovei prin hotărârea nr. 63 din 28 februarie 2019.
15. Postolache, Victoria. Securitatea economică a sectorului bancar în condiţiile contemporane / Victoria Postolache, Andrei Curac // Asigurarea viabilităţii economico-manageriale pentru dezvoltarea durabilă a economiei regionale în condiţiile integrării în Uniunea Europeană: Materialele Conf. şt. intern., Bălţi, 16-17 septembrie, 2016. – Iaşi : Editura Pim, 2017. – P. 383-388. – ISBN 978-606-13-3642-5.
16. Gîrlea Mihail Securitatea financiară a sistemului bancar prin intermediul implimentării acordului Basel III / Financial security of the banking system through the implementation of Basel III agreement. În: Studia Universitatis Moldaviae, seria Ştiinţe exacte şi economie nr. 2 (62), Chişinău, CEP USM, 2013, ISSN 1857-2073, ISSN ONLINE 2345-1033, p. 84-88.
17. Clichici, D. promovarea securităţii financiare a sistemului bancar prin intermediul implementării acordului basel ii/ promoting financial security of the banking system through the implementation of basel ii agrument. în: revista ştiinţifico-didactică economica, an.XIX, nr.3(77), septembrie 2011, Chişinău, p.77-84. ISSN 1810-9136

EXTERNAL AND INTERNAL ASSESSMENT OF HOSPITAL SERVICE SECURITY SPECIFIC RISK

EVALUAREA EXTERNĂ ȘI INTERNĂ A RISCURILOR SPECIFICE SECURITĂȚII SERVICIILOR DE OSPITALITATE

Buzdugan Adriana
Doctor în științe economice, conferențiar universitar
Universitatea de Stat din Moldova
e-mail: buzdugan.adriana@gmail.com

Abstract
Industria ospitalității este un grup complex de diferite tipuri de afaceri și o comunitate care oferă diverse servicii vizitatorilor. Cazarea este cea mai prioritară direcție în domeniul ospitalității și include hoteluri, moteluri, pensiuni și chiar cămine universitare. Un alt aspect al industriei de ospitalitate îl reprezintă parcurile de distracții, parcurile tematice, parcurile acvatice, terenurile de golf, stațiunile de schi și multe altele care se încadrează în această categorie. Cazinourile, barurile și cluburile de noapte sunt alte fațete unice ale ospitalității care au propriile lor considerații speciale. Alte facilități care completează această industrie sunt arenele, stadioanele și locurile de evenimente în aer liber.
În ceea ce privește securitatea în industria hotelieră, este atât de dificil de ținut la distanță și în afara unui hotel deschis publicului, persoanele care ar putea aduce prejudicii sau crea stări de nesiguranță. Multe dintre metodele tradiționale de securitate, cum ar fi încuietori, alarme și camere de luat vederi, sunt utilizate în instalațiile unităților de cazare, dar trebuie aplicat și metode mai creative, cum ar fi patrulare, recunoaștere comportamentală, descurajare pasivă și conștientizare.
Evaluarea riscurilor este complicată, deoarece trebuie de luat în considerare siguranța oaspeților și infracțiunile împotriva persoanelor. Indiferent dacă proprietatea este în faza de proiectare, finalizată recent sau o locație cu istorie, trebuie definitivat procesul de evaluare a riscurilor. O evaluare a riscurilor cercetată și luată în considerare ajută la gestionarea planului de măsuri de protecție și oferă o protecție juridică pentru măsurile întreprinse.

Cuvinte cheie: *ospitalitate, securitate, risc, hotel, sistem de securitate.*

Clasificator JEL: *Z3*

INTRODUCERE

Multe hoteluri funcționează de ani de zile și nu au realizat vreodată o evaluare formală a riscurilor. Evaluările informale ale riscurilor sunt efectuate în mod constant de către profesioniști în securitate, ingineri și manageri de risc. Formal sau informal, procesul este în mare parte același. Decizia fundamentală a managerilor este dacă ar trebui de elaborat individual acest proces sau de angajat un profesionist din domeniu. Un consultant din extern poate adăuga o integritate evaluării riscurilor, fiind un profesionist cu experiență și resurse necesare pentru a face o analiză amănunțită și o evaluare consecventă pentru a adăuga credibilitate unității de cazare. Singurul motiv pentru care nu se apelează la un expert din exterior este costul. Cu toate acestea, costurile pot fi justificate prin economii în alte domenii.

CONȚINUT

Riscurile potențiale din industria ospitalității includ inovația, problemele de siguranță, dezastrele naturale și riscul reputațional.

Inovația. A patra revoluție industrială a adus conexiuni digitale fără precedent. Odată cu acestea vine riscul de securitate cibernetică. Internetul, utilizarea aplicațiilor

mobile pentru a procura servicii, a debloca ușile camerelor de hotel și a îndeplini alte sarcini, inteligența artificială și alte tehnologii pot oferi criminalilor cibernetici oportunități sporite de a accesa informațiile personale ale clienților, informațiile despre cardul de plată și obiectele de valoare.

Probleme de siguranță. Acestea includ siguranța alimentelor, alunecările și căderile și alte pericole fizice.

Dezastrele naturale includ evenimente meteorologice volatile și epidemii de boli, ambele devenind mai frecvente pe măsură ce climatul global se încălzește.

Riscul reputațional. Întrucât consumatorii se bazează din ce în ce mai mult pe recenziile online ale clienților, riscul reputațional este un domeniu cheie de monitorizat pentru ospitalitate.

Spre deosebire de alte industrii, afacerile din sectorul ospitalității nu au un singur standard industrial sau cadru de reglementare care să ghideze strategiile de gestionare a riscurilor. Prin urmare, unii aleg să adauge un ofițer șef de risc, care poate supraveghea riscul în materie de ospitalitate din evaluarea riscurilor până la finalizarea conformității.

Riscul expus hotelurilor este evaluat pentru a determina tipul de risc care afectează activele implicate în hoteluri. John Fay [1, p.415] susține că evaluarea expunerii la risc determină efectul pe care evenimentul îl va avea asupra perturbării organizației, de exemplu, răpirea în cazul în care unul dintre invitați este răpit și ținut ostatic de persoane necunoscute, pentru extorsiunea de bani sau secrete comerciale nedivulgate, de la directorul financiar al hotelului.

În 1993, într-o tentativă de jaf, un turist (oaspete) britanic, Gary Colley, a fost ucis într-un hotel din Florida, Statele Unite ale Americii. Acest incident a avut un impact negativ asupra industriei hoteliere, biroul de externe britanic a recomandat turiștilor britanici să nu mai trimită oaspeți la hotelurile din Florida. [4, p.21]

Hotelierii la nivel global monitorizează pe larg personalul contractat și efectuează controale biografice asupra angajaților interni. Reprezentanții industriei hoteliere au luat decizia de a dezvolta un departament care se va ocupa de prevenirea riscurilor generate de securitatea hotelului [3, p.78].

Prevederile fundamentale pentru asigurarea siguranței hotelurilor sunt:

- formarea unui set exhaustiv de obiective pentru a asigura siguranța hotelului;
- analiza listei posibilelor amenințări, clasificarea probabilităților de risc și a daunelor potențiale;
- implementarea unei abordări integrate și a combinației reciproce de măsuri și soluții organizaționale, tehnice și de personal;
- minimizarea costurilor prin criteriul „eficiență / cost”;
- asigurarea supraviețuirii, flexibilității și controlul complexului de securitate;
- posibilitatea dezvoltării, modernizării și schimbării configurației complexului de securitate.

Conceptul de securitate a hotelului include nu numai protecția împotriva atacurilor criminale, ci și crearea de măsuri preventive pentru a asigura protecția împotriva incendiilor, exploziei și a altor evenimente de urgență.

O soluție eficientă la problema securității hoteliere necesită o abordare sistemică bazată pe o analiză a funcționării facilității, identificând zonele cele mai vulnerabile și în special amenințările stringente, elaborând toate scenariile posibile ale acțiunilor criminale și dezvoltând contramăsuri adecvate.

O abordare integrată presupune combinația optimă de măsuri organizaționale, tehnice și fizice de prevenire și răspuns în timp util la orice situație periculoasă. O

importanță majoră trebuie de acordat alegerii corecte a mijloacelor tehnice și a sistemelor de securitate, proiectării, instalării și întreținerii corectă în cadrul facilităților.

Măsuri organizatorice pentru a asigura securitatea hotelului

Metoda tradițională de sporire a securității prin creșterea numărului de angajați nu dă rezultatul dorit, atât din considerente economice, cât și eficiența scăzută a acestei abordări. O persoană care este de serviciu este supusă oboselii, neglijenței, coliziunii cu infractorii, șantajului, intimidării etc. Singura soluție corectă la problema siguranței este utilizarea unei abordări sistemice, integrate, care combină metode de natură organizațională, tehnică și fizică în combinația lor corectă și o determinare rezonabilă a ponderii fiecărei componente.

Măsurile organizatorice includ: sisteme special dezvoltate pentru reglementarea comportamentului personalului de serviciu și al angajaților responsabili de siguranță; desfășurarea de activități de instruire specială a personalului de securitate; tehnologia serviciilor hoteliere; principiile organizării procedurii de acces și protecție a diferitelor categorii de camere de hotel și spații de birouri; reglementarea acțiunilor angajaților în situații extreme.

Trebuie remarcat în special faptul că marele (poate principalul) pericol al hotelului este posibilitatea de incendiu, incendiul accidental sau deliberat, necesită, de asemenea, dezvoltarea și implementarea unor măsuri organizatorice și tehnice adecvate și este una dintre cele mai importante componente ale unui sistem integrat de securitate.

Este evident că trecerea la un nou concept modern de securitate hotelieră, care prevede utilizarea unor echipamente speciale complexe, necesită o revizuire a aspectelor tactice în activitatea diferitelor servicii hoteliere.

Este necesar să se pună în aplicare următoarele măsuri organizatorice:

- să se dezvolte instrucțiuni detaliate de acțiune în toate situațiile de urgență posibile și să le aducă la cunoștință fiecărui angajat;
- să se elaboreze instrucțiuni scurte, clare, extrem de informative și intuitive despre echipamentul de siguranță al oaspeților,
- să fie incluse reguli scurte pentru comportamentul în caz de urgență;
- să se organizeze regulat sesiuni de instruire pentru îmbunătățirea calificărilor personalului de securitate, antrenament fizic și de luptă, să se efectueze instruire pentru tot personalul hotelului privind regulile de utilizare a echipamentului complexului de securitate;
- să se organizeze pentru personal o examinare periodică (cel puțin o dată pe an) a cunoștințelor în domeniul securității, să se organizeze o pregătire suplimentară pe măsură ce personalul se schimbă și hotelul este modernizat;
- să se organizeze un serviciu de inginerie profesional (în cadrul personalului serviciului de securitate), ale cărui responsabilități ar include întreținerea tehnică a complexului de automatizare hotelieră, instruirea și consultarea personalului altor servicii hoteliere, alte activități (dezvoltate individual pentru fiecare hotel specific).

Ofițerii de securitate studiază în permanență experiența operării hotelurilor și activitatea serviciilor lor de securitate, statisticile privind infracțiunile, pentru a avea interacțiuni de consultare cu specialiști din serviciile de securitate de stat, securitatea împotriva incendiilor și agențiile de aplicare a legii.

Astăzi, profesioniștii din domeniul ospitalității au la dispoziție diverse mijloace de combatere a criminalității: lacăte electronice pentru carduri, seifuri, sisteme de alarmă antiefracție și supraveghere video etc.

Trebuie remarcat faptul că, în condițiile moderne, securitatea hotelurilor este imposibilă fără un sistem de echipamente tehnice de securitate. Măsurile de securitate, dezvoltate și implementate în hotel, ar trebui să vizeze îndeplinirea următoarelor sarcini:

- asigurarea siguranței și securității oaspeților și a bunurilor lor personale în timpul șederii lor în hotel;
- protejarea proprietății hoteliere împotriva acțiunilor ostile (furt, vandalism etc.);
- asigurarea protecției hotelului (a clădirii în sine și a tot ceea ce se află în ea) împotriva actelor teroriste (atacuri, sabotaje etc.);
- menținerea ordinii publice și asigurarea conduitei adecvate în toate zonele publice ale hotelului;
- oferirea oaspeților liniște și intimitate în timpul șederii în hotel
- asigurarea posibilității unui răspuns imediat și eficient în cazul oricărui eveniment ce necesită intervenția personalului hotelului sau a reprezentanților departamentelor terțe (de exemplu poliție, ambulanță etc.);
- asigurarea unei conduite adecvate, precum și a integrității și onestității întregului personal al hotelului;
- asigurarea posibilității ca hotelul să ofere servicii speciale pentru a asigura securitatea sporită a funcționarilor de rang înalt, pentru care sunt impuse cerințe speciale.

Aplicarea acestor măsuri de securitate nu numai că va proteja clientul în timpul șederii sale la hotel, ci și va proteja angajații de acuzațiile nefondate. Și acest lucru, împreună cu alte aspecte, va crește reputația hotelului și, ca urmare, va crește rata de ocupare a acestuia.

Parametrul important în asigurarea siguranței clientului în timpul șederii sale la hotel este restricționarea și controlul accesului în cameră.

Ușile de intrare ale tuturor camerelor de oaspeți trebuie să fie echipate cu dispozitive de închidere a ușilor, montate din interior, încuietori interne suplimentare fără cheie, care sunt montate la o înălțime de 1,5 m de podea.

Ieșirile de incendiu de pe toate etajele trebuie să fie echipate cu dispozitive de închidere a ușilor și dispozitive de blocare care asigură ieșire și intrare liberă folosind chei mecanice sau carduri cu chei.

Pentru a asigura o ședere confortabilă a clienților în hotel, merită să fie folosite seifuri mici în camere și/sau un depozit centralizat de obiecte de valoare (cutii de depozitare).

Fiecare cameră de hotel trebuie să fie dotată cu un mini-seif, care este controlat (închis și deschis) de codul personal al clientului. Mărimea seifului este determinată de tipul camerei, cu toate acestea, ar fi preferate seifurile care pot stoca un computer laptop. Pentru ca persoanele autorizate să ofere asistență clienților la deschiderea seifurilor în caz de urgență, trebuie furnizat un dispozitiv principal, care este controlat de un cod special stabilit de securitatea hotelului.

Depozitarea centralizată a obiectelor de valoare ale clienților (cutii de depozitare), situate lângă biroul recepției. Clienții pot închiria o cutie (sau seifuri) într-o astfel de unitate de depozitare pentru a depozita articole voluminoase deosebit de importante și valoroase, cum ar fi arme de foc, haine de blană, valori mobiliare etc.

Fiecare celulă de stocare trebuie să fie deschisă cu două chei: cheia principală este păstrată de personalul de serviciu și cheia privată dată clientului.

Camera de depozitare ar trebui să aibă:

- ✓ pereți capitali;
- ✓ uși din metal (sau lemn tare);

- ✓ un mecanism de blocare automată a ușilor, care nu permite lăsarea ușii în mod eronat deschisă;
- ✓ control de acces (ușile sunt deschise folosind un card personal codat și / sau cod personal) cu capacitatea de a transmite un semnal secret de pericol în cazurile în care ușile sunt deschise sub constrângere;
- ✓ un sistem de alarmă de securitate.

Intrarea în spațiul de stocare trebuie vizualizată prin supraveghere video cu înregistrarea imaginii video.

Sistemul centralizat de alarmă de securitate din hotel este un mijloc de asigurare a securității zonelor hotelului, prevenind pătrunderea necontrolată în incinta clădirii și în camerele individuale.

Pentru a asigura monitorizarea continuă a alarmelor, panoul de control este amplasat într-un loc în care personalul este prezent non-stop (aceasta poate fi o cameră de control, o cameră de securitate, o recepție a hotelului).

Alarmelor de securitate pentru deschidere sunt supuse pentru:

- toate ieșirile de urgență din hotel;
- toate ușile exterioare care sunt în mod normal închise;
- ușile spațiilor de service cu echipamente, de obicei funcționează fără personal de service (motorină, transformatoare, cazan, centrală telefonică automată);
- ușile unui număr de zone critice ale hotelului, care trebuie protejate atunci când nu sunt utilizate în mod activ. Acestea sunt cămări de băuturi alcoolice, camere cu echipamente electronice (centru TV, server etc.), birouri de administrare, contabilitate (casierie).

Alarmele cu deschidere magnetică trebuie ascunse sau încorporate.

În acele locuri în care sunt necesare măsuri speciale, este necesar să se instaleze alarme de mișcare volumetrice.

Pentru transmiterea alarmei, sunetele de alarmă sunt instalate în următoarele locații:

- ✓ Recepție;
- ✓ Casierie;
- ✓ Biroul administrativ.

Sistemul de alarmă de securitate trebuie să fie echipat cu dispozitive de alarmă sonore și vizuale (sonerie, dispozitive de semnalizare stroboscopică), care trebuie să atragă atenția personalului asupra alarmei.

Este necesar să se prevadă un sistem de supraveghere video centralizat. Sistemul ar trebui să ofere capabilități de supraveghere în timp real și o evidență pentru studii ulterioare. În lifturi și scările între etaje, camerele video ar trebui să fie așezate astfel încât ușile camerei să nu intre în câmpul vizual al camerelor video. Este necesar să fie asigurată înregistrarea de pe camerele video. Monitoarele de supraveghere principale, aparatele de comutare și dispozitivele de înregistrare ar trebui instalate în biroul de securitate sau al administratorului de serviciu.

De asemenea, este necesar să se asigure un spațiu amenajat pentru vizualizarea și documentarea informațiilor video. În hotelurile moderne cu un număr mare de angajați, este recomandabil să fie echipată o intrare specială de serviciu, precum și să fie asigurat un control automat al accesului angajaților și un sistem de urmărire a orei fixe de sosire la serviciu a personalului. Sistemul ar trebui să restricționeze intrarea persoanelor care nu au acces folosind un lacăt sau încuietoare, să fie înregistrată intrarea angajaților în timp real, să fie asigurată generarea și tipărirea rapoartelor, inclusiv cantitatea de timp lucrată de angajați pe zi, lună.

Prevederile menționate pot fi utilizate ca bază pentru construirea unui sistem de securitate al hotelului. Cu toate acestea, în fiecare caz specific, alegerea sistemelor și instrumentelor este strict individuală.

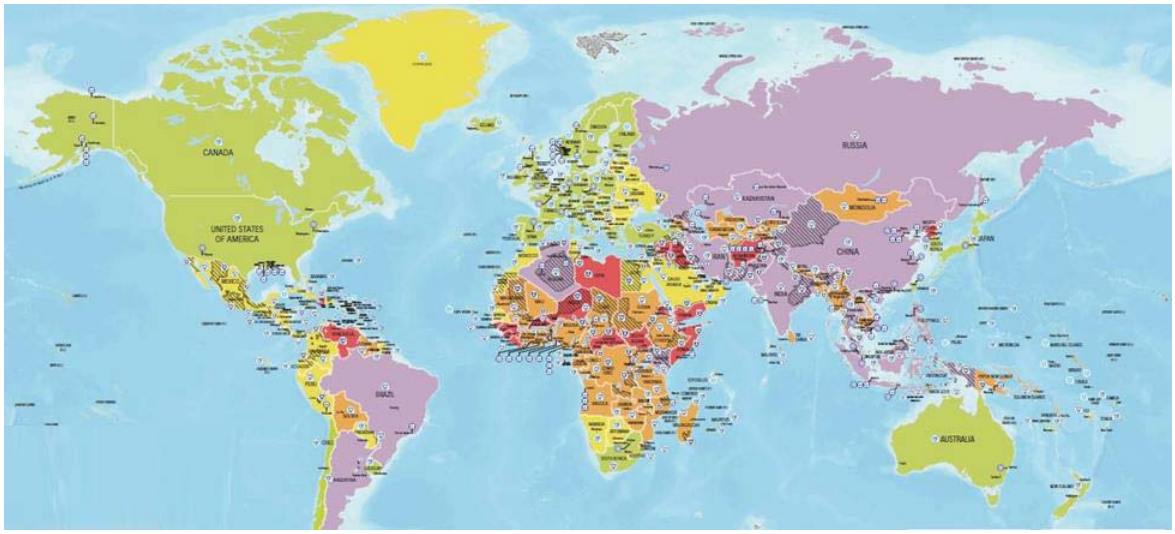


Figura 1. Harta internațională a riscurilor de călătorie 2020 pe țări

Sursa: [2]

RISC EXTREM DE CĂLĂTORIE

Controlul guvernamental, legea și ordinea pot fi minime sau inexistente pe zone întinse. Amenințare gravă a atacurilor violente ale grupurilor armate care vizează călătorii și turiștii internaționali. Serviciile guvernamentale și de transport sunt abia funcționale. Părți mari ale țării sunt inaccesibile străinilor.

RISC ÎNALT DE CĂLĂTORIE

Protestele violente sunt frecvente și pot viza sau perturba străinii; pot fi exacerbate de probleme de guvernanță, inclusiv de securitate sau capacitate de ordine și lege. Criminalitatea violentă și terorismul prezintă riscuri semnificative, directe sau accidentale, pentru călătorii și turiștii internaționali.

Este obișnuită violența comunitară, sectară sau rasială, iar străinii pot fi direct vizați. Anumite părți ale țării sunt inaccesibile sau sunt interzise călătorului.

RISC MEDIU DE CĂLĂTORIE

Se produc tulburări politice periodice, proteste violente, sau acte sporadice de terorism. Călătorii și turiștii internaționali se pot confrunta cu riscuri de violență comunitară, sectară sau rasială și infracțiuni violente. Capacitatea serviciilor de securitate și de urgență și a infrastructurii variază. Acțiunea industrială poate perturba călătoria.

RISC MIC DE CĂLĂTORIE

Ratele criminalității violente sunt scăzute, iar violența rasială, sectară sau politică sau tulburările civile sunt mai puțin frecvente. Dacă terorismul este o amenințare, grupurile au capacități operaționale limitate, iar actele de terorism sunt rare. Serviciile de securitate și de urgență sunt eficiente, iar infrastructura este solidă. Acțiunea industrială și întreruperea transportului sunt rare.

RISC NESEMNIFICATIV DE CĂLĂTORIE

Ratele infracțiunilor violente sunt foarte mici. Nu există violență politică semnificativă sau puține tulburări civile și violențe sectare, comunale, rasiale sau vizate împotriva străinilor. Serviciile de securitate și de urgență sunt eficiente, iar infrastructura este solidă. Serviciile de transport sunt la un standard ridicat, cu înregistrări de siguranță bune și doar întreruperi ocazionale ale călătoriei. Acțiunile industriale care afectează serviciile esențiale sunt rare.

VARIAȚII REGIONALE

Zonele de risc de securitate a călătoriilor sunt zone dintr-o țară în care riscurile cu care se confruntă călătorii și turiștii internaționali sunt diferite de riscul mediu general al țării, necesitând de obicei un nivel diferit de pregătire.

CONCLUZII

Pentru a conduce o afacere hotelieră eficientă, este important să existe o listă de verificare a siguranței și securității hotelului pentru efectuarea verificărilor rapid și eficient. Totul, începând de la securitatea împotriva incendiilor până la procedurile de curățare, precum și instruirea și documentația trebuie să fie acoperite în verificările zilnice.

BIBLIOGRAFIE

1. Fay J.J. Encyclopaedia of Security Management. 2nd ed. Burlington: Butterworth-Heinemann, 2007. 688 p.
2. Ollila John. Travel Risk Map For 2020. https://loyaltylobby.com/2019/11/20/travel-risk-map-for-2020/
3. Wood R.C. Key Concepts in Hospitality Management (SAGE Key Concepts series) (1st Edition). New York: SAGE Publications Ltd, 2013. 200 p.
4. Zhao J. Ho. T., Brown M. P. Examining hotel crimes from police crime reports: Crime Prevention and Community Safety In: :An International Journal, Vol. 11, 2009, p. 21-33. Disponibil online: http://link.springer.com/article/10.1057/cpcs.2008.17 (accesat 24 noiembrie 2020).

IDENTIFICATION OF ECONOMIC SECURITY RISKS AS OBJECTS OF ACCOUNTING AND ANALYTICAL PROVISION OF THE ENTERPRISES MANAGEMENT

ИДЕНТИФИКАЦИЯ РИСКОВ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КАК ОБЪЕКТОВ УЧЕТНО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ УПРАВЛЕНИЯ ПРЕДПРИЯТИЯМИ

Василишин Станислав
Кандидат экономических наук, доцент
Харьковский национальный аграрный университет им. В.В. Докучаева
e-mail: vasylishynstanislav@gmail.com

Яровая Валентина
Кандидат экономических наук, доцент
Харьковский национальный аграрный университет им. В.В. Докучаева
e-mail: yarovaya.stat@gmail.com

Abstract
The article is devoted to the substantiation of theoretical and methodological provisions for the identification of economic security risks as objects of accounting and analytical support for enterprise management as an urgent issue in the context of deepening crisis processes in the modern economy. The theoretical and methodological platform for strengthening the effectiveness of economic security risk management has been proposed, which along with the identification and management components of the existing logical chain of risk management is supplemented by the accounting and analytical component. It has been proved that the introduction of such an approach in management contributes to strengthening economic security through the adoption of prompt and relevant management decisions to identify and eliminate the negative impact on economic security of risks and threats to business.

Keywords: *accounting, accounting and analytical support, digitalization, economic security, risk.*

JEL Classification: *M40, M41*

ВВЕДЕНИЕ

Управление рисками является важным рычагом укрепления экономической безопасности предприятий в условиях рынка. Эффективность такого управления зависит от надлежащего информационно-аналитического обеспечения, которое представлено рациональным построением финансового, управленческого учета, анализа и контроля. Распространенная ныне практика учетно-аналитического обеспечения управления предприятиями находится в процессе адаптации к изменениям нормативно-правового обеспечения и приближения отечественной практики учета и отчетности к требованиям международных стандартов отчетности. Ведь от обеспечения надлежащего уровня экономической безопасности хозяйствующих субъектов напрямую зависит от единства и системности учета, анализа и контроля как составляющих организационно-экономического механизма управления предприятиями.

Учетно-аналитическое обеспечение управления предприятиями и рисками экономической безопасности нашло отражение в научных исследованиях украинских ученых, среди которых Н. Бондарь, Т. Бочуля, Л. Гнилицкая, Д. Грицишен, В. Дерий, В. Евдокимов, С. Жук, С. Легенчук, А. Петрук, Н. Правдюк, Г.

Ткачук, И. Федулова, М. Шигун, А. Шерстюк и др. В то же время установление сущности, факторов, инструментов методологии и организации функционирования системы учетно-аналитического обеспечения управления экономической безопасностью, в условиях усиления деструктивного влияния рисков вызывает необходимость более глубоких исследований.

Целью исследования является обоснование теоретических и методических положение по идентификации рисков экономической безопасности как объектов учетно-аналитического обеспечения управления предприятиями. Теоретической и методологической основой исследования являются базисные положения диалектического метода познания, в частности индукция и дедукция. Для достижения поставленной цели и решения задач в диссертации использованы также монографический, абстрактно-логический метод, методы сравнения и системного подхода.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

В общем виде исследования экономической безопасности на уровне предприятий требует дальнейшего анализа с целью изучения новых вариантов поиска существования хозяйствующего субъекта в бизнес-среде. Окончательный выбор относительно использования того или иного подхода или отдельных его составляющих остается за каждым предприятием и зависит от таких факторов, как развитие предприятия, виды деятельности, амбиции владельцев и др.

Как справедливо отмечает Л. Гнилицкая, современная система учетно-аналитического обеспечения требует нового сущностного наполнения как комплекса методов, методик, процедур и моделей, предназначенных для обоснования принятия управленческих решений в сфере обеспечения экономической безопасности предприятия [2].

Общеизвестно, что ядром управления экономической безопасностью является управление рисками и угрозами, которые оказывают влияние на нее. Известного ирландского экономиста и банкира Ричарда Кантильона считают основоположником первой концепции предпринимательства и, по мнению многих ученых, отцом термина «предприниматель», под которым он понимал человека, который работает в условиях риска, поскольку торговцы, фермеры и другие мелкие собственники покупают товар по известной цене, а продают - по неизвестной, то есть действуют в условиях риска [1].

Есть основания полагать, что учетно-аналитическое обеспечение управления экономической безопасностью должно соотноситься с особенностями установления сущности, классификации и характеру проявления рисков как объектов учетно-аналитического обеспечения.

Результаты анализа литературных источников позволяют сгруппировать внешние и внутренние угрозы системы бухгалтерского учета, которые могут негативно повлиять на безопасность предприятия (рис. 1).

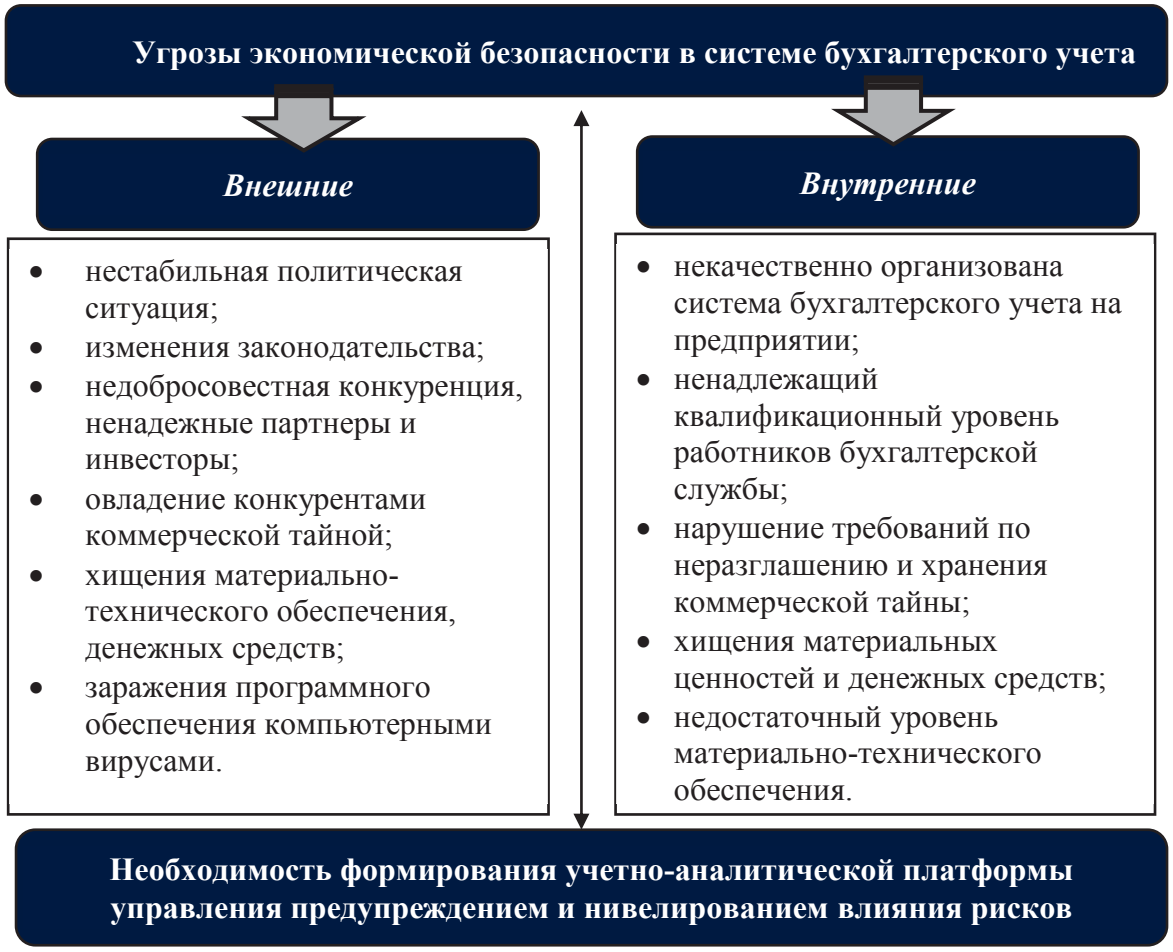


Рисунок 1. Классификация угроз экономической безопасности в системе бухгалтерского учета

Источник: авторская разработка

Приведенный перечень угроз отражает риски, находящихся на «поверхности» среды функционирования предприятия, и может быть ориентиром при разработке общих методологических основ построения учетной политики в части укрепления экономической безопасности. Однако для учета всестороннего проявления рисков экономической безопасности и оперативного их нивелирования в процессе риск-менеджмента необходимо четкое и последовательное сочетание процессов идентификации рисков, учетно-аналитического обеспечения и управления последствиями их воздействия.

Согласно этому тезису предлагаем учитывать упомянутые обстоятельства через реализацию трехэтапной теоретико-методологической платформы управления рисками экономической безопасности усиления объектных возможностей учетно-аналитического обеспечения (рис. 2).

Рисунок 2. Дифференциация уровней реализации теоретико-методологической платформы управления рисками экономической безопасности

Источник: авторская разработка

В соответствии с этим первым этапом реализации риск-менеджмента является идентификация рисков, которая представляет собой процесс выявления, исследования и описания рисков, которые могут повлиять на достижение целей организации в рамках интегрированной системы менеджмента. Этот процесс включает выявление источников рисков, исследование событий, их причин и возможных последствий. Перечень должен быть максимально полным, ведь неидентифицированные риски могут представлять существенную опасность для достижения поставленных целей, вызывать потерю контроля над процессами и привести к потере перспективных возможностей [3].

Вместе с тем идентификацию стратегических и операционных рисков обуславливает природа экономической безопасности; финансовые риски мы связываем с рисками искривления и недостоверного раскрытия показателей финансовой отчетности, а риски диджитализации – со стремительным процессом развития ИТ-технологий и их всесторонним использованием в бухгалтерском учете и экономическом анализе.

Следующим этапом реализации риск-менеджмента экономической безопасности учетно-аналитическое обеспечение, которое предусматривает рассмотрение идентифицированных рисков сквозь призму объектных возможностей бухгалтерского учета и экономического анализа. Специфичность и разносторонность каждой составляющей рисков влияют на все без исключения составляющие активов, собственного капитала, обязательств и хозяйственных процессов. Именно поэтому риск-менеджмент требует применения безопасностноориентированной учетной политики, которая будет иметь целью укрепления экономической безопасности предприятия через эффективную систему информационного обеспечения управленческих процессов.

Заключительным этапом управления рисками является принятие и реализация управленческих решений, которые будут способствовать как удовлетворению

потребностей пользователей информации, так и достижению должного уровня внешней и внутренней экономической безопасности предприятий.

Ученый В.М. Жук отмечает, что «бухгалтерский учет не ограничивается информационно-сервисной функцией управления, а представляет собой полноценный социально-экономический институт. Институт бухгалтерского учета существует независимо от восприятия или не восприятия научным сообществом. Это объективная реальность. Однако усиление положительного влияния этого института на социально-экономическую среду, рост его значимости нуждается в обновлении теоретической основы» [4, с. 21]. Итак, учетно-аналитическое обеспечение идентификации рисков предприятия представляет собой систему сбора, подготовки, регистрации и обработки данных первичного бухгалтерского, налогового, статистического и управленческого учета, а также данных аналитических расчетов для принятия на их основе управленческих решений, направленных на обеспечение защиты экономических интересов предприятия от внешних и внутренних угроз [5].

Именно поэтому в системе учетно-аналитического обеспечения управления предприятиями важно анализировать взаимосвязь между видами рисков и объектами учета, на которые они влияют, и статьями финансовой отчетности, которые такие объекты представляют. Среди специфических рисков экономической безопасности, которые требуют особого внимания при построении учетно-аналитического обеспечения, мы предлагаем выделять риск недостоверности финансовой отчетности; риск потери ликвидности и платежеспособности; инвестиционный риск; риск неэффективного управления активами; инфляционный риск; юридический риск; налоговый риск; кредитный риск; риск невыполнения обязательств и риски диджитализации.

ВЫВОДЫ

Таким образом, построение архитектуры учетно-аналитического обеспечения управления экономической безопасностью предприятий должна базироваться на стройной модели предложенной платформы риск-менеджмента, которая определяет направленность учетной политики, предопределяет трансформацию подходов к отображению отдельных объектов учета, их анализа и безопасности представления в финансовой отчетности и удовлетворяет заданный уровень экономической безопасности. Предложено теоретический подход к установлению сущности и проявлений специфических рисков экономической безопасности через объектную призму учетно-аналитического обеспечения управления экономической безопасностью предприятий, что приводит к трансформации подходов к отображению отдельных объектов учета, их анализа и безопасности представления в финансовой отчетности и удовлетворяет заданный уровень экономической безопасности.

БИБЛИОГРАФИЯ

1. Хизрич Р., Питерс М. Предпринимательство, или как завести собственное дело и добиться успеха: Вып. I. Предприниматель и предпринимательство / пер. с англ.; под. общ. ред. В.С. Загашвили. Москва: Прогресс, 1992. 160 с.
2. Федулова І. Ідентифікація господарських ризиків. *Вісн. КНТЕУ*. 2017. № 4. С. 89–103.

3. Гнилицька Л.В. Обліково-аналітичне забезпечення функціонування системи економічної безпеки суб'єктів господарювання як об'єкт наукових досліджень. *Управління проектами та розвиток виробництва.* 2011. № 1(37). С. 142-150.
4. Жук В.М. Розвиток теорії бухгалтерського обліку: інституціональний аспект: монографія. Київ: ННЦ «ІАЕ», 2018. 408 с.
5. Ткачук Г. Ідентифікація економічних ризиків в обліково–аналітичній системі підприємства. *Економіка харчової промисловості*. 2015. Вип. 4. Т. 7. С. 80–88.

FINTECH AND EFFECTIVE COMPETITION IN THE F INANCIAL-BANKING SYSTEM

FINTECH ȘI CONCURENȚA EFECTIVĂ ÎN SISTEMUL BANCAR ȘI FINANCIAR*

Chicu Veronica
Doctorandă, Academia de Studii Economice din Moldova
e-mail: veronica.chicu@ase.md

Abstract
FinTech se referă la soluțiile tehnologice pentru sectorul financiar. În fiecare dintre domeniile unde este prezent, FinTech nu doar a transformat afacerile și procesele existente, dar a creat și altele noi. Tehnologia a deschis calea unor posibilități noi atât pentru furnizorii de servicii financiare, cât și pentru consumatorii acestor servicii. Simplul acces al consumatorilor non-bancari la dispozitivelor mobile, a permis Tehnologiei financiare să valorifice segmente ale pieței nedeservite până la acel moment, încurajând și promovând astfel incluziunea financiară. Tehnologia financiară, este unul dintre cele mai captivante domenii din afacerile globale de azi, prezentând și cel mai înalt ritm de creștere. Aceasta a schimbat modul în care oamenii se gândesc la bani și la schimbul de valoare într-un timp real.

Cuvinte cheie: *FinTech, Blockchain, finanțare P2P, inteligență artificială, Machine Learning*

Clasificator JEL: *O33, G10, G21, G23*

INTRODUCERE

În contextul progresului tehnic și științific înregistrat în ultimii ani la nivel mondial, sectorul financiar s-a pomenit în situația în care instituțiile financiare nu aveau posibilitatea de a oferi clienților săi produsele la care aceștia se așteptau. Această nișă creată de decalajul între cererea și oferta de produse financiare moderne a fost rapid ocupată de FinTech (Financial Technology).

De fapt, perioada modernă a Tehnologiei Financiare își are începutul în anul 1867, când primul cablu telegrafic transatlantic făcea posibilă comunicarea în regim real între pieţele financiare principale. Iar pe parcursul ultimilor cinci ani, au fost trase mai multe cabluri subacvatice de comunicare decât în ultimii 150 ani în total.

O următoare etapă importantă în dezvoltarea FinTech s-a desfășurat în perioada celui de-al doilea Război Mondial, fiind depuse eforturi considerabile în dezvoltarea criptării și sistemelor de spargere a codurilor, fiind puse bazele pentru Inteligența Artificială. Progresele astfel înregistrate au stimulat, în perioada ulterioară, dezvoltarea tehnologiilor informatice până la conceptele cunoscute astăzi ca FinTech și RegTech (Regulatory Technology).

FinTech cuprinde astăzi cinci domenii majore: Finanțe și investiții, Operațiuni și gestionarea riscurilor, Plăți și infrastructură, Securitatea datelor și monetizare și Interfața utilizatorilor [1, p.20]. În fiecare dintre aceste domenii, Tehnologia nu doar a transformat afacerile și procesele existente, dar a creat și sub-domenii noi.

* Ref: la proiect din Program de stat cifrul 20.80009.0807.42 Configurarea businessului inovațional în contextul concurenței regionale

IMPACTUL FINTECH ASUPRA SECTORULUI FINANCIAR

Dacă inițial sectorul financiar prezenta o reticență față de FinTech, acesta fiind mai agil și mai puțin constrâns de reglementări, companiile FinTech erau privite ca fiind concurenți perturbatori cu potențial de a răsturna modelele de afaceri existente și de a obține o cotă semnificativă pe piața bancară. Pe parcursul dezvoltării tehnologiilor financiare însă, sectorul financiar a reacționat în timp util, multe instituții financiare făcând echipă cu diverse start-up-uri pentru ași spori eficiența și pentru a avea acces la noi piețe și produse. Totodată, multe companii FinTech au ales să se alăture unor jucători importanți pe piața financiară pentru a avea, la rândul lor, acces direct la piețe deja formate, dar și la finanțare la costuri minime prin intermediului unui parteneriat de încredere.

Analiza impactului FinTech asupra sectorului financiar în general, poate fi structurată pe un șir de inovații care stau la baza principalelor modificări și evoluții:

– Industria globală a plăților digitale, la baza cărora stă Sistemul de decontare pe bază brută în timp real (SDBTR), s-a dezvoltat rapid în ultimii ani, aducând pe piață mai multe instrumente, inclusiv plățile mobile P2P și portofele mobile. Potrivit The Fintech Times, valoarea medie a tranzacției per utilizator pe segmentul de plăți mobile din Europa aproape s-a dublat în ultimii trei ani, ajungând la 931 USD în anul 2020, iar statisticile prezintă o dinamică în creștere a acestui indicator și o triplare a valorii lui până în anul 2023 comparativ cu cea înregistrată în 2017 [6]. Totodată, potrivit unui studiu a companiei Deloitte, aproximativ 20% din posesorii conturilor bancare din Orientul Mijlociu utilizează soluții FinTech pentru efectuarea transferurilor P2P [5].

– Digitalizarea informației permite crearea și operarea mai ușoară a piețelor online de capital, unde datele pot fi analizate și procesate la un cost eficient de către participanții care au nevoie de capital, informația fiind ulterior plasată pe platforme relevante pentru potențialii furnizori de capital. În același timp, posibilitatea interacționării exclusiv online cu clienții, permite platformelor online, băncilor virtuale și e-brokerilor să se extindă mai rapid și la costuri semnificativ mai mici decât în condiții tradiționale. Totodată, un impact important îl are și urmărirea comportamentului consumatorilor atât online, cât și offline, prin intermediul aplicațiilor și gadgeturilor inteligente, precum smart ceasuri, mașini, dispozitive casnice.

– Afacerile SaaS și Cloud computing permit instituțiilor financiare să evite cheltuieli considerabile de capital pentru crearea infrastructurilor IT necesare la momentul creării modelului de business sau la etapa extinderii pe noi piețe. Totodată, conexiunea prin Cloud permite transferul de servicii și date între dispozitive: clienții pot beneficia de serviciile financiare prin interfețe precum dispozitive smart, iar instituțiile adună informații relevante despre necesitățile și preferințele clienților.

– Succesul și popularitatea tehnologiei blockchain este datorat răspândirii criptomonedelor, dintre care cea mai cunoscută este bitcoin. Cu toate acestea, datorită combinației dintre puterea tot mai mare de calcul și analiză a datelor sistemelor informatice, consolidarea conectivității în Europa și evoluția constantă a sistemelor de inteligență artificială, potențialul de utilizare a tehnologiei registrelor distribuite nu se limitează doar la criptomonede [4]. O utilizare a acestei tehnologii este reprezentată de crearea Organizațiilor Autonome Distribuite (DAO), care permit executare autonomă, în baza anumitor condiții, prin contracte smart, cu mecanisme inovatoare de guvernanță bazate pe vot direct și consens. Efectul implementării DAO, prin eforturile de excludere a intermedierii, ar putea fi propagat nu doar pe piața de capital de risc, atingând astfel însăși conceptul de societate pe acțiuni și având un impact asupra unor funcții ale guvernului.

– Inteligența artificială schimbă într-un ritm foarte rapid interfețele utilizatorilor Alternative Finance și oferă o gamă largă de instrumente printre care: recunoașterea

amprentelor, facial recognition sau amprenta vocală, care permit gestiunea identității biometrice; chatbots care pot oferi clienților recomandări personalizate; dar și algoritmii pentru analiza nevoilor și formarea modelelor de comportament, sau utilizate pentru credit scoring.

FinTech a deschis calea unor posibilități noi atât pentru furnizorii de servicii financiare, care au obținut acces la noile piețe, cât și pentru consumatorii acestor servicii. Simplul acces al consumatorilor non-bancari la dispozitivelor mobile, a permis industriei FinTech să valorifice segmente de clienți nedeserviți până la acel moment, încurajând și promovând astfel incluziunea financiară.

IMPACTUL FINTECH ASUPRA SECTORULUI BANCAR

Pe parcursul ultimilor ani, și în special în urma crizei economice din 2008, sectorul bancar a trecut și trece în continuare printr-o transformare la nivel global, fiind afectate practic toate aspectele activității, începând cu modelele de business ale băncilor, și terminând cu comportamentul bancar al consumatorilor.

Potrivit Oberlo [8], în întreaga lume există 3,5 miliarde de utilizatori de smartphone-uri, iar tot mai mulți utilizatori ai serviciilor bancare preferă să acceseze aceste servicii direct de pe telefon. Tehnologiile Cloud au contribuit în acest sens la îmbunătățirea semnificativă a experienței utilizatorilor, făcând posibil accesul în timp real la informația financiară, prin intermediul internetului. Totodată, sistemele de tipul SDBTR, de asemenea în timp real, permit efectuarea tranzacțiilor de orice tip: transferuri, deschiderea depozitelor și conturilor de economii, convertirea valutei, etc. Toate aceste servicii sunt oferite clienților băncilor în condiții de siguranță, fiind utilizate tehnologii de criptare, parole de unică folosință, chei electronice, etc.

Dezvoltarea tehnologiilor de plată au un impact echivoc în special în ceea ce ține de transferurile P2P. Pe lângă mediul tradițional, bancar, în care aceste operațiuni se pot desfășura, există noi tendințe care implică companiile FinTech în acest proces, totodată fiind posibilă și eliminarea completă a băncii în calitate de intermediar al unor astfel de tranzacții. Evidențe clare ale acestor transformări cu impact asupra sistemului bancar servesc companii ca Alipay sau WeChat Pay (China), Faster Payments (UK).

Un alt aspect al influenței tehnologiilor noi asupra sistemului bancar poate fi observat la analiza utilizării FinTech pentru remitențe. Astfel, datorită rolului sporit al furnizorilor FinTech, costurile de transmitere a remitențelor este în scădere, în timp de viteza de efectuare a tranzacțiilor este în creștere. Efectul acestor modificări este resimțit, în principal, în țările în dezvoltare, pentru care remitențele reprezintă una din principalele intrări de fonduri [2, p.3].

Există numeroase studii care demonstrează că abordarea FinTech oferă o predicție mai bună asupra probabilității de nerambursare a împrumutului în perioade normale, dar și în cele de șocuri mari exogene [3, p.1]. În comparație cu băncile tradiționale, „băncile virtuale” (cum ar fi MYBank, XW Bank) oferă împrumuturi întreprinderilor care nu au acces la creditarea tradițională. Împrumuturile sunt mai mici și cu o durată mai mică comparativ cu cele ale unei bănci tradiționale, iar rata medie a creditelor neperformante se ridică la circa 2%.

La momentul actual, finanțarea P2P oferă consumatorilor posibilitatea de a alege între contractarea unui împrumut de la o companie FinTech: simplu și într-un timp foarte scurt, însă la un preț mai ridicat și un împrumut tradițional de la o instituție bancară.

În același timp, pentru a face față concurenței, băncile tradiționale, apelând la parteneriate cu companii FinTech, sau dezvoltând propriile tehnologii, și-au regândit

strategiile, au implementat și implementează în continuare noi tehnologii pentru a rămâne eficiente, majorându-și profitul și reducându-și costurile.

Impactul FinTech asupra costurilor este de asemenea important. Reducerea costurilor aferente utilizării Inteligenței artificiale și Machine Learning (ML) în procesarea informației clienților, de utilizare a chatbots pentru înlocuirea treptată parțială sau completă a personalului consultant precum și de diminuare a spațiilor utilizate datorită reducerii numărului de personal necesar ș.a. reprezintă elemente ușor cuantificabile și urmează să încurajeze în continuare modificarea modelelor de business în sectorul bancar.

În general tendința către digitalizare și inovație tehnologică va remodela sectorul financiar global și modul în care companiile financiare interacționează cu clienții lor. Majorarea continuă a numărului dispozitivelor mobile utilizate, precum și creșterea numărului furnizorilor FinTech reprezintă principalele premize pentru această dezvoltare alimentând apariția noilor soluții și produse care ar răspunde mai bine nevoilor clienților, sporind totodată accesibilitatea, viteza și comoditatea. În consecință, așteptările clienților cu privire la serviciile financiare vor continua să crească odată cu dezvoltarea tehnologică în toate domeniile, estimându-se o mare probabilitate ca băncile să nu poată ține pasul cu acestea, decât renunțând la modelele tradiționale de business și orientându-se spre combinarea acestora cu noile tehnologii [2, p.4].

STATISTICI ȘI TENDINȚE FINTECH

Potrivit raportului Statista [7], valoarea totală a investițiilor în companiile FinTech pe parcursul anilor 2010-2019 a prezentat o dinamică generală crescătoare, cu un spor mediu anual de cca 67,8%. În anul 2019, în FinTech au fost realizate investiții în valoare de 135,7 miliarde USD.

Potrivit aceleiași surse, 38% din împrumuturile de consum contractate în anul 2020 în SUA au fost acordate de companii FinTech (date la 31 august 2020), iar în februarie 2020, în SUA erau înregistrate 8775 start-up-uri FinTech, în Europa, Orientul Mijlociu și Africa – 7385 companii, iar în Asia Pacific – 4765. Către anul 2025, se stimează că valoarea globală a împrumuturilor P2P va atinge 1000 miliarde USD.

PRNewswire [9] a estimat că piața mondială a FinTech va ajunge în anul 2022 la 309,98 miliarde USD, cu o rată anuală de creștere de 24,8%.

Potrivit Worldpay research, în anul 2021, cardurile de credit, cardurile de debit și portofelele mobile vor depăși numerarul la toate punctele de vânzări din întreaga lume [10].

Analiza Techtic [11] prezintă șase tendințe în domeniul FinTech pentru 2020-2021:

1. Se anticipează intrarea FinTech în zonele cu provocări financiare reale, întrucât, potrivit unui raport al Băncii Mondiale, aproape 1,7 miliarde de persoane încă nu au acces sau nu fac parte dintr-un sistem financiar.
2. Se prevede o automatizare suplimentară în industria FinTech în scopul optimizării eficienței și reducerii erorilor în seturile de date și în procese.
3. Conform tendinței din celelalte domenii, căutarea vocală s-ar putea infiltra și în sectorul FinTech. În ceea ce privește operațiunile bancare sau financiare, căutarea vocală ar putea fi implementată pentru executarea unor sarcini la obținerea soldurilor, inițierea cererilor, verificarea condițiilor pieței pentru investiții, ș.a.
4. Dat fiind faptul că majoritatea oamenilor preferă conversațiile în scris, FinTech ar putea dezvolta această direcție prin crearea posibilităților de mesagerie chatbot, comunicarea prin e-mail sau mesaje text.
5. Se anticipează majorarea tendinței de utilizare a portofelelor digitale, întrucât utilizarea acestora este simplă și nu se limitează la utilizarea pe o singură platformă.

6. Optimizarea securității digitale va rămâne a fi o prioritate pentru FinTech, întrucât acestea operează cu date sensibile și cu caracter personal, care necesită a fi protejate cu mare strictețe.

CONCLUZII

Tehnologiile financiare, reprezentând unul dintre cele mai captivante domenii din afacerile globale de azi, prezintă totodată industria cu cel mai înalt ritm de creștere, ritmul anual depășind 60 la sută. Într-un timp destul de restrâns, de doar puțin peste un deceniu, industria Fintech a schimbat modul în care oamenii se gândesc la bani și la schimbul de valoare în timp real.

Companiile FinTech au ajuns astăzi la cârma industriei financiare, creând o gamă largă de produse și servicii financiare noi, cu scopul de a face gestionarea banilor mai ușoară și mai eficientă. Accesul la fonduri a devenit mult mai transparent și descentralizat, iar pe lângă metodele tradiționale de finanțare prin împrumuturi și credite ipotecare, consumatorii au acum acces la surse alternative precum finanțarea participativă și împrumuturile P2P. Iar utilizarea inteligenței artificiale și ML permite tranzacționarea algoritmică sau automată la burse.

FinTech are un impact global asupra furnizării de servicii financiare. Plățile mobile au constituit un promotor al incluziunii financiare. Analiza în evoluție a structurii pieței financiare demonstrează o sporire a concurenței și eficienței, inducând totodată noi riscuri pentru stabilitatea și integritatea financiară. Ca urmare echilibrarea priorităților politice concurente continuă să reprezinte o provocare cheie. În timp ce apar preocupări privind riscurile sporite pe care le prezintă FinTech, monitorizarea activității acestora în prezent se limitează în continuare doar la activități și entități din perimetrul de reglementare tradițional, fapt ce rezidă în necesitatea modernizării cadrelor de reglementare financiară.

BIBLIOGRAFIE

1. Buckley R., Arner D.W., Barberis J.N. (2016). *The Evolution of Fintech: A New Post-Crisis Paradigm?*. SSRN Electronic Journal, pp.46. Disponibil online: https://www.researchgate.net/publication/313365410_The_Evolution_of_Fintech_A_New_Post-Crisis_Paradigm
2. Cortina J.J., Schmukler S.L. (2018). *The Fintech Revolution: A Threat to Global Banking?* Research & Policiy Briefs No.14, World Bank Chile Center and Malaysia Hub, pp.4
3. Huang Y., Zhang L., Li Z., Qiu H., Sun T., Wang X. (2020). *Fintech Credit Risk Assessment fr SMEs: Evidence from China*. IMF WP/20/193, pp.42
4. *Avizul Comitetului Economic și Social European privind „Tehnologia blockchain și tehnologia registrelor distribuite – infrastructuri ideale pentru economia socială”*. Jurnalul Oficial al Uniunii Europene, C 353/1, 2019. Disponibil online: https://eur-lex.europa.eu/legal-content/RO/TXT/?toc=OJ%3AC%3A2019%3A353%3ATOC&uri=uriserv%3AOJ.C_.2019.353.01.0001.01.RON
5. Faridi O. (2020). *Apps for P2P Money Transfers and Account Aggregation are Most Popular Fintech Solutions in the Middle East: Survey*. Crowdfund Insider. Disponibil online: https://www.crowdfundinsider.com/2020/07/163834-apps-for-p2p-money-transfers-and-account-aggregation-are-most-popular-fintech-solutions-in-the-middle-east-survey/

6. Patel M. (2020). *Digital Payments in Europe to Surpass $802bn Transaction Value This Year, The Fintech Times*. Disponibil online: https://thefintechtimes.com/digital-payments-in-europe-to-surpass-802bn-transaction-value-this-year/
7. https://www.statista.com/
8. https://www.oberlo.com/blog/mobile-usage-statistics
9. https://www.prnewswire.com/
10. https://worldpay.globalpaymentsreport.com/
11. https://www.techtic.com/

Economic Security at the Individual Level

INTERCONNECTION OF PUBLIC HEALTH INFORMATION SYSTEMS FOR THE OPERATIVE MONITORING OF THE PANDEMIC SITUATION IN THE REPUBLIC OF MOLDOVA

Oprea Serghei
PhD, Associate Professor
Academy of Economic Studies of Moldova
e-mail: opreaserghei@ase.md

Abstract
The paper examines the current situation in the field of operational monitoring and reporting of cases of SARS-Cov-2 infection in the Republic of Moldova. The existing problems of this process, mostly performed in manual mode, are highlighted. It mentions the unnecessary waste of time by the doctors involved in the fight with COVID-19 for the manual completion of the daily reports sent for centralization to the hierarchically superior medical organizations. The main information systems used in the field of public health in the Republic of Moldova are reviewed and their basic functionality is mentioned. The lack of a centralized information system for collecting and processing primary medical data, necessary for operational and strategic decisions by the central administration, is accentuated. It is proposed the concept of interconnection of medical information systems and profile databases through the automated information system of primary health care and the creation within this system of a subsystem for monitoring and reporting the epidemiological situation in the Republic of Moldova.

Keywords: *health information systems, operative monitoring, pandemic situation.*

JEL Classification: *L86, I13*

INTRODUCTION

In the field of public health in the Republic of Moldova, a series of medical information systems are implemented to record the services provided to the population of the republic.

The National Health Insurance Company (NHIC) registers the citizens included in the Compulsory Health Insurance System (CHIS) in the database "**Register of persons insured in the system of compulsory health insurance**". This database is organized in accordance with legal requirements and is a component part of the automated information system "Compulsory Health Insurance". An insurance number is assigned to the person registered in the "Register of persons insured in the compulsory health insurance system". The records in the "Register of persons insured in the compulsory health insurance system" are made on the basis of the state identification number (IDNP) or the series and number of the valid identity card in the national passport system, for persons who do not have IDNP, and of the number of compulsory health insurance. The status of insured person is verified by querying the automated information system "**Compulsory health care insurance**" by accessing the official website of the NHIC (**http://vsa.cnam.gov.md/app/verify/**)

The NHIC information system has a reduced functionality for citizens: the status of insured person in the field of compulsory health insurance is checked or the registration of the family medicine is checked. In the latter case, the citizen obtains information about the public health medical institution to which he is affiliated, registration data and the name of the family doctor.

The automated information system "**Reporting and evidence of medical services**" (AISREMS) ensures the real-time monitoring of the provision of medical services and the reporting of data to the National Health Insurance Company. Within AISREMS, doctors can identify the person in the NHIC database, check their insured or uninsured status, and in the case of the insured patient - fill in the referral ticket online for medical services. Through the system it is possible to make online appointments at medical services, accessing the link **https://sirsm.cnam.gov.md**. The database is continuously updated with information on medical services prescribed to patients by doctors, appointments made by doctors and patients, the number and volume of services contracted and the real-time execution of services in accordance with the contract with the medical institution. The stored information is used to prepare synthesis and analysis reports.

Territorial Medical Associations (TMA) use both the NHIC information system and the automated information system "Primary Health Care" (AISPHC) (**https://sia.amp.md/**). AISPHC allows the computerization of the activities of the medical, administrative and management staff within the health units, the evidence, the control and the automated coordination of the activity of the basic subdivisions of the public medical institution of the Primary Health Care, as well as the accumulation of information necessary for decision making and data processing, including those related to the health status of the beneficiaries of medical services. In the automated system are stored and processed personal data of citizens, such as: IDNP, name, surname, patronymic, date of birth, sex, citizenship, blood type, health insurance number, education, job, position, profession, type and number of identity document, patient's mobile phone, email, number of children, marital status, medical file number.

For this reason, the authentication of doctors in the AISPHC is possible by using the government service **MPass** (**https://sia.amp.md/siaamp**/) by electronic signature, mobile signature or electronic identity card. The functionality of the automated information system "Primary Health Care" is described in the AISPHC User Manual [1].

RESULTS AND DISCUSSIONS

Along with the medical-organizational activities for monitoring the situation with the spread of COVID-19 on the territory of the Republic of Moldova, the Ministry of Health, Labor and Social Protection developed a series of prevention and control measures, stipulated in a series of orders issued.

Thus, in order no. 213 of March 2, 2020 [2] was approved the Bulletin accompanying the biological sample for the detection of SARS-Cov-2 virus (COVID-19) (hereinafter Accompanying Bulletin) and the WHO Provisional Form for reporting probable and confirmed cases of Covid-19 infection (hereinafter WHO Provisional Form).

Analyzing the structure of the Bulletin accompanying the biological sample for the detection of SARS-Cov-2 virus (COVID-19) we can see the following moments:

1. The accompanying bulletin contains 41 positions, is filled in **manually** by the ascertaining doctor, is signed and initialed in the same way **manually**.
2. Sender information to be filled in **manually** each time
3. The information with the patient's personal data is filled in **manually**
4. The patient's travel data and border transit data shall also be completed **manually**.

As concrete proposals for solving the moments set out above it can be mentioned:

- Elaboration within the AISPHC (sia.amp.md) of **an informational subsystem for monitoring the epidemiological situation** in the territory, **interconnected** with other government information systems and profile databases;

- Design within the information subsystem for monitoring the epidemiological situation in the territory of **Web interfaces** for the **collection of primary medical data** about patients and their storage in the database.
- Development of a **Web interface** for the **automatic generation of statistical forms and reports** necessary for real-time monitoring of the situation in the territories and centralization of statistical data.
- Using the **electronic signature** to identify the doctor and authorizing the document developed in the AISPHC;
- Implementation of the functionality of **automated completion of routine data** from forms (date of completion, time of dispatch, medical institution, etc.)
- **Retrieving personal data** by using the **specialized bulletin scanning technique** and obtaining personal data from **interconnected databases** (NHIC database, Border Police database, etc.)
- **Retrieving patient travel data** from the Border Police database.
- **Automatic transmission of data** to the authorized medical institutions of the National Agency for Public Health (NAPH)
- **Automated evidence** of suspicious and confirmed cases and transmission of related information to the Territorial Medical Associations and family doctors concerned (depending on the patient's place of residence).
- **Automatic generation** of **daily reports** of suspected or confirmed cases of disease in the territories.

For example, the practical implementation of the above recommendations would reduce in only one form of the Accompanying Bulletin the number of positions to be filled from 41 to 17 (all ticked), considerably **reducing the time** taken to complete the document.

Likewise, the completion of the WHO Provisional Form by the responsible worker of the National Agency for Public Health provides for the manual completion of at least 94 positions. Most of the positions to be filled are ticked (confirmation of an election), however, there is a series of positions, which could be filled in automatically:

- Patient information can be filled in automatically from the NHIC or AISPHC databases.
- The clinical information can be filled in automatically from the AISPHC database, using the data entered by the family doctor when taking the case for monitoring or from the computer systems of the hospitals from the patient's electronic file.
- Information regarding the patient's travel can be partially completed with the data taken from the Border Police database and from the AISPHC database, entered by the family doctor when taking the case for monitoring.
- Laboratory information may be completed automatically with the response sent by the specialized laboratory for the detection of SARS-Cov-2 virus (COVID-19).

CONCLUSIONS

In the orders of the Ministry of Health, Labor and Social Protection no. 294 of 20.03.2020 [3] and no. 389 of 10.04.2020 [4], **5 forms** of reporting are specified, which are currently completed manually by the competent bodies and are sent in the form of Excel files for centralization to the higher hierarchical bodies, where they are processed in the same way manually. The waste of the doctor's working time to complete a documentation leads to a drastic decrease in the efficiency of the actual medical act, the doctor being obliged to perform routine activities and not to treat the patient. In this context, the maximum reduction of the time for completing the medical documentation and the

automatic generation of statistical forms and reports becomes a primary priority for the public health system of the Republic of Moldova.

The development within the AISPHC of an information subsystem for monitoring the epidemiological situation in the territory would solve the problem of **reporting and centralizing statistical data** on the current situation in the territories. The numerical fields in these reports contain aggregation values, which can be obtained automatically by querying the AISPHC database, cardinally reducing the number of hours worked unnecessarily to complete momentary documents with volatile operating data. It will also increase the efficiency of crisis reporting and increase the objectivity of operational data, necessary to make a correct operative and strategic decisions.

The idea of interconnection and interoperability of medical information systems **can be extended over time to the national level** by creating an information system for monitoring the epidemiological situation in the Republic of Moldova, connected to medical and government information systems on a common computer platform. The **MCloud** information platform (https://stisc.gov.md/ro/content/mcloud) could serve as a platform for implementing the future information system for monitoring the epidemiological situation. The **MCloud** platform is a common government information infrastructure, which operates on the basis of "cloud computing" technology, hosted in the consolidated infrastructure of data centers. The platform is a model for the provision of IT services, through the telecommunications system of public administration authorities, as well as through public communications networks, exclusively through secure data access and transport channels. The **MCloud** platform is used exclusively by central administrative authorities and organizational structures within their sphere of competence, subordinated to the Government.

The **MConnect** interoperability platform can be used as an integration platform for various information systems within an information subsystem for monitoring the epidemiological situation (https://mconnect.gov.md/#/)

BIBLIOGRAPHY

1. *Manual de utilizare SIA AMP. Medic de familie*. (2018). Available at: http://www.cnam.md/httpdocs/editorDir/file/book/mf.pdf
2. *Ordinul nr. 213 din 02 martie 2020 "Cu privire la măsurile de prevenire și control al infecției cu Coronavirusul de tip nou (COVID-l9)".* Available at: https://msmps.gov.md/sites/default/files/legislatie/ordin_nr_213_din_02.03.2020.pdf
3. *Ordinul nr. 294 din 20 martie 2020 "Cu privire la realizarea misurilor de evidență și raportare a datelor privind COVID-I9".* Available at: https://msmps.gov.md/sites/default/files/legislatie/ordin_nr._294_din_20.03.2020-_cu_privire_la_realizarea_masurilor_de_evidenta_si_raportare_a_datelor_privind_covid-_19.pdf
4. *Ordinul nr. 389 din 10 aprilie 2020 "Cu privire la realizarea măsurilor de evidență și raportare a datelor privind tratamentul la domiciliu a pacienfilor cu forme usoare a infecției cu COVID-l9 și numărul de persoane care au beneficiat de asistență medicală în Centrul COVID-l9"* Available at: https://msmps.gov.md/sites/default/files/legislatie/ordinul_nr._389_din_10.04.2020_cu_privire_la_realizarea_misurilor_de_evidenta_si_raportare_a_datelor_privind_tratamentul_la_domiciliu_a_pacientilor_cu_forme_usoare_a_infectiei_cu_covid-19.pdf

DIGITAL TRANSFORMATION VIEWPOINTS IN THE CONTEXT OF HUMAN DEVELOPMENT AT THE HOUSEHOLD AND INDIVIDUAL LEVEL

ВЗГЛЯД НА ЦИФРОВУЮ ТРАНСФОРМАЦИЮ В КОНТЕКСТЕ РАЗВИТИЯ ЧЕЛОВЕЧЕСКОГО ПОТЕНЦИАЛА НА УРОВНЕ ДОМОХОЗЯЙСТВА И ЛИЧНОСТИ

Ишмухаметов Наиль
Кандидат экономических наук, доцент
Башкирский государственный университет
e-mail: IshmukhametovNS@bashedu.ru

Abstract
The article deals with the phenomena of digital transformation and the network economy, as well as the issues of their impact on the processes of human development of households and individuals in modern conditions. The paper proposes two aspects of the analysis of digital transformation: in relation to the concepts of "digitization" and "digitalization", as well as a system of new institutions formed due to the processes of automatization, robotization, informatization, networkization, digitalization, and artificial intelligence technologies. It is concluded that network technologies create an institution of network space, which exists with its own "rules of the game" and mechanisms that ensure the implementation of these rules. At the same time, an important addition to network technologies can be the institute of artificial intelligent systems, including intelligent information security systems. The role of the "Internet of things" as a concept of network space is noted. The concept of "network household" is proposed as a virtual assembly of households that physically exist in different spatial coordinates to perform part of the traditional functions of households. The key problems of human potential development at the household and individual levels are highlighted: ultra-fast depreciation of knowledge potential, both in the professional sphere in the labor markets and in the consumer knowledge sector, technological and social aspects of digital transformation, new "growth points" in the digital economy. It is noted that under the influence of digital transformation, the education system itself and the content of the education process are changing, and at the same time, the modern student is changing, who is more ready for distance online learning than those who studied many years ago. A brief analysis of the penetration of digital technologies at the household level and the development of digital skills and competencies at the personal level is carried out.

Keywords: *digital transformation, digital economy, network economy, human development, household, individual, digital competencies.*

JEL Classification: *D10, D13, D19*

ВВЕДЕНИЕ

Цифровая трансформация есть современная тема серьезных дискуссий как в обществе в целом, так и в научных кругах, и в сообществах узких специалистов по различным направлениям цифровизации промышленности и других секторов экономики. В обсуждении понятия «цифровая трансформация» важными представляются, как минимум, два аспекта данного феномена:

1) Выход исследователя на понятие цифровой трансформации во взаимосвязи с такими узкоспециализированными и технически связанными понятиями, как «оцифровка» (Digitization) и «цифровизация» (Digitalization);

2) Взгляд на цифровую трансформацию как систему новых институтов, формирующихся ввиду исторически обусловленной последовательности процессов автоматизации (automatization), роботизации (robotization), информатизации (informatization), сетевизации (networkization) и цифровизации вкупе с повсеместным проникновением технологий искусственного интеллекта (AI, artificial intelligence).

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

По первому аспекту, логика которого отражена на рис. 1, не всегда правильно понимается не только цифровая трансформация, но и цифровизация, которую понятийно применяют к процессам оцифровки и информатизации. Не секрет, что многие представители бизнеса и правительственных структур ошибочно полагают, что процессы оцифровки автоматически приведут к цифровизации, а впоследствии – к цифровой трансформации. Таким образом, на первых порах возникает вполне практическая задача по закреплению однозначного понимания этих понятий для формирования так называемого цифрового мышления (digital mindset) [2].

Рисунок 1. Понятие цифровой трансформации во взаимосвязи с понятиями «оцифровка» и «цифровизация»

Значимость нового типа мышления можно, в частности, объяснить тем, что цифровая трансформация требует повсеместного проникновения цифровых технологий и соответствующих социокультурных изменений. Цифровая трансформация в большей степени связана с развитием человека, чем с развитием цифровых технологий, проникая в мыслительную деятельность человека, отражаясь на расширяющихся возможностях человеческого капитала. Это отражение находит свой отклик, прежде всего, в потребительской стороне жизнедеятельности современного человека, поскольку, на наш взгляд, тренды движения глобальной экономики таковы, что человек в долгосрочной перспективе будет всё больше времени проводить в потреблении, потребительской активности, а не в производстве и производственной деятельности [9].

Уже сегодня с экономической точки зрения человек интересен в первую очередь как потребитель, занятость которого и источники доходов становятся вторичными факторами. Свидетельством тому является широкая научно-практическая дискуссия, которая развернулась в мировой экономической науке и социологии вокруг концепции универсального базового дохода, и говорит о смене парадигмы «экзистенциальной формулы» обеспечения базовых потребностей человека в его жизнедеятельности, в том числе экономической.

Возрастающее значение человека-потребителя отнюдь не значит отсутствие важности социокультурных изменений для сферы производства. Действительность заключается в том, что современное производство – это во многом производство с минимальным присутствием человека не только в роли производственного рабочего основного и вспомогательного состава, но и как служащего. Организационные изменения бизнеса таковы, что по ряду специальностей человек-сотрудник выталкивается из сферы непосредственно производства в сферу обращения, ориентированную на клиента, но и здесь процессы цифровой трансформации и технологии искусственного интеллекта показывают впечатляющий потенциал заменимости человека на чат-боты, коботы и т.п. Сетевизация производства в значительной степени задает тренды глобальной конкурентоспособности стран, их

участия в глобальных цепочках создания стоимости и «интеграции в глобальные производственные сети и цепочки создания стоимости» [1].

По второму аспекту хотелось бы отметить особую роль сетевизации экономики и других сфер, где технологическая сторона цифровой трансформации выводит на первое место сетевые технологии как основу цифровизации. Речь идет, к примеру, о технологии «интернета вещей» (англ. Internet of Things, IoT) как концепции сетевого пространства, соединяющего физические объекты реального мира друг с другом и с виртуальными объектами цифрового мира с целью установления сетевого взаимодействия между ними и/или с внешней средой. Что характерно, результатом реализации этой концепции на практике исследователи видят такие технико-экономические изменения, которые также позволяют минимизировать присутствие человека или исключить его из цепочки операций.

На наш взгляд, процессы сетевизации приведут к возникновению феномена «сетевых домохозяйств» и сетевого поведения индивидов. Представляется, что «сетевое домохозяйство» есть некая виртуальная точка сборки домохозяйств, физически существующих в разных пространственных координатах (в других жилищах, населенных пунктах, странах) для выполнения некоторой части традиционных функций этих домохозяйств. Например, функции удаленной (дистанционной) помощи в обучении, воспитании, психологической помощи, социальной работе усилиями членов одного домохозяйства для членов другого.

Некие примитивные формы такого взаимодействия можно наблюдать и сегодня, но для качественно нового уровня сетевизации, включая виртуальную (VR) и дополненную (AR) реальность, тактильный интернет, требуются технологии связи пятого поколения, 5G. При этом немаловажными останутся общие цифровые навыки домохозяйств и индивидов в составе их человеческого капитала, в особенности для формирования и развития «цифровой культуры» и обеспечения цифровой и информационной безопасности. С начала 2020 года «ситуация с проникновением сетевых технологий в сферу потребления в корне изменилась и, по всей видимости, будет изменяться и дальше. Можно сказать, что пандемия здесь выступила своеобразным триггером тех процессов, которые в долгосрочной перспективе повлекут за собой смену существующего технологического уклада и, как следствие, кардинальные изменения в структуре потребительского рынка» [8].

Таким образом, взгляд на цифровую трансформацию как систему новых институтов позволяет сделать промежуточный вывод: сетевые технологии создают институт сетевого пространства, который, как и любой другой институт, существует со своими «правилами игры» и механизмами, обеспечивающими выполнение этих правил. Альтернативный взгляд на сущность института дает возможность при определенных обстоятельствах трактовать институт как поведение сетевых участников внутри сетевого пространства, задающего неформальные ограничения и формальные правила такого поведения.

В контексте развития человеческого потенциала не менее значимым представляется институт искусственных интеллектуальных систем, которые способны стать важным дополнением к сетевым технологиям, включая интеллектуальные системы информационной безопасности. Перспективным для применения не только в сфере бизнеса, но и на уровне домохозяйств и даже индивидов, видится соединение систем искусственного интеллекта с облачными технологиями по типу проекта Watson от IBM.

Переходя к актуальным вопросам развития человеческого потенциала домохозяйств в контексте цифровой трансформации, следует заметить, что «режим

самоизоляции, массовый переход на дистанционное обучение в период пандемии показали всю важность развития не только технологического, но и социального фундамента цифровизации: многие домохозяйства не могут быстро перестроиться с точки зрения не только трудовых, но и потребительских навыков» [8]. При этом неравенство домохозяйств по доходам усиливает неравенство «цифровых» возможностей. «Задолго до пандемии коронавируса технологические решения в области сетевизации получили распространение в экономике, оказывая влияние на ограниченную часть потребительского сектора, прежде всего, в точках пересечения тех интересов индивидуальных потребителей и домохозяйств, которые были связаны с инновациями, интернет-технологиями и информационными системами» [8], то есть «информационно продвинутых» потребителей и домохозяйств.

По нашему мнению, сетевые услуги представляют собой новую «точку роста» в цифровой экономике, которая способна обеспечить развитие как традиционного сектора промышленности, так и сектора услуг в виде сервисной отрасли в сетевом пространстве экономики. Это можно объяснить тем, что «сетевые услуги в своей сущности материальны в той части, где начинают свой путь к потребителю (материальную основу составляют сетевое оборудование, линии связи и т.п.), и нематериальны в той части, где соединяются с каким-либо нематериальным сетевым благом – к примеру, «облаком» в сети как результатом соединения виртуальной среды с удалённым доступом и онлайн-хранилищами данных» [8].

При этом американская компания International Data Corporation (IDC) прогнозирует, что глобальная сфера данных вырастет с 33 зеттабайт в 2018 году до 175 зеттабайт к 2025 году [4, с. 3]. Вместе с тем, некоторой частью наблюдателей высказывается скепсис относительно качества этих данных и опасение, что человечество будет в большей степени наращивать генерацию «цифрового мусора».

Специфика отношений в новой экономике такова, что возникает проблема измерения ценности не только массива данных, но и обработанной информации, а также контента, восприятие ценности которого может изменяться в зависимости от текущей конъюнктуры на данном рынке. Кроме того, «к цепочкам формирования добавленной стоимости в их денежном измерении может добавляться параллельная цепь неденежных измерителей выгод и издержек для производителей и потребителей». По сути, в процессе цифровой трансформации усугубляется проблема измерения ценности как традиционных, так и новых товаров и услуг, что приводит к появлению альтернативных измерителей ценности благ, включая эмоциональные, например, так называемые лайки (англ. like), как инструмент, позволяющий оперативно измерить потребительское одобрение услуг [3].

Еще одной ключевой проблемой развития человеческого потенциала мы считаем сверхбыстрое обесценение потенциала знаний, как в профессиональной сфере на рынках труда, так и в потребительском секторе знаний. В исследовании «Атлас новых профессий» эксперты прогнозируют, что до 2030 года исчезнут 57 профессий, и появятся 186 новых профессий [1]. Как следствие, практически каждый человек в роли наемного работника должен принять для себя и использовать на практике принципы «lifelong learning», обучения на протяжении жизни, т.е. непрерывного образования. Однако собственно человеческий потенциал, и прежде всего потенциал мотивации отдельно взятого индивида является здесь ограничительным фактором распространения этих принципов на практике. Многие проблемы современного человека лежат в русле тайм-менеджмента и выбора приоритетов личностного развития, когда внешние обстоятельства вроде бы подталкивают к гибкости и принятию перемен, но человек теряется в изобилии

информационных источников и возможностей. Другое дело, когда обучение рассматривается индивидом как осознанная потребность, и он следует скорее внутренней мотивации, а не внешним обстоятельствам. Необходимо отметить, что под воздействием цифровой трансформации меняется также сама система образования и содержание процесса образования, и вместе с этим меняется современный обучающийся – он в большей степени готов к дистанционному онлайн-обучению, чем обучавшиеся 5-10 лет назад.

Результаты цифровой трансформации – это не только онлайн-образование и новые способы обмена информацией, эмоциями и прочим контентом, но и расширение возможностей реализации человеческого капитала в онлайн-пространстве благодаря наличию цифровых навыков и компетенции. В исследовании «Цифровые навыки и компетенция, цифровое и онлайн обучение» отмечается, что «в ЕС по-прежнему явно ощущается нехватка цифровых навыков и компетенции: при том, что 90 % профессий сегодня требуют некоторого уровня цифровых навыков и компетенции, почти половина (44%) европейских работников обладают лишь базовыми цифровыми навыками, а у 22% из них такие навыки отсутствуют вовсе» [7, с. 6]. Европейским странам, безусловно, следует обратить на этот аспект пристальное внимание, учитывая, что по показателю проникновения интернета, рассчитанного исходя из доли охваченного населения, Европа занимает второе место в мире (87.2%) после Северной Америки (90.3%), тогда как наибольший прирост показывают другие континенты мира.

ВЫВОДЫ

В качестве вывода можно отметить, что современные условия развития человеческого потенциала заданы факторами цифровой трансформации и, прежде всего, фактором сетевизации экономики, претендуя на роль новых «точек роста» мировой экономики. Появление и развитие новых точек роста в экономике связано с качеством ее человеческого потенциала и уровнем цифровых навыков населения.

Текущие процессы цифровизации на базе развития сетевого пространства экономики необходимо анализировать с учетом тех возможностей и ограничений, которые они предоставляют на уровне домохозяйства и личности, в том числе с точки зрения технологических и социальных аспектов цифровизации. Рост научного интереса к цифровой трансформации в ближайшем будущем будет в значительной степени обусловлен возможностями развития человеческого потенциала на уровне домохозяйства и личности, и в перспективе – на уровне «сетевых домохозяйств».

БИБЛИОГРАФИЯ

1. Antoniuk L.L., Cherkas N.I. Global Economic Networkization in the Competitive Growth of Countries. IEP, 31, 2019, pp.82–100. Available at: http://iepjournal.com/journals_eng/31/2019_3_Antonyuk_Cherkas.pdf.
2. Chapco-Wade, C. Digitization, Digitalization, and Digital Transformation: What's the Difference? Medium. Available at: https://medium.com/@colleenchapco/digitization-digitalization-and-digital-transformation-whats-the-difference-eff1d002fbdf.
3. John L.K., Mochon D., Emrich O., Schwartz J. What's the Value of a Like? Harvard Business Review. March–April, 2017 Issue. Available at: https://hbr.org/2017/03/whats-the-value-of-a-like.

4. Reinsel D., Gantz J., Rydning J. The Digitization of the World from Edge to Core. An IDC White Paper. November, 2018 Available at: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-dataage-whitepaper.pdf.
5. World Internet Users Statistics and 2020 World Population Stats. Internet World Stats. Available at: https://www.internetworldstats.com/stats.htm.
6. Атлас новых профессий. Available at: http://atlas100.ru/index/.
7. Брольпито А. Цифровые навыки и компетенция, цифровое и онлайн обучение. Европейский фонд образования, Турин, 2019. Available at: https://www.etf.europa.eu/sites/default/files/2019-08/dsc_and_dol_ru_0.pdf.
8. Ишмухаметов Н.С. Воздействие цифровизации на потребительское поведение домохозяйств в современных условиях // Экономика и управление: научно-практический журнал. 2020. № 4 (154). С. 21-25. Available at: https://www.elibrary.ru/item.asp?id=43775371 DOI: 10.34773/EU.2020.4.4
9. Ишмухаметов Н.С. Россинская Г.М. Роль потребительского потенциала и потребительских способностей в формировании человеческого капитала // Евразийский юридический журнал. 2016. № 8 (99). С. 351-353.

ENSURING THE SECURITY OF THE POPULATION THROUGH THE ROUMANIAN PENSION SYSTEM

ASIGURAREA SECURITĂȚII POPULAȚIEI PRIN SISTEMUL DE PENSII AL ROMÂNIEI

Roman Ana Maria
Doctorandă, Universitatea Liberă Internațională din Moldova
e-mail: august_anamaria@yahoo.com

Spînu Ana
Doctor în științe economice, conferențiar universitar
Universitatea Liberă Internațională din Moldova
e-mail: aspinu@ulim.md

Abstract
The actuality of the subject is explained by the fact that in Romania, pensions are the main form of social insurance. The public pension system is based on the principle of solidarity between the generations, and the people who are in activity pay monthly social contributions, the state in turn paying the pensions of those who have left the activity through a redistribution mechanism. The role of the pension system is to transfer resources from the currently active generation to the retired generation. The aim of the research is to identify the benefits of the public pension system in Romania. The main research methods applied to the elaboration of the article are induction, deduction, analysis, synthesis, documentation and observation. As a result of the research, we consider necessary to develop a medium and long term strategy on pension insurance system, the existence of a computerized record in the pension system and the establishment of a system of monitoring, analysis and policies in the field of pensions.

Keywords: *pension system, types of pensions, contribution, social security.*

JEL Classification: *H55*

INTRODUCERE

Pensiile reprezintă modalitatea de restituire a contribuțiilor plătite în perioada de cotizare, sub forma unei cote din venitul înlocuit, determinată pe baza metodei de calcul specifică fiecărei țări, a algoritmului și formulei de calcul stabilite prin lege în funcție de principii și criterii naționale și universale.

Potrivit Dicționarului Explicativ al Limbii Române, pensia este definită ca sumă de bani acordată lunar persoanelor care au ieșit din producție pentru limită de vârstă sau pentru invaliditate, precum și urmașilor acestor, în cazurile prevăzute de lege [2].

Conform ramurilor securității sociale, pensiile pot fi de următoarele tipuri: de bătrânețe (limită de vârstă); anticipate (parțial anticipate); de invaliditate și de urmaș. Aceste tipuri de pensii sunt în concordanță cu riscurile acoperite și sunt administrate prin sistemul asigurărilor sociale. Pentru a evalua și previziona nivelurile pensiilor trebuie avute în vedere cele două procedure principale de calcul: stabilirea pensiilor și actualizarea pensiilor. Acestea sunt procedure permanente. Stabilirea pensiilor constă în calculul pensiilor pentru noii intrați în system prin pensionare, iar actualizarea este procedura de ajustare a pensiilor deja stabilite la valori actuale.

CONSIDERAȚII GENERALE

Pensiile constituie principala formă de ocrotire a cetățenilor prin asigurările sociale.

În România, cuantumul fondurilor asigurărilor sociale de stat depinde, în principal, de mărimea veniturilor realizate de personalul încadrat în muncă, deoarece agenții economici și instituțiile publice plătesc contribuțiile pentru asigurările sociale în funcție de aceste venituri. Sursele de constituire a fondurilor asigurărilor sociale sunt:

- Contribuțiile pentru asigurările sociale de stat;
- Contribuțiile pentru asigurările sociale datorate de unitățile particulare bazate pe libera inițiativă;
- Contribuția salariaților și pensionarilor care merg la tratament și odihnă;
- Contribuția pentru pensia suplimentară;
- Alte venituri.

Ca urmare a sistematizării concepțiilor autorului [1, p.41] și în baza reglementărilor în vigoare, constatăm că la baza stabilirii dreptului la pensie se află câteva principii, și anume:

a) Imbunătățirea raportului dintre pensie și salariul tarifar, adică realizarea unei corelări juste între nivelul pensiilor și cel al salariilor; acest principiu stimulează perfecționarea pregătirii angajaților și creșterea aportului la dezvoltarea economico-socială a țării;

b) Echitatea socială, adică pensiile sunt stabilite în concordanță cu contribuția fiecărui cetățean la dezvoltarea economico-socială a țării, realizând, în același timp, un raport echitabil între veniturile care provin din salariu și cele care se obțin din pensie, astfel încât să se asigure stimularea persoanelor care lucrează în diferite domenii economice, sociale, culturale etc., precum și realizarea unor proporții echitabile între diferite categorii de pensii;

c) Solidaritatea socială, potrivit căruia participanții la sistemul public de pensii își asumă reciproc obligații și beneficiază de drepturi pentru prevenirea, limitarea sau înlăturarea riscurilor sociale;

d) Egalitatea socială, care garantează tuturor participanților la sistemul public de pensii, contribuabili și beneficiari, un tratament nediscriminatoriu în ceea ce privește drepturile și obligațiile reglementate de lege;

e) Fondurile bănești necesare plății pensiilor se formează din contribuțiile agenților economici, ale instituțiilor, ale salariaților, ale întreprinzătorilor particulari și ale cetățenilor;

f) Stimularea realizării unei vechimi cât mai mari în muncă;

g) Determinarea cuantumului pensiile în funcție, în primul rând, de condițiile existente la locul de muncă;

h) Justa corelare a pensiei de invaliditate cu pensia pentru munca depusă și limită de vârstă;

i) Unicitatea pensiei constă în faptul că o persoană poate primi o singură pensie de bază integrală de asigurări sociale; dacă aceeași persoană este îndreptățită să primească două sau mai multe pensii de bază, ea poate opta oricând pentru una dintre ele;

j) Neimpozabilitatea pensiilor până la un anumit nivel, conform căruia pensiile, în acest moment, potrivit Codului Fiscal aprobat prin Legea nr. 227/2015, modificat, începând cu 01 ianuarie 2018 pentru veniturile din pensii se plătește un impozit care se calculează în procent de 10% pentru sumele care rezultă prin deducerea din valoarea pensiei a sumei de 2000 lei [3];

k) Imprescribilitatea dreptului la pensie, potrivit căruia orice persoană care îndeplinește condițiile legale pentru a primi o pensie poare oricând să ceară înscrierea la

pensie, oricât timp ar fi trecut de la naşterea dreptului la pensie, ceea ce nu duce la decăderea din acest drept pentru viitor;

l) Incesibilitatea dreptului la pensie, potrivit căruia dreptul la pensie nu poate fi cedat nici total, nici parțial; acest principiu se întemeiază pe considerentul uman că primirea pensiei este un drept personal menit să asigure pensionarului condiții materiale și spirituale decente de trai; după încasarea în fiecare lună a pensiei, nimic nu-l poate împiedica însă pe pensionar să doneze pensia în parte sau integral unei alte persoane;

m) Indexarea, majorarea și recorelarea pensiilor. În condițiile manifestării procesului inflaționist din economia românească pe fundalul liberalizării prețurilor, au fost luate măsuri pentru indexarea, majorarea periodică și recorelarea tuturor categoriilor de pensii. Datorită inflației invariabile și galopante, indexările și majorările pensiilor nu au ținut pasul cu creșterea prețurilor.

Apreciem că ar fi necesar ca la fiecare indexare a pensiilor să se aibă în vedere cel puțin următoarele elemente: rata reală a inflației comparativ cu perioadele anterioare; păstrarea unui raport constant între pensia medie și salariul mediu; actualizarea pensiilor pe baza salariilor curente; stabilirea unui cadrul legal de indexare automată a pensiilor atunci când prețurile și rata inflației depășesc un anumit prag; corectarea periodică a coeficienților de indexare. Până în prezent, cu fiecare indexare, pensiile, ca și salariile reale, au rămas mereu în urmă față de creșterea prețurilor.

Statul român garantează dreptul la pensie al fiecărui cetățean, indiferent de sex și naționalitate, și acordă sprijin material prin asistența socială persoanelor inapte de muncă și lipsite de mijloace de existență.

Prin asigurările sociale de stat se acordă următoarele pensii: pensia pentru munca depusă și limita de vârstă; pensia de invaliditate; pensia anticipată; pensia anticipată parțială; pensia de urmaș.

În cazul pensiilor, principala metodă de estimare este metoda modelului de regresie pe baza factorilor de influență, corelată cu metod normativă. Pentru elaborarea modelului de regresie o primă etapă este analiza statisticilor descriptive și a histogramelor.

În perioada 1990-2010, pensia medie de asigurări sociale (incluzând și agricultorii) a fost de 176,5 lei, iar valoarea mediană a fost de 72,6 lei. Pe fondul unui proces inflaționist accelerat înregistrat începând cu anul 1991, statisticile descriptive nu oferă o imagine a evoluției reale a pensiilor pentru munca depusă.

Pensiile de asigurări sociale au crescut linear până în anul 2006. În anul 2008 a început majorarea pensiilor pentru persoanele care au realizat stagii de cotizare în grupe superioare de muncă. Tot în acest an s-a încheiat teoretic procedura de recalculare a pensiilor pentru personale pensionate înainte de aprilie 2001. Procedura de recalculare a prelungită până la sfârșitul anului 2010 cu acordarea drepturilor în cadrul termenului legal de prescripție de 3 ani.

În perioada 2001-2010 pensia medie de asigurări sociale a avut valoarea medie de 396 lei, situată între un nivel minim de 312 lei și un maxim de 778 lei.

În continuare sunt prezentate careva date statistice referitoare la sistemul de pensii al României pentru anul 2019.

Numărul mediu de pensionari a fost de 5157 mii persoane, în scădere cu 50 mii persoane față de anul precedent iar numărul mediu de pensionari de asigurări sociale de stat a fost de 4672 mii persoane, în scădere cu 12 mii persoane faţa de anul precedent;

Pensia medie lunară (determinată luând în calcul sumele pentru pensiile tuturor categoriilor de pensionari - de asigurări sociale, invaliditate, urmaș etc., plătite de casele de pensii, inclusiv sumele plătite pensionarilor de către CNPP, MapN, MAI, SRI, Ministerul

Culturii și Identității Naționale și Casa de Asigurări a Avocaților) a fost de 1292 lei, în creștere cu 10,2% față de anul precedent.

Pensia medie de asigurări sociale de stat a fost de 1247 lei, iar raportul dintre pensia medie nominală netă de asigurări sociale de stat pentru limită de vârstă cu stagiu complet de cotizare (fără impozit și contribuția de asigurări sociale de sănătate) şi câştigul salarial mediu net a fost de 48,4% (comparativ cu 50,9% în anul precedent);

Indicele pensiei medii reale față de anul precedent, calculat ca raport între indicele pensiei nominale pentru calculul pensiei reale şi indicele preţurilor de consum a fost de 105,6% (fig.1).

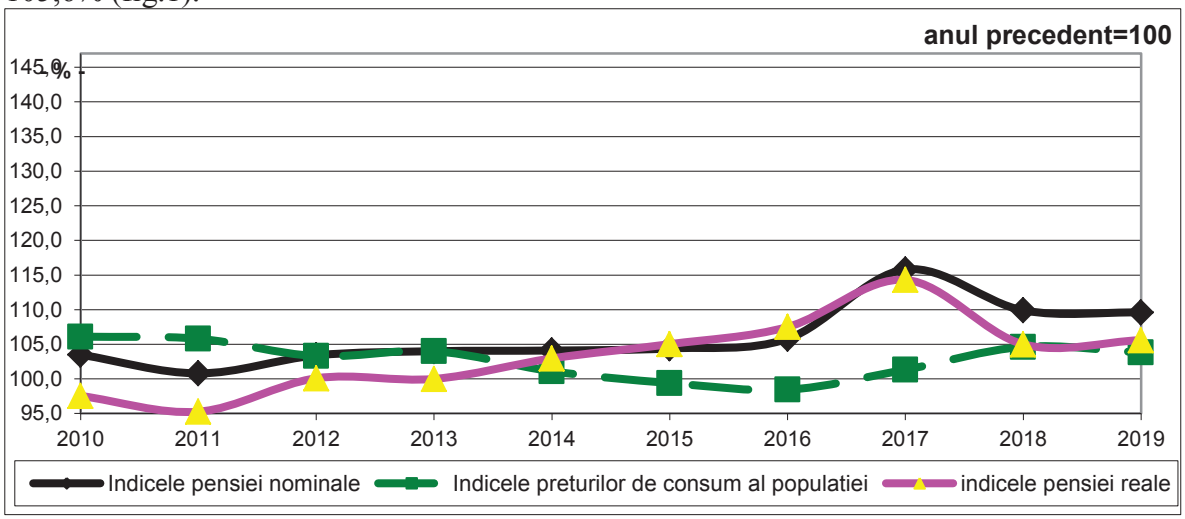


Figura 1. Evoluţia indicelui pensiei nominale şi a indicelui preţurilor de consum în România în perioada 2010-2019

Sursa: https://insse.ro/cms/sites/default/files/com_presa/com_pdf/pensii_2019r.pdf

Evoluția numărului mediu de pensionari și a pensiei medie lunare în anul 2019 comparativ cu anul 2018 este reprezentată în tabelul 1.

Tabelul 1. Numărul mediu al pensionarilor şi pensia medie lunară

	Numărul mediu - mii persoane -		*Pensia medie - lei lunar -*	
	2018	*2019*	*2018*	*2019*
TOTAL	**5207**	**5157**	**1172**	**1292**
din care, după nivelul de pensionare:				
Asigurări sociale	**5204**	**5155**	**1172**	**1293**
din care, de asigurări sociale de stat	4684	4672	1126	1247
din care, asigurări sociale după categorii de pensii:				
A) Limită de vârstă	3993	3992	1321	1453
B) Pensie anticipată	21	19	1349	1511
C) Pensie anticipată parţial	88	92	1022	1179
D) Invaliditate	550	514	641	671
E) Urmaş	552	538	647	710

Sursa: https://insse.ro/cms/sites/default/files/com_presa/com_pdf/pensii_2019r.pdf

Comparativ cu anul precedent numărul mediu de pensionari a scăzut cu 50 mii persoane, iar cel al categoriei aparținând asigurărilor sociale de stat cu 12 mii, iar pensia

medie lunară și pensia medie de asigurări sociale de stat au crescut comparativ cu același an, cu 10,2%, respectiv cu 10,7%.

În anul 2019, pensionarii de asigurări sociale dețin ponderea majoritară (99,9%) în numărul total de pensionari. Pensionarii de asigurări sociale de stat reprezintă 90,6% în totalul celor de asigurări sociale. Pe categorii de pensii, numărul pensionarilor pentru limită de vârstă a fost preponderent (77,4%) în cadrul pensionarilor de asigurări sociale. Pensionarii cuprinși în categoriile de pensii – anticipată şi anticipată parţial - au reprezentat 2,2%.

Raportul pe total dintre numărul mediu de pensionari de asigurări sociale de stat şi cel al salariaților a fost de 9 la 10; acest raport prezintă variații semnificative în profil teritorial.

Numărul total al beneficiarilor conform prevederilor Ordonanței de Urgență a Guvernului nr.6/2009 privind instituirea pensiei sociale minim garantate (în prezent - indemnizație socială), în anul 2019, a fost de 1037,6 mii persoane, din care: 849,6 mii persoane din sistemul asigurărilor sociale de stat, reprezentând 18,2% din totalul pensionarilor din această categorie; 175,4 mii persoane din rândul pensionarilor proveniţi din fostul sistem pentru agricultori, reprezentând 58,8% din totalul acestora; 12,6 mii persoane din sistemul militar, reprezentând 1,8% din totalul acestei categorii.

Pensia medie lunară a înregistrat o ușoară creștere (+0,8%) în trimestrul I 2020 față de trimestrul precedent.

În trimestrul I 2020 numărul mediu de pensionari a fost de 5133 mii persoane, în scădere cu 7 mii persoane față de trimestrul precedent; numărul mediu de pensionari de asigurări sociale de stat a fost de 4670 mii persoane, în creștere cu o mie persoane față de trimestrul precedent; pensia medie lunară (determinată luând în calcul sumele pentru pensiile tuturor categoriilor de pensionari - de asigurări sociale, invaliditate, urmaş etc.- plătite de casele de pensii, inclusiv sumele plătite pensionarilor de către CNPP, MapN, MAI, SRI, Ministerul Culturii și Identității Naționale și Casa de Asigurări a Avocaților) a fost de 1423 lei, în creștere cu 0,8% față de trimestrul precedent; pensia medie de asigurări sociale de stat a fost de 1374 lei, iar raportul dintre pensia medie nominală netă de asigurări sociale de stat pentru limită de vârstă cu stagiu complet de cotizare (fără impozit și contribuția de asigurări sociale de sănătate) şi câştigul salarial mediu net a fost de 50,8% (comparativ cu 51,1% în trimestrul precedent); indicele pensiei medii reale față de trimestrul precedent, calculat ca raport între indicele pensiei nominale pentru calculul pensiei reale şi indicele preţurilor de consum a fost de 99,5%.

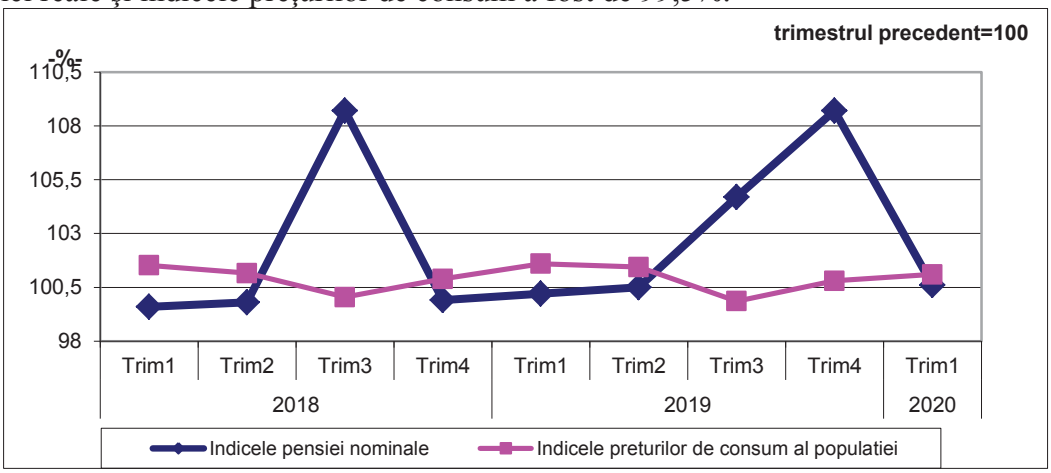


Figura 2. Evoluţia indicelui pensiei nominale şi a indicelui preţurilor de consum în perioada 2018-2020

Sursa: https://insse.ro/cms/sites/default/files/com_presa/com_pdf/pensii_tr1r20.pdf

Dreptul la *pensie de invaliditate* este acordat asiguraților care și-au pierdut total sau cel puțin jumătate din capacitatea de muncă, din cauza accidentelor de muncă, a bolilor profesionale și tuberculozei, a bolilor obișnuite și accidentelor care nu au legătură cu munca.

Acordarea pensiilor de invaliditate este condiționată de producerea cel puțin a unuia dintre aceste riscuri și de regulă și de stagiul de cotizare realizat în raport cu vârsta la care a intervenit riscul de invaliditate.

Cuantumurile pensiilor de invaliditate se stabilesc în funcție de stagiul realizat, de stagiul necesar de cotizare și de tipul de invaliditate în care este încadrat riscul produs.

Există categorii de pensionari de invaliditate care și-au realizat stagiul complet de cotizare, dar la data producerii invalidității nu aveau vârsta pentru a beneficia de pensie pentru limită de vârstă cu stagiul complet de cotizare. Printre aceste categorii de pensionari, pensiile sunt egale cu pensia de limită de vârstă dacă ar fi avut acest drept. În formula de calcul a pensiilor de invaliditate legiuitorul a prevăzut în mod corect compensarea stagiului potențial pe care l-ar fi putut realiza asiguratul dacă nu se producea riscul de invaliditate prin acordarea de punctaje aferente stagiului potențial, diferențiate pe tipuri de invalidități.

Cuantumul mediu al pensiilor de invaliditate era în anul 2005 de 230 lei pentru pensiile de gr. I, 213 lei pentru pensiile de invaliditate e gr. II și 203 lei pentru pensiile de invaliditate de gr. III, corespunzătoare punctajelor medii anuale în baza actualului algoritm de calcul, al pensionărilor categoriilor d asigurați cu stadii potențiale reduse.

La nivelul anului 2010, cuantumurile medii erau de 559 lei, 564 lei și 548 lei. În anul 2018 cuantumul mediu era de 641 lei, iar în anul 2019 era de 671 lei.

Pensiile anticipate se acordă începând din anul 2011 cu cel mult 5 ani înaintea împlinirii vârstei standard de pensionare, persoanelor care au realizat un stagiu de cotizare prevăzut de lege pentru generația din care fac parte. Singurul dezavantaj al pensiilor anticipate este nevalorificarea stagiilor asimilate (armată, studii, alte stagii asimilate), care este o "penalizare" minoră în raport de acordarea pensiei cu 5 ani mai devreme.

Sistarea pensionărilor anticipate pe parcursul anului 2010, a fost recompensată de legiuitor prin reducerea condiției de depășire a stagiului de la 10 ani în plus la 8 ani peste stagiul standard de cotizare. Din analiza comparativă a seriilor de date pe tipuri de pensii se constată situarea acestui tip de pensie cu puțin sub nivelul pensiilor pentru limită de vârstă și vechime complete. La nivelul anului 2010 pensia medie anticipată a crescut la 980 lei față de anul 2005 când se înregistra o valoare medie de 391 lei. In anul 2018 pensia medie anticipată a crescut la 1349 lei, iar în anul 2019 se înregistra la o valoare medie de 1511 lei.

Pensia anticipată parțial se cuvine, cu cel mult 5 ani înaintea împlinirii vârstei standard de pensionare, persoanelor care au realizat stagiul complet de cotizare, precum și celor care au depășit stagiul complet de cotizare cu până la 8 ani. Acest tip de pensie este penalizat începând cu anul 2011 cu diminuarea cuantumului cu 0,75% pentru fiecare lună de anticipare, până la îndeplinirea condițiilor de trecere la categoria de pensie pentru limită de vârstă. Nivelul cuantumurilor acestui tip de pensie de 696 lei cât s-a înregistrat în anul 2010 reflectă aplicarea procentelor de diminuare progresive de la 0,05% pe lună (între 9-10 ani de anticipare) și 0,50% pe lună de anticipare (pentru un stagiu depășit cu până la 1 an). În anul 2018 pensia medie anticipată parțial a crescut la 1022 lei, iar în anul 2019 se înregistra la o valoare medie de 1179 lei.

Pensia de urmaș se acordă copiilor și soțului supraviețuitor în condițiile prevăzute de lege. Cuantumurile scăzute ale pensiilor de urmaș sunt explicate prin faptul că maximum pe care îl poate obține ca pensie urmașul este de 50% din pensia pe care o avea titularul sau la care avea dreptul. În anul 2010 pensia medie de urmaș era de 396 lei ceea

ce situează acest tip de pensie peste jumătate din nivelul mediu al pensiei din sectorul de stat care era de 744 lei în luna decembrie 2010. În anul 2018 pensia medie de urmaș a crescut la 647 lei, iar în anul 2019 se înregistra la o valoare medie de 710 lei.

CONCLUZII

În concluzie constatăm că mecanismul de redistribuire reprezintă un ansamblu care are la bază un set de reguli și principii, în care se utilizează o bază și un tip de finanțare, o formulă de calcul a beneficiilor și care constă în repartizarea beneficiilor în funcție de acestea și în funcție de particularitățile și politicile naționale. Cea mai cunoscută formă de redistribuire din România este transferul inter generațional de resurse, fiind caracteristica principală a sistemelor de pensii publice, ce constă în faptul că generațiile actuale plătesc contribuții pentru pensiile viitoare. În același timp, în prezent, resursele colectate de la salariați și de la alte persoane asigurate în mod individual nu sunt stocate, ci pe calea redistribuirii sunt transformate pensii pentru generațiile actuale de beneficiari. În scopul asigurării securității populației prin sistemul de pensii considerăm oportună elaborarea unei strategii pe termen mediu și lung privind persoanele vârstnice, existența unei evidențe informatizate în sistemul de pensii și înființarea unui sistemul de monitorizare, analiză și politici în sfera pensiilor.

BIBLIOGRAFIE

1. Bistriceanu Gheorghe D. Sistemul asigurărilor din România. București, Editura Economică, 2002, 432 p.
2. Dicționar explicativ al limbii române. https://www.dex.md/definitie/pensie
3. Legea nr. 227/2015 privind CODUL FISCAL din 8 septembrie 2015. În: MONITORUL OFICIAL al României, nr. 688 din 10 septembrie 2015.
4. https://insse.ro/cms/sites/default/files/com_presa/com_pdf/pensii_2019r.pdf
5. https://insse.ro/cms/sites/default/files/com_presa/com_pdf/pensii_tr1r20.pdf

WELL-BEING AND FORCED TECHNOLOGIZATION OF STUDENTS IN COVID LOCKDOWN MONTHS

WELL-BEING ŞI TEHNOLOGIZAREA FORȚATĂ A STUDENȚILOR ÎN LUNILE DE CARANTINĂ COVID

Dănuț Simion
Doctorand, lector universitar, Magistru în psihologie
Universitatea Tehnică a Moldovei
e-mail: simion2simion@gmail.com

Abstract
The shock of quarantine in the months of CoVid short-circuited the entire society. Quarantine it has largely affected all those social structures that have lagged behind in the process of technological modernization. One of these sectors was the education system. Teachers and students alike have been forced to assimilate technology and new interactive work programs. And the period of transit to another kind of normalcy has become more stressful than people imagine. In this article I will try to determine the relationship between studets psychological well-being and CoVid quarantine under the influence of new technologies.

Keywords: *pandemic, psychological well-being, students, teachers.*

JEL Classification: *O11, O38, O47, O52*

INTRODUCERE

Șocul carantinării în lunile CoVid a scurtcircuitat întreaga societate. Acesta a afectat în mare măsură toate acele structuri sociale ce au rămas în urmă cu procesul de modernizare tehnologică. Unul dintre aceste sectoare a fost și sistemul de învățământ. Cadre didactice și studenți deopotrivă au fost puși în situația de a asimila forțat tehnologie și noi programe de lucru interactiv. Iar perioada de tranzit către un alt fel de normalitate a devenit una generatoare de stres. Raportul dintre starea de bine psihologică și carantina CoVid sub influența noilor tehnologii la studenți aceasta voi încerca să determin în prezentul articol.

Cuvinte cheie: pandemie**,** stare de bine psihologică, studenți, profesori.

În cercetarea de faţă ne vom focaliza pe acea parte a psihologiei pozitive şi anume starea de bine şi comportamentul specific influenţat de lunile de carantină Covid la studenți. Principalul scop al lucrării de faţă este acela de a identifica şi evalua legătura între starea de bine psihologică a studenților şi digitalizarea instituțională forțată din instituțiile de învățământ superior din Republica Moldova; datele cercetării noastre fiind diseminate prin analiza unui grup de sudenți prinși la lecții în toată acea perioadă de tranzit de la normalitate la normalitate relativă.

REZULTATELE CERCETĂRII

Putem remarca cu mare interes faptul că în ultimii ani a crescut atenția pentru studierea conceptului de stare de bine psihologică. Aceste studii s-au concentrat preponderent pe afectele pozitive și negative asupra satisfacției vieții. Studiul științific al stării de bine subiective a apărut și s-a extins ca o reacție la accentul copleșitor pe care cercetătorii din domeniul psihologiei aplicate îl puneau pe dimensiunile negative ale adaptării și funcționării individului uman în diverse contexte.

Starea de bine este cercetată prin prisma a două mari paradigme: hedonică și eudaimonică. Paradigma hedonica pune accentul pe plăcere şi dorinţe şi este măsurată prin emoţiile pozitive raportate la emoţiile negative şi satisfacţia legată de viaţă [3]. Paradigma eudaimonică porneşte de la Aristotel şi este introdusă în psihologie prin paradigma umanistă de către A. Maslow, prin autoactualizarea, şi de către C. Rogers, prin tendinţa individului de a atinge sinele ideal si a deveni o persoană pe deplin funcţională [2, pp.40-41]. Astfel, starea de bine psihologică face referire la „efortul de a atinge perfecţiunea, adică de realizarea adevăratului potenţial al persoanei" [5, p.100]. Aceste cercetări s-au concentrat asupra afectelor pozitive şi negative şi a satisfacţiei în viaţă ele extinzându-se mai apoi și asupra modului în care individul percepe diverse aspecte ale funcționării sale, de exemplu măsura în care simte că are controlul asupra vieții, că ceea ce face are un sens și că merită făcut, că are relații satisfăcătoare cu ceilalți (Abbott și colaboratorii, 2006). Viața poate fi grea, iar dezamăgirile și provocările sunt inevitabile. Cu toate acestea, cercetările științifice au arătat că există unele strategii și abilități care permit oamenilor să navigheze mai eficient în provocările vieții și să se bucure de viață în ciuda supărărilor.

La sfârșitul anilor '80 și începutul anilor '90 Carol Ryff a dezvoltat un model utilizat pe scară largă de bunăstare psihologică având la bază șase factori. Acești șase factori sunt considerați astăzi ca fiind șase componentele majore ale bunăstării: 1) primul factor este acceptarea de sine; aceasta implică conștientizarea propriilor calități pozitive. 2) Al doilea factor este relații pozitive cu ceilalți; componenta aceasta se referă la sănătatea vieții interpersonale la capacitatea de a iubi și a empatiza. 3) Autonomie. Autonomia se referă la gradul de independență pe care îl are o persoană în luarea deciziilor și la modul în care acționăm în fața normelor sociale și culturale. 4) Stăpânirea mediului. Stăpânirea mediului este măsura în care cineva își poate alege mediul și îl poate adapta pentru a se potrivi nevoilor și trebuințelor sale. 5) Scopul în viață. Scopul e de dorit să se găsească în obiective și căile prin care se poate efectua concret schimbarea. Acest e de dorit să fie adaptabil și dinamic. 6) Creșterea personală se referă la o traiectorie precisă în viață și o dezvoltare personală continuă. Așadar creierul nostru se modelează în funcție de ceea ce noi gândim, simțim și facem iar efectele gândirii pozitive se știe că întărește sistemul imunitar, mărește energia vitală, crește longevitatea.

Digitalizarea forțată în perioada carantină a făcut ca studenții și profesorii să iasă oarecum din zona lor de confort și să se îndepărteze de modelul tradițional al abordării lecțiilor. Internetul în acele luni cu vârfuri pandemice și izolare a explodat la propriu prin tot felul de programe și instrumente interactive de lucru cu studenții. Instituțiile de învățământ inclusiv superior au fost luate total pe nepregătite. Starea de izolare, lucrul forțat de la domiciliu, lipsa condițiilor de studiere eficientă, lipsa tehnicii și cerințele instituționale confuze a făcut ca numărul de cazuri de stres și depresie în rândul studenților să crească simțitor. Studenții au căutat centre psihologice și psihologi pentru oferirea de servicii corespunzătoare. Au fost oarecum în avantaj studenții din suburbii care și așa învățau de acasă. Pentru restul, însă, prinși între cămine și/sau drumul spre casă, a fost o adevărată povară. Iar primele îmbolnăviri în rândul lor a schimbat cu totul perspectiva procesului pedagogic.

Cu toate acestea, chiar dacă responsabilitatea față de lecții a crescut treptat și au asimilat alături de cadrele didactice zeci de ore de webinare online metodele de predare ale cadrelor didactice au rămas preponderent aceleași; la fel nevoiți să asculte interminabile prelegeri și să copieze lecțiile numai că acum acest lucru se realizează din fața unui laptop și nu frontal cum era făcut până de curând. Studenții fiind obișnuiți deja cu noile tehnologii s-au adaptat ceva mai ușor la noile rigori.

Cercetarea efectuată a scos la iveală faptul că dintr-un număr de total de 59 studenți din două grupe ce au participat la prelegeri și seminarii 42 studenți s-au adaptat rapid și au asimilat noua tehnologie ca pe ceva firesc 17 au avut careva probleme de adaptare și nici unul nu a fost pus în situația de a abandona orele din lipsa tehnologiei (fig. 1).

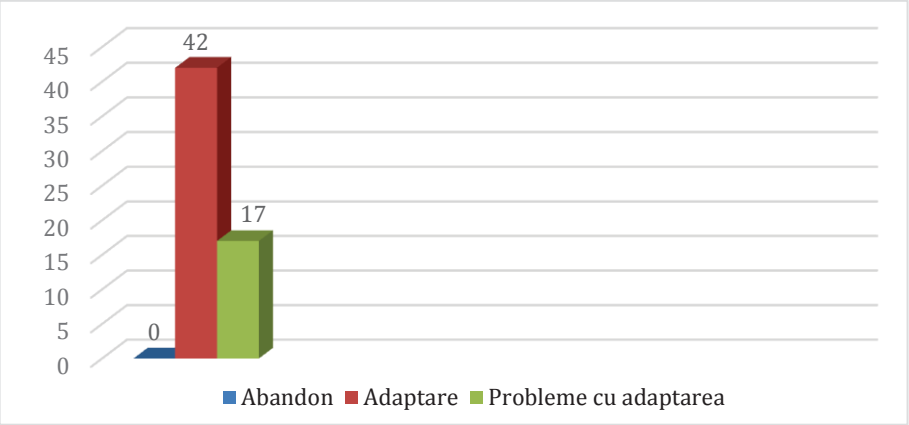


Figura 1. Capacitatea de adaptare la noi cerințe

Majoritatea studenților, 50 dintre ei, în perioada de izolare au folosit preponderent pentru conectare laptopul în comunicarea cu profesorii (fig.2), pe al doilea loc aflându-se telefonul mobil, 9 studenți au avut ca formă intermediară de comunicare smartfonul. S-a constatat că o parte din blocajul comunicațional venea ori din lipsa tehnologiei ori din cauza problemelor de la compania furnizoare a serviciilor de internet.

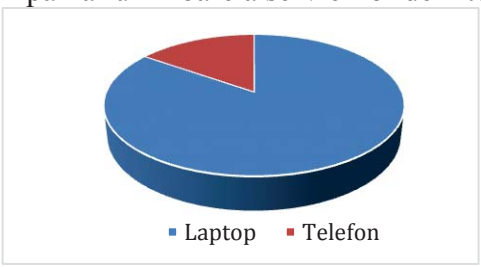


Figura 2. Tehnologii de comunicare utilizate

La câteva luni de carantină, înainte ieșirea în vacanță am constatat că adaptarea studenților la noile cerințe este net superioară față de situația de la intrarea în pandemie aceasta îmbunătățindu-se considerabil din 59 de studenți toți au învățat a folosi laptopul cu programele sugestionate de universitate pentru comunicarea cu profesorii, telefonul fiind folosit doar în cadrul unor situații excepționale.

Mai putem constata faptul că la intrarea în pandemie din toți cei 59 de studenți majoritatea au manifestat rezistență la a face orele în regim online. La sfârșit de semestru însă situația era oarecum diferită (fig.3). Din 59 de studenți, 45 ar fi preferat și pentru viitor realizarea orelor doar online într-o o formă mixtă de interacțiune sincron și asincron și doar 14 ar fi dorit frontal tot timpul.

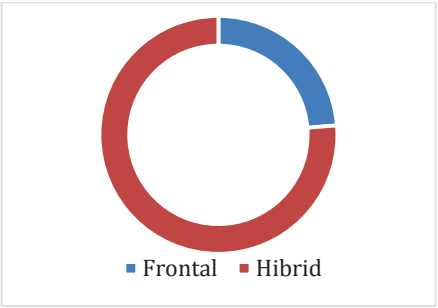


Figura 3. Regimul de studii preferat de studenți

Un sondaj realizat în România în perioada 18-23 noiembrie 2020 ”Percepții despre calitatea educației online” pe un eșantion de 9.401 elevi, 3.265 de cadre didactice și 4.965 de părinți, arată că, deși contextul pandemic a forțat digitalizarea educației și profesorii și-au îmbunătățit competențele digitale, iar elevii s-au obișnuit cu utilizarea diverselor platforme online, doar 23% dintre elevi și 36% dintre părinți susțin că elementele digitale vor continua să fie folosite și în sistemul față în față. Singurii optimiști, sunt profesorii, 60% consideră că educația față în față va integra elemente digitale după reîntoarcerea fizică la școală.

În acest moment, 72% dintre elevi și 67% dintre profesori desfășoară orele online conform orarului pe diferite platforme video. O proporție de aproximativ 25% dintre elevii și cadrele didactice desfășoară educația online atât în sistem sincron, cât și asincron. Cu toate acestea, deși există premisele pentru participarea la educația online, cei mai mulți dintre profesori organizând orele, calitatea acestora devine îndoielnică din perspectiva celor trei grupuri vizate – elevi, cadre didactice și părinți”, arată sondajul.

În viziunea elevilor și a părinților, unele dintre cadrele didactice sunt rigide în desfășurarea activităților online: pun absențe elevilor dacă nu au camera deschisă sau dacă s-au deconectat de la internet, dau note mici dacă elevii au probleme tehnice, nu revin asupra informațiilor care nu au fost înțelese sau notate de către elevi etc”, mai relevă sondajul. Datele din sondajul efectuat în țara vecină fiind mult asemănător și cu ceea ce se întâmplă în mod real în teren și în Republica Moldova.

Mai putem constata că, procesul izolării a atras după el și multe beneficii. Unul dintre acestea o reprezintă folosirea cu folos a tehnicii computerizate în procesul de predare, învățare și asimilare. După cum bine știm învățământul nu mai pune de mult accentul pe asimilarea și reproducerea informației ci pe căutarea și diseminarea ei. Folosirea informației atunci când este nevoie cu maximum de impact.

Chiar dacă studenții s-au obișnuit cu predarea online și noile programe de interacțiune precum: google meet, microsoft teams, zoom, moodle etc., în continuare acuză o parte din probleme. Încă există o lipsă a tehnicii performante la unii dintre studenți și a internetului. Din acest punct de vedere multe dintre instituțiile gazdă depun eforturi constante pentru a gestiona eficient situația studenților care nu dispun de tehnică și nu pot participa la orele online. O alternativă fiind crearea unor săli speciale cu păstrarea distanței fizice în cadrul universităților prin care studenții folosind produse speciale precum laptopurile și tabletele se pot conecta cu cadrele didactice.

Obligativitatea pentru a deschide camerele și de a participa activ la ore. Aici însă în anumite cazuri ne lovim și de o problemă legală încă nesoluționată; invadarea spațiului personal și intim al studentului. Deseori în interacțiunea online apare o lipsă de motivație a studenților cât și a unora dintre profesori. Timpul pentru pregătirea lecțiilor crește simțitor pe când materia studiată rămâne aceeași. Unele lecții devin plictisitoare, stresante, obositoare și de multe ori lecțiilor predate nu sunt pe deplin înțelese. Lipsa spațiului adecvat la studenți precum și la unii dintre profesori. Mai putem adăuga apariția unor stări de anxietate și lipsa motivației iar o problemă acuzată de mulți dintre studenți este lipsa socializării. Timpul îndelungat petrecut în fața ecranelor laptopurilor sau tabletelor produce o mai mare oboseală și stres. Din acest punct de vedere ar trebui să existe în cadrul orelor online mai multe și dese pauze iar timpul orelor redus.

Se constată totuși și multe lucruri pozitive la studenți dar și la profesori în interacțiunea sincronă unul dintre acestea fiind îmbunătățirea comunicării cu studenții. Avem apoi abordarea unor metode noi și interesante la profesori în procesul de predare al prelegerilor și timpul petrecut pentru seminarii. Deseori se folosesc metode alternative în evaluare ceea ce sporește corectitudinea evaluării și scade coruperea și cumpărarea notelor.

Și nu în ultimul rând putem constata o creștere a activității studenților mai introvertiți în cadrul orelor teoretico-practice. Mai putem adăuga spre final o creștere a confortului și siguranței, mai multă încredere în sine și timp poate ceva mai mult pentru continuarea sau descoperirea de noi hobby-uri și pasiuni.

Cum majoritatea orelor sunt acum în regim online, în continuare sunt prezentate câteva reguli de comunicare online pentru studenți.

1. Scrieți orarul lecțiilor pe o foaie de hârtie și aduceți acest lucru în atenția tuturor membrilor familiei. Lipiți pe ușă camere in afiș cu ,,nu deranjați,, sau ,,am intrat online,,. Cu siguranță nu vreți să vă treziți cu surprize în timpul orei de la profesorul X.

2. Înainte de a intra în online e recomandabil să fi mâncat ceva și să fi făcut puține exerciții pentru dezmorțit oasele, dregeți-vă vocea. Vocea somnoroasă se cunoaște oricum și oricât ați încerca să ascundeți acest lucru.

3. Porniți și verificați camera, calibrați-o înainte de a intra în direct. Nu de alta dar nu o să de-a chiar bine apariția altor părți ale corpului pe ecranul laptopului.

4. Folosiți o fotografie reală când vă logați și sunteți gata să comunicați online. Se întâmplă ca sistemul să nu facă față fluxului de intrări iar camerele se deconectează automat rămânând în spate doar o simplă fotografie. Am comunicat cu rachete, câini, tatuaje, femei semi-dezbrăcate, crocodili, schelești, ninja și chiar dinozauri. Sincer nu am știut că sunt atât de ...polivalent. E bine totuși ca profesorul chiar dacă aveți camera oprită să știe cui i se adresează.

5. Atenționați organizatorul, profesorul, moderatorul dacă părăsiți lecția sau ședința chiar și pentru o perioadă scurtă de timp. Profesorii mai fac din când în când și câte o prezență la mijlocul lecțiilor și ar fi ciudat să vă caute prin toată ,,rețeaua,, iar voi sunteți la: prășit, dormit sau...toaletă; nu uitați unele lucruri chiar necesită timp.

6. Semnalizați din timp când doriți să vorbiți.

7. Oferiți profesorului sau moderatorului neapărat feedback. O prezentare sau prelegerea este formată din voi toți; profesor plus student/elev. Și nu uitați, voi chiar aveți o voce.

7. La sfârșitul orei luați-vă la revedere. Personal prefer un simplu mesaj de ”la revedere”, ”o zi minunată” etc., (eu chiar le citesc); când toți deschid microfoanele e cam hărmălaie și de multe ori asurzitor.

CONCLUZII

Conchidem că sistemul de învățământ așa cum era înainte nu are cum să mai fie, nu cred că ne vom mai întoarce vreodată la educația pre covid și din acest punct de vedere ar trebui să existe o viziune clară și pe termen lung din partea instituțiilor statului. E nevoie de planuri noi și de alternative viabile în caz de calamități atât la studenți cât și pentru profesori. E nevoie în același timp de o educație față în față integrată în și cu noile tehnologii chiar dacă partea de digitalizare a educației va continua și ar trebui să continue. În aceeași măsură e nevoie de o mai mare implicare a studenților în procesul instructiv educativ și de căutat eventual soluții pentru studenți inclusiv de la studenți. O altă necesitate este reglementarea prin lege a numărului de ore minime și maxime ce pot fi suportate în fața calculatorului. Consider că ar trebui deasemenea să se investească în continuare în competențele studenților pentru desfășurarea orelor în mediul online. Școala online cu regret a mai scos un lucru la suprafață ce trebuie tratat cu mare seriozitate și de găsit cât mai curând soluții; diferența dintre diversele pături sociale la studenți, lucru vizibil la nivelul tehnologiei folosite în conectarea la ore și interacțiunea cu cadrele didactice.

BIBLIOGRAFIE

1. Diener E. și al. Subjective well-being: Three decades of progress. În: Psychological Bulletin, vol. 125, nr. 2, p. 276-302, 1999.
2. Daniel David , Aurora Szentágotai-Tătar,Tratat de psihologie pozitiva, Iași: Polirom. 2017. 344 pg. ISBN: 978-973-46-6234-0
3. Ryan, R. M., & Deci, E. L. (2001). On happiness and human potentials: A review of research on hedonic and eudaimonic well-being. Annual review of psychology, 52(1), 141-166.
4. Ryff, C. D. (1989). Happiness is everything, or is it? Explorations on the meaning of psychological well-being. Journal of personality and social psychology, 57(6), 1069.
5. Ryff, C. D., & Keyes, C. L. M. The structure of psychological well-being revisited. Journal of personality and social psychology, 69(4), 719. 1995
6. Rogers, C., A deveni o persoană. Bucureşti: Ed. Trei, 2008, 560p. ISBN: 978-973-707-244-3
7. Shane J. Lopez, Jennifer Teramoto Pedrotti, C. R. Snyder. Positive Psychology The Scientific and Practical Explorations of Human Strengths (3rd Edition). SAGE Publications, Inc. 2015 p. 353. ISBN 978-1-4522-7643-4
8. Percepții despre calitatea educației online. Sondaj. [citat 06.12.2020]. Disponibil: https://cdn.edupedu.ro/wp-content/uploads/2020/12/Rezultate-sondaj-online_calitatea-educatiei-online_dec2020.pdf

THE SECURITY OF ONLINE PAYMENTS THROUGH E-COMMERCE SERVICES OF THE REPUBLIC OF MOLDOVA BANKS

SECURITATEA PLĂȚILOR ONLINE PRIN SERVICIILE E-COMMERCE AL BĂNCILOR DIN REPUBLICA MOLDOVA

Balan Mariana
Profesor de discipline economice, grad didactic întâi
Colegiul Național de Comerț al ASEM
e-mail: cncasem18@gmail.com

Enachi Olga
Profesor de discipline economice, grad didactic întâi
Colegiul Național de Comerț al ASEM
e-mail: olgaenachi2015@gmail.com

Abstract
The Banking sector represents a vital component of our nation's infrastructure. Financial Institutions provide a large scale of products form the large bank institutions to the smallest community banks and credit unions. The rise of financial institutions and its role in our daily life exposes banking sector to increasingly more crises. The banking sector as a part of financial sector is best path to economic prosperity, development, and sustained wealth of nation, this way the banking crises threat national security.
E-commerce quickly becomes an instrument of strategic importance for companies. The efficient management of these changes is a condition for the success or failure of the e-commerce. Digitized banking system is a way for companies to survive and to be competitive in a modern economy.

Keywords: *National Security, Central Bank, Banking, Technological Innovation, E-commerce, Activation during shopping, Payments, Mobile payments.*

JEF Classification: *E580, K400, O320, O330*

INTRODUCERE

Securitatea economică reprezintă un concept complex şi dinamic. Complexitatea sa derivă din multitudinea de procese şi fenomene economice, sociale, financiare. Pe de altă parte, aici, intervine consistent globalizarea, văzută atât ca proces, cât şi ca fenomen care acţionează sistematic şi permanent asupra economiilor naţionale. Dinamismul său este dat de ritmul alert al proceselor şi fenomenelor economice care se produc atât la nivel naţional, cât şi planetar.

Securitatea economică ar trebui percepută ca fiind un factor esenţial al securităţii naţionale şi anume acela care asigură resursele şi echilibrul dinamic al celorlalte componente ale acestui sistem.

În prezent, asistăm la apariţia pe scena lumii a noi factori transnaţionali şi nonstatali care dispun de mijloacele necesare şi suficiente pentru a conduce şi duce la acţiuni la nivel mondial. Noile vulnerabilităţi, riscuri şi ameninţări cu care se confruntă astăzi omenirea impun, la începutul acestui secol, ca, în mod obligatoriu, conceptul de securitate să se articuleze în jurul principiilor securităţii internaţionale, al securităţii naţionale şi al securităţii umane. Lanţul acestei relaţiei se găseşte în securitatea economică, în calitatea sa de dimensiune a securităţii internaţionale şi statale, precum şi de resursă a securităţii umane.

CONȚINUT

Sistemul bancar este unul din sectoarele cele mai profund integrate în economia națională, datorită activității sale de creditare, precum și de colectare și agregare a economisirilor populației, entităților economice. Prin urmare, acesta este și cel mai sensibil la schimbările privind situația și expectanța macroeconomică, manifestând un comportament pro-ciclic.

Necesitatea asigurării securităţii sectorului bancar se datorează faptului că în prezent, activitatea bancară este prezentă oriunde, în cadrul tuturor relaţiilor economice, fie acestea sunt relaţiile cu persoanele fizice care utilizează produsele bancare pentru propriile necesităţi, fie cu persoanele juridice care-şi realizează activitatea prin intermediul băncilor fiind utilizatorii direcţi a produselor bancare. Noţiunea de securitate economică a sectorului bancare se înţelege abilitatea acestuia de a rezista factorilor destructivi a pieţii financiare şi de a asigura supravieţuirea sistemului bancar în condiţiile unei concurenţe stringente. Securitatea bancară [7] mai presupune și sistemul de protecție a informațiilor bancare si a mijloacelor financiare aflate în gestiunea băncii.

Anul 2020 este anul care a dat peste cap orice previziuni și a impus presiune asupra sectorului bancar și chiar poate mai mult. Pe lângă faptul că sunt agenți economici, băncile mai sunt și unul dintre pilonii de bază ai stabilității financiare. Iar această perioadă impune întreprinderea unor măsuri neordinare pentru a asigura stabilitatea necesară. ***E-commerce*** devine un instrument tot mai solicitat pentru economie. Băncile comerciale din R. Moldova în această perioadă au fost foarte receptive la toate schimbările și au pus la dispoziție o ofertă tot mai mare de servicii accesibile atât pentru persoanele juridice cât și persoanele fizice pe platforme de servicii e-commerce. Dezvoltarea continuă a tehnologiilor informaționale are o contribuție semnificativă la elaborarea și implementarea noilor sisteme de plăți și decontări, a instrumentelor de plată fără numerar, a sistemelor automatizate de deservire la distanță care, din cauza gradului de complexitate, sunt expuse la riscuri ce necesită a fi monitorizate și gestionate în modul corespunzător. Banca Națională a Moldovei încurajează cetățenii să utilizeze metodele de plată fără numerar, cum ar fi aplicațiile internet și mobile payments, plățile securizate pentru comerțul electronic, precum și cardurile pentru plata bunurilor și serviciilor în puncte comerciale. Aceste metode sunt mult mai igienice decât utilizarea numerarului și constituie o bună practică de prevenire a răspândirii bolilor transmisibile, inclusiv a virozei de tip COVID-19.

Astfel în Republica Moldova sistemul de plăți electronice este monitorizat și securizat de către Banca Națională a Moldovei. [8] Scopul supravegherii îl constituie asigurarea funcţionării stabile şi eficiente a sistemelor de plăţi şi decontări, precum şi asigurarea eficienţei şi siguranţei instrumentelor de plată fără numerar şi a sistemelor de deservire bancară la distanţă. Banca Naţională supraveghează sistemele de plăţi şi decontări, funcţionarea stabilă şi eficientă a cărora este esenţială pentru stabilitatea financiară şi implementarea politicii monetare şi valutare, precum şi mecanismele de gestionare a riscurilor stabilite în cadrul sistemelor utilizate pe scară largă de către populaţie pentru efectuarea plăţilor şi transferurilor.[1] De asemenea, în vederea promovării încrederii publicului în efectuarea plăţilor fără numerar, Banca Naţională aplică Politica de supraveghere a sistemului de plăţi în Republica Moldova, aprobată prin HCE al BNM nr. 299 din 27.10.2016. [2]

Domeniul supravegherii instrumentelor de plată fără numerar și a sistemelor automatizate de deservire la distanță, supravegherii sunt supuse:

1. Cardul de plată reprezintă un suport de informație standardizat și, după caz, personalizat prin intermediul căruia deținătorul, de regulă, cu utilizarea numărului personal

de identificare și /sau a unor alte coduri care permit identificarea sa, în funcție de tipul cardului de plată are acces la distanță la contul de plăți la care este atașat cardul de plată în vederea efectuării anumitor operațiuni de plată.

Pe parcursul trimestrului I, anul 2020, indicatorii activității cu carduri de plată și-au menținut tendința de creștere, numărul cardurilor aflate în circulație majorându-se cu 6,7 la sută față de aceeași perioadă a anului precedent, iar numărul plăților fără numerar efectuate cu cardurile emise în țară și-a menținut trendul de creștere, cu 38,3 la sută față de perioada similară a anului precedent.

În trimestrului II, 2020, indicatorii activității cu carduri de plată deasemenea și-au menținut tendința de creștere, numărul cardurilor aflate în circulație majorându-se cu 7,6 la sută față de aceeași perioadă a anului precedent, iar numărul plăților fără numerar efectuate cu cardurile emise în țară și-a menținut trendul de creștere, cu 32,5 la sută față de perioada similară a anului precedent. Conform datelor pentru trimestrul de referință, 87,4 la sută din număr și 88,6 la sută din valoarea operațiunilor de TC au fost inițiate în format electronic prin intermediul SADD (sistemele automatizate de deservire la distanță), ceea ce reflectă gradul de digitalizare a serviciilor de plată în Republica Moldova.

Tabelul 1. Indicatorii activității în cadrul sistemului de plăți cu cardurile de plată în perioada anului 2019 (mii lei)

Denumirea indicatorului	*Trimestrul 3*	*Trimestrul 2*	*Trimestrul 1*
Numărul de operațiuni cu carduri emise în RM și efectuate în RM pe parcursul perioadei analizate.	16,565,201	16,213,334	14,590,564
Valoarea operaţiunilor cu carduri emise în Republica Moldova și efectuate în Republica Moldova pe parcursul perioadei analizate.	15,946,294.6	15,253,188.6	13,985,587.1
Numărul de operaţiuni cu carduri emise în Republica Moldova și efectuate în străinătate pe parcursul perioadei analizate.	3,532,745	3,167,742	3,222,058
Valoarea operaţiunilor cu carduri emise în Republica Moldova și efectuate în străinătate pe parcursul perioadei analizate.	2,026,365.8	1,788,179.3	1,611,529.8
Numărul de operaţiuni cu carduri emise în străinătate și efectuate în Republica Moldova pe parcursul perioadei analizate.	2,397,997	2,397,997	2,397,997
Valoarea operaţiunilor cu carduri emise în străinătate și efectuate în Republica Moldova pe parcursul perioadei analizate.	2,653,284.9	2,174,217.4	1,710,627.1

Sursa: https://www.bnm.md/bdi/pages/reports/dsp/DSP1.xhtml

2. Transferul de credit reprezintă o serie de operațiuni care încep prin inițierea de către plătitor a unui ordin de plată și transmiterea acestuia prestatorului de servicii de plată în scopul punerii la dispoziția unui beneficiar a unei anumite sume de bani. Transferul de credit poate fi inițiat atât în numele clientului prestatorului de servicii de plată, cât și nemijlocit de către prestatorul de servicii de plată în nume și pe cont propriu. [3]

3. Debitarea directă constă dintr-o serie de proceduri în care debitarea contului de plăți al plătitorului se realizează în baza informației primite de la beneficiarul plății și a consimțământului acordat de către plătitor privind debitarea contului său.

Debitarea directă rămâne a fi un instrument mai puțin utilizat pe teritoriul RM. La finele trimestrului II al anului curent, acest instrument a fost utilizat de către 10,7 mii de plătitori în creștere semnificativă față de finele trimestrului I care a constituit 9,7 mii plătitori. Debitarea directă este utilizată doar de către persoanele fizice, iar în majoritatea cazurilor este vorba de plata serviciilor comunale.

4. Sistemele automatizate de deservire la distanță (în continuare – sisteme ***ADD***) sunt soluții informatice și/sau echipamente care după caz facilitează accesarea la distanță de către utilizator a contului de plăți, obținerea de informații privind starea contului de plăți și a operațiunilor realizate, efectuării operațiunilor de plată, atât prin utilizarea electronică a instrumentelor de plată fără numerar, cât și prin primirea automatizată a numerarului, precum și schimbul de mesaje autentificate între utilizatorul sistemului și prestatorul său. Sistemele automatizate de deservire la distanță pot fi clasificate în: pc-payments, internet-payments (browser based payments), mobile-payments, telephone-payments, terminal-payments.

Sistemele automatizate de deservire la distanță (SADD) devin tot mai populare în rândul utilizatorilor, astfel se constată o majorare a numărului deținătorilor SADD la finele trimestrului I 2020 comparativ cu perioada similară a anului precedent, care se datorează, în special, creșterii considerabile a utilizatorilor sistemelor de tip mobile-payments. Numărul deținătorilor activi a consemnat o tendință de creștere de 83,5 la sută, ceea se explică prin creșterea necesității de a utiliza SADD pentru efectuarea plăților de la distanță, în special, în contextul situației epidemiologice din țară.

Tabelul 2. Evoluția sistemelor de plăți și serviciilor de plată în perioada 2019-2020 / per prestator

	Total pe prestatori		*B.C. „MAIB" S.A.*		*B.C. „MOLDINCOMBANK" S.A.*		*B.C. „VICTORIABANK" S.A.*	
	2019	*2020*	*2019*	*2020*	*2019*	*2020*	*2019*	*2020*
Dispozitive speciale	*406*	*439*	*182*	*196*	*25*	*29*	*199*	*214*
Platforme de comerț electroni	*393*	*412*	*176*	*190*	*25*	*25*	*192*	*197*

Sursa: https://www.bnm.md/bdi/pages/reports/dsp/DSP2.xhtml

În domeniul supravegherii instrumentelor de plată fără numerar și sistemelor ADD, Banca Națională a Moldovei efectuează următoarele:

1) colectează date privind siguranța și eficiența instrumentelor de plată fără numerar și a sistemelor ADD. Datele folosite în scopul supravegherii sunt colectate în baza rapoartelor statistice prezentate de către ***prestatorii de servicii de plată*** (în continuare - ***PSP***), a informațiilor obținute în cadrul controalelor pe teren efectuate la aceștia, precum și din sursele de informare în masă (internet, presa scrisă etc.);

2) monitorizează apariția noilor tehnologii în domeniu. Evoluțiile înregistrate în domeniul tehnologiilor informaționale influențează în mod direct caracteristicile serviciilor de plată și implicit nivelul de siguranță și eficiență a instrumentelor de plată fără numerar, sistemelor ADD. Valorificarea acestor evoluții permite creșterea eficienței supravegherii ca urmare a introducerii unor noi metode de protecție împotriva fraudelor, optimizarea mecanismelor de efectuare a plăților, precum și cunoașterea noilor tipuri de fraude;

3) analizează și evaluează indicatorii de eficiență și siguranță în baza informației și datelor obținute atât de la PSP, cât și ca urmare a cercetărilor proprii în vederea identificării situației actuale și evoluțiilor recente în utilizarea instrumentelor de plată fără numerar/sistemelor ADD, a siguranței acestora, precum și a măsurilor ce pot fi întreprinse

în vederea îmbunătățirii valorii indicatorilor; gradul de complexitate, deplinătate și criteriile de suficiență a serviciilor oferite;

4) întreprinde măsurile relevante. În cazul constatării abaterilor la indicatorii aferenți siguranței și eficienței instrumentelor de plată/sistemelor ADD, Banca Națională intervine prin ajustarea cadrului normativ, formularea de recomandări sau întreprinderea altor măsuri potrivite în vederea sporiri soliditățiii acestora.

Avantajele utilizării instrumentelor de plată fără numerar:

1. *Simplitate* – poți efectua plăți simplu.
2. *Securitate* – plățile fără numerar sunt mai sigure și te scutesc de necesitatea de a purta sume de bani în numerar. Mai mult decît atât, emitenții de carduri de plată investesc în continuu în tehnologiile de securitate ultra-moderne care pot identifica și preveni tranzacțiile frauduloase înainte ca acestea să poată avea loc.
3. *Convenabil* – poți utiliza cardurile de plată pentru a accesa conturile tale de plată în orice moment de oriunde în lume. Cardul de plată reprezintă cea mai rapidă și mai simplă modalitate de a face cumpărături la locul de vânzare sau pe Internet .
4. *Flexibilitate* – diversitatea de carduri disponibile în zilele noastre îți oferă mai multă libertate de a alege cum și când plătești pentru bunuri și servicii. Cardurile de plată sunt acceptate oriunde, și-ți oferă acces sigur și convenabil la banii tăi.
5. *Recompense* – diverse bănci oferă carduri de plată cu programe de loialitate care iți permit să câștigi anumite sume de bani, bilete de avion sau alte recompense.

În contextul obiectivului strategic de promovare a plăților fără numerar, în calitate de indicator ce reflectă gradul de digitalizare a serviciilor de plată, se va monitoriza ponderea ordinelor de plată inițiate în mod electronic de către clienții băncilor, precum și măsurile întreprinse de aceștia pentru sporirea numărului de plăți inițiate în mod electronic.

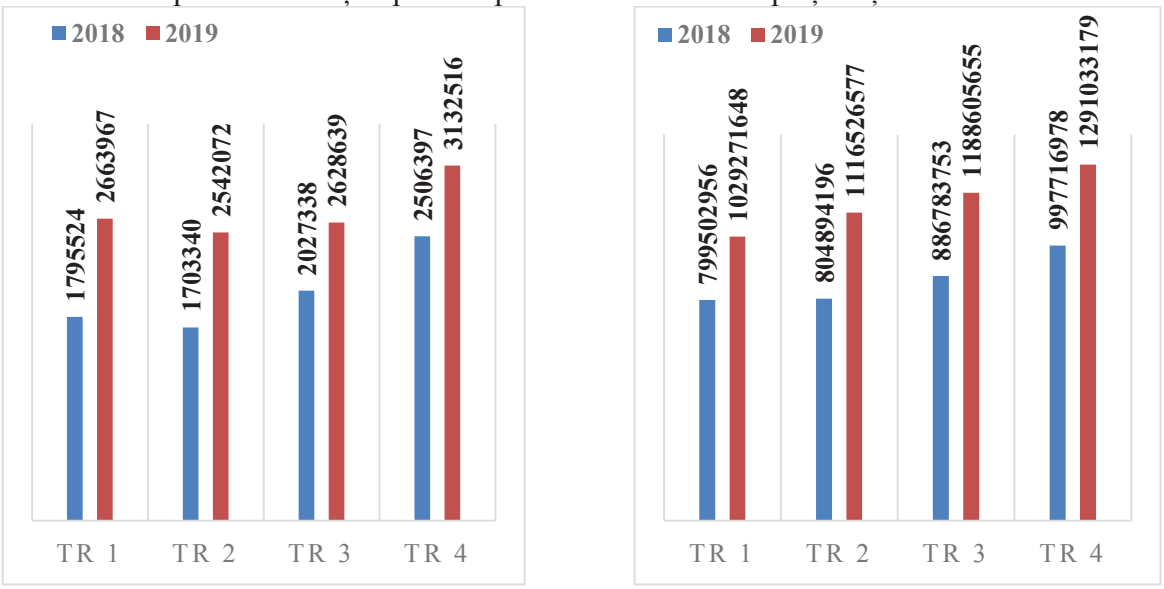


Diagrama 1. Numărul și valoarea tranzacțiilor efectuate cu carduri de plată din Republica Moldova

Sursa: https://www.bnm.md/bdi/pages/reports/dsp/DSP4.xhtml

Un sistem de securitate utilizat de către băncile comerciale din R. Moldova pentru sporirea gradului de încredere în serviciile de e-commerce este 3D-Secure. Este un sistem antifraudă dezvoltat de Visa și MasterCard. Folosirea acestui sistem permite creșterea securității tranzacțiilor online, prin solicitarea unei parole la fiecare plată online. În caz de pierdere sau furt, cardul înrolat la 3D Secure, nu poate fi folosit de terțe persoane pentru cumpărături online. Se elimină astfel riscul fraudei prin copierea informațiilor de plată sau

prin generarea aleatoare de numere de carduri și utilizarea lor ulterioară pe Internet. Prin folosirea acestui sistem de tranzacționare se așteaptă o reducere a disputelor din fraudele rezultate din tranzacțiile on-line cu cel puțin 80%.

Deținătorul cardului se poate orienta pentru cumpărături numai către site-urile care afișează logo-urile Verified by Visa sau Mastercard SecureCode. În aceste magazine virtuale, user-ul este solicitat să se autentifice la fiecare tranzacție păstrand astfel controlul asupra cumpărăturilor on-line.

Procesul de autentificare nu necesită instalarea vreunei aplicații speciale pe computerul clientului și nici nu îngreunează navigarea pe Internet și determină creșterea încrederii în aceasta modalitate de a cumpăra bunuri/servicii.

Funcționarea serviciului 3-D Secure [11] implică efortul comun al băncilor emitente de carduri, al băncilor cu care posesorii magazinelor virtuale au încheiat contracte de acceptare la plată a cardurilor, al comercianților respectivi și al organizațiilor internaționale de carduri. Pe măsură ce tot mai multe magazine virtuale împreună cu bancile lor și tot mai multe bănci emitente de carduri aderă la acest serviciu, crește încrederea tuturor părților implicate în tranzacțiile pe Internet și implicit volumul acestora, scăzând concomitent riscul de fraudă.

3D Secure este un serviciu ataşat cardului tău care îţi asigură cumpărături on-line protejate. Tehnologia 3D Secure a apărut ca răspuns la necesitatea dezvoltării unor mijloace prin care să se verifice dacă persoana care face o plată pe Internet este chiar deținatorul real al cardului - prin solicitarea de introducere suplimentar la datele standarde necesare pentru efectuarea cumpărăturii (numărul cardului, data valabilităţii şi codul CVV2) a unei parole unice primite de deținător prin E-mail sau SMS în momentul efectuării tranzacţiei în mediul Internet. [12]

Tehnologia 3D Secure se aplică doar la comercianţii, care au afişat pe site-ul lor unul din logo-urile – ceea ce confirmă faptul că acești comercianţi sunt certificaţi la aplicarea tehnologiei de către Sistemele Internaţionale de Plăţi cu carduri.

Desenul 1. Logo-urile Sistemelor Internaţionale de Plăţi cu carduri
Sursa: https://www.maib.md/ro/ghidul-autentificarii-prin-3d-secure/

Activarea cardurilor pentru utilizarea tehnologiei 3D Secure se efectuiază la prima tranzacţie de achitare prin Internet, pe site-ul comerciantului, pe care este afişat logo-ul prezentat mai sus. Activarea respectivă se numeşte *Activation during shopping – Activarea în procesul de efectuare a cumpărăturii.*

Internetul a devenit un canal de comeț cu o putere incontestabilă în a facilita și crește vânzările unei game din ce în ce mai largi de produse și servicii. Infrastructura e-commerce descrie hardware-urile, softwareurile și rețelele utilizate în comerțul electronic. Toate aceste componente necesită, desigur, și o bună practică de management și nemijlocit digitalizare. E-commerce este unul dintre sectoarele cu cea mai rapidă creștere. Moldova nu face excepție, cu o piață în continuă dezvoltare și care urmărește rapid tendințele globale. Studiul de măsurare a traficului și a audienței pe internet, realizat de Biroul de audit pentru circulație și internet (BATI) în parteneriat cu Gemius, arată că piața online a Moldovei a crescut în ultimii ani. În ianuarie 2020, Moldova a înregistrat un număr de 3,07

milioane de utilizatori de internet. În 2019, 12% mai mulți moldoveni au achiziționat produse sau servicii online comparativ cu 2018 și cu 24% mai mult decât în 2017. [13]

CONCLUZII

Urmează o perioadă în care digitalizarea va accelera şi mai mult. Viitorul este al băncilor digitalizate, standardizate, care vor găsi soluţii prin care să ofere servicii evitând contactul fizic. Există apetit şi dorinţă de inovaţie din partea instituţiilor bancare. Activităţile bancare tradiţionale se văd provocate din ce în ce mai mult, poate chiar într-o progresie exponenţială, de către firme abia înfiinţate care aduc masiv avansul tehnologic în zona serviciilor financiare. Unele estimări arată că transformările digitale pot creşte cu cca. 30% veniturile unei bănci tradiţionale, în special în cazul produselor precum creditele pentru nevoi personale şi operaţiunile de plăţi. În acelaşi timp, prin digitalizare, accesul clienţilor la servicii financiare va câştiga flexibilitate, iar concurenţa, tot mai intensă, dintre furnizorii de asemenea servicii va conduce la reducerea costurilor pentru clienţi.

Digitalizarea este necesară deoarece sistemul național de plăți este în cea mai mare parte susținut și generat de bănci. Prin bănci are loc peste 90% din finanțarea economiei, băncile dețin know-how performant care este necesar în implementarea serviciilor digitale și în securitatea cibernetică. Introducerea digitalizării, indiferent de ce binefaceri aduce, provoacă diminuarea numărului de angajați bancari. Automatizarea, centralizarea și externalizarea, sunt procese care conduc spre reducerea numărului de unități bancare și la centralizarea activității. De fapt acesta este și sensul digitalizării, diminuarea costurilor și eficiență sporită. Un banking modern nu poate fi gândit decât în consonanță cu economia digitală. Astfel, pentru a deveni o societate adaptată la schimbări, incertitudini și provocări, Republica Moldova trebuie să adopte un cadru de politici bine corelate pentru o abordare sistemică pe termen lung a dezvoltării durabile. Drept urmare, sistemul financiar este un sector de politici cheie care poate susține economia națională și contribui la dezvoltarea societății.

O economie modernă şi dinamică nu este posibilă fără un sistem bancar sănătos, modern şi predictibil. Rolul băncilor este esenţial în economie tocmai pentru că facilitează finanţarea investiitor şi a consumului. Un sistem bancar puternic înseamnă o economie puternică, iar o economie puternică înseamnă prosperitate pentru toţi cetăţenii.

BIBLIOGRAFIE

1. Legea cu privire la serviciile de plată și moneda electronică nr. 114 din 18.05.2012 // publicat în MO al RM.- 2012, nr.193- 197, art.661
2. Hotărârea Comitetului Executiv al BNM nr. 299 din 27.10.2016 Cu privire la aprobarea Politicii de supraveghere a sistemului de plăţi în Republica Moldova
3. Regulamentul cu privire la transferul de credit, aprobat prin Hotărârea Consiliului de Administraţie al Băncii Naţionale a Moldovei nr.373 din 15.12.2005 // Monitorul Oficial al Republicii Moldova, 2005, nr.176-181/643 (cu modificările şi completările ulterioare).
4. Hotărârea Comitetului Executiv al BNM nr. 299 din 27.10.2016 Cu privire la aprobarea Politicii de supraveghere a sistemului de plăţi în Republica Moldova
5. Postolache V., Curac A. Securitatea economică a sectorului bancar în condițiile contemporane // în Materialele Conferinței Științiifice Internaționale “Asigurarea

viabilității economico-managerială pentru dezvoltarea durabilă durabilă a economiei regionale în condițiile integrării în UE".- Bălți,2017.- p.292-295
6. https://www.bnm.md/ro/content/sistemul-national-de-plati/ , accesat 23.11.2020
7. https://administrare.info/economie/10310-conceptul-general-al-securit%C4%83%C5%A3ii-b%C4%83ncii-comerciale/, accesat 24.11.2020
8. https://www.bnm.md/ro/content/sistemul-national-de-plati/ , accesat 23.11.2020
9. https://www.bnm.md/bdi/pages/reports/dsp/DSP1.xhtml, accesată 24.11.2020
10. https://www.bnm.md/bdi/pages/reports/dsp/DSP2.xhtml/ , accesat 24.11.2020
11. https://ro.wikipedia.org/wiki/3D_secure , accesat 25.11.2020
12. http://www.bancamea.md/news/cumparaturile-pe-internet-au-devenit-mai-protejate-odata-cu-implementarea-sistemului-de-securitate-3d-secure, accesat 25.11.2020
13. http://www.bati.md/ , accesat 25.11.2020
14. https://www.bnm.md/bdi/pages/reports/dsp/DSP4.xhtml , accesat 25.11.2020

Information Security

IoT APPLICATION IN SMART CITIES WITH AN ACCENT ON T RAFFIC AND TRANSPORTATION

Čekerevac Zoran
DSc, Professor
"UNION-Nikola Tesla" University in Belgrade (Serbia)
e-mail: zoran@cekerevac.eu

Prigoda Lydmila
DSc, Professor
Maikop State Technological University, Maykop, Adygeya Republic, Russia
e-mail: lv_prigoda@mail.ru

Bogavac Milanka
PhD, Professor
"UNION-Nikola Tesla" University in Belgrade (Serbia)
e-mail: bogavac.milanka@gmail.com

Abstract
With the increasing influx of population, live in cities is becoming increasingly difficult. The paper analyzes the implementation of IoT in some areas of functioning of "smart cities" with emphasis on the organization of transport and the application of new technologies in this regard. Some examples from advanced cities are also presented.

Keywords: *smart city. IoV. IoT. transportation. urban traffic*

JEL Classification: *L86, I13*

INTRODUCTION

With the increasing influx of population, live in cities is becoming increasingly difficult in every respect. From the organization of supply, life, and work, to the liberation of cities byproducts of the population living in them. Each area individually needs to be refined, and it is improving. Since the improvement of one area of life usually influences another, and that the accelerated development of one area does not mean general improvement, there appeared the concept of the so-called "smart" cities. They should provide an overall comfortable, economical, sustainable, and safe life for their residents. Basic support for this idea is provided by information technologies based primarily on IoT, wireless communications, innumerable sensors, and above all by the Internet and LPWAN and 5G networks. Deployment of a wide range of IoT applications should provide smart infrastructure in areas such as transportation, electricity, water supply, waste disposal, residential construction, and public services.

We will not discuss here the potential harmfulness of new technologies to health since hardly any epochal invention has remained unused. We will keep the focus on the technical, technological, and social aspects of the application of IoT in traffic in smart cities hoping that living organisms can evolve aligning with new living conditions.

SMART CITIES AND IoT

According to Gulan [1] in January 2019, there were 4,709 settlements or villages in Serbia (according to the Constitution of the Republic of Serbia, there is no category of

villages), of which 1,200 are in the phase of disappearance, with 50,000 empty houses without owners and another 150000 in which no one is living. At the same time, the population of the capital, Belgrade, from the million it had in the early 1970s, rose to 1,639,121, of which 1,166,800 live in the central part (according to the 2011 Census [2]**), with a tendency of further growth towards an estimated 1,215,996 inhabitants in the central part of the city in 2020** [3]**. According to the Bureau of Statistics** [4] **during 2018, 122,193 persons changed their place of residence, i.e. permanently moved from one to another settlement of the Republic of Serbia. Mostly, migration leads to cities. Also, the total population of Serbia tends to fall.**

The situation is similar in the surrounding countries and the whole world. According to the UN, today, 54% of people around the world live in cities, and by 2050 that percentage should rise to 68% [5]. The growth of urbanization will also entail an increasing number of problems. More and more people in a confined space will mean higher traffic density, and therefore more air and noise pollution, less green space, and more traffic jams, leading to the need for intelligent transport systems and vehicles with fewer emissions of toxic components. In this, one should not see only air pollution, but pollution of nature in general.

A smart city is a framework, consisting mainly of information and communication technologies (ICT). A large part of the ICT framework is an intelligent network of connected objects and machines that transmit data using wireless technology and the cloud. Cloud-based IoT applications receive, analyze data, and enable real-time responses. Communities can improve energy distribution, facilitate the waste collection, reduce traffic density, and even improve air quality with the help of IoT.

Many cities have started implementing some IoT solutions. Planned or unplanned, but IoT solutions are being introduced in many areas. One of the most visible is the introduction of surveillance systems that provide insight into the movement of vehicles (and people). In addition to allowing traffic congestion to be monitored, these systems are also used for other purposes, including controlling the speed of vehicles on the streets.

Belgrade, Serbia, and surroundings

Initiatives related to the smart city approach are often mentioned in Serbia, but except for the Smart City Festival, the Smart City SEE19 regional conference, and individual competitions for "best smart city solutions", there is little organized action. What leads to a smart city generally takes place within the individual, weakly, and rarely connected projects. Noticeable displays are showing the number of vacancies in certain public city garages, several displays on the part of the highway passing through the city, which indicate the state of the highway. And, this is more or less all that is visible to the residents. The city of Niš was selected to be a pilot project of the smart city initiative. If the project realizes as it was conceived, Niš could become the first smart city in the region. Sensors will guide drivers to the parking spot. Digital monitoring of waste containers will show when the containers are full. Remote detection of malfunctions in the water supply system will be applied as well as the systems that read the energy consumption. [6]

At the end of 2019 and early 2020, an air quality measurement system arose to the focus of the people in Serbia. The population was able to monitor the level of air pollution in some cities and some parts of the cities. It turned out that the air breathed by the people very often and for a long time was at the level of "dangerous" and that Serbian cities, including Belgrade, were in the group of the most polluted cities in the world. The situation was similar in Sarajevo, Tuzla, Zenica, Pljevlja, Peja, Strumica, Lisice, etc. A network of Klimerko devices was formed in Serbia, which provided the population with results on the state of the air through the website vazduhgradjanima.rs. Although the

accuracy of measurement can be discussed, it is evident that these IoT systems have influenced the awareness of the population. Many went for the purchase of masks and air purifiers, and a significantly reduced number of people on the streets was visible.

Amsterdam

Amsterdam, as one of the leaders in creating smart cities, launched an initiative ten years ago to improve its economy, environment, government, living, and mobility. Within the Smart City (ASC) project, seven areas have been identified with several different activities. More details on this initiative can be found at [7], and only some of them, closely related to the topic of this paper, will be cited here.

1. Infrastructure and technology:

a) *Investing in Internet traffic*. Due to its geographical location, Amsterdam is in a situation where 11 of the 15 transatlantic data cables either pass through or are connected to Amsterdam. In this way, Amsterdam is the second-largest Internet exchange point in the world.
b) *IoT living lab*. An area of 3,700 square meters was equipped with IoT-enabled smart beacons that communicate via LoRaWan. Users can access data from the beacons using Bluetooth-enabled devices. The data user can use for developing their apps. The idea was to let startups and innovators test IoT solutions in real urban environments.
c) *City alerts*: oriented to provide operation instructions to rescuers in real-time. [8]
d) *Smart city lighting*: Special LED lighting goes up when cyclists are nearby and dims after they pass.

2. Smart energy: Amsterdam is working to increase energy use from renewable sources. In addition to maintaining such facilities, the city also allows residents to produce electricity and exchange it using the GridFriends system. They can also install solar panels. The Comfort cooling system is in use to cool buildings in the Amsterdam Houthaven district by transmitting heat to a river that flows nearby.

3. Smart mobility: Amsterdam residents traditionally use their bicycles for transportation massively. 63% of residents use their bicycles daily. Also, there is an increase in the number of electric cars by 53% in 2016 and in the car-sharing, which saw an increase of 376%. Although noticeable, car-sharing is still at the level of somewhere about 1% of the total number of car rides. [9] Also, it is interesting the application of the Parkshuttle, an autonomous platform that can carry around 2500 passengers daily with five stations using six vehicles.

4. Circular city: The idea is that everything produced in the city is recycled in the city for producing new products and services, and to reduce waste and costs for the procurement of raw materials.

Seul

By 2024, Seoul plans to invest the US $ 1.24 billion in turning the city into a "capital of big data." [10]. According to the same source, over 50,000 IoT sensors will be deployed throughout the city. These devices will collect data on dust, light intensity at night, pedestrian and vehicle movements, and many other things that will help city authorities come up with an appropriate policy. And surveillance cameras will get smarter. The Seoul administration plans to install additional 17,280 surveillance cameras by 2021 with algorithms that automatically notify the police about brawls/fights and other forms of misconduct. Free Wi-Fi will expand so that all city buses will have free Wi-Fi in 2020. [11] Also, electricity consumption in 1000 single-member households with one senior member will be monitored to avoid dangerous situations.

Singapore

Singapore is using digital innovation to offer the best public services to its citizens, and the local government has implemented many projects under the "Smart Nation" initiative. For example, more than 52,000 surveillance cameras have been set up to enable police to respond quickly in the event of any problem. Also, the "eXchange" platform enables state-owned agencies to exchange data, while the "OneService" mobile application directs citizens' complaints to the competent institutions. [12]. Within transportation projects there were launched [13]:

– *Autonomous vehicle trials in Singapore*; In 2015, A*STAR's self-driving vehicle was the first vehicle of its kind to receive regulatory approval for public road testing.

– *Contactless fare payment for public transport* uses RFID technology.

– *On-demand shuttle*; The shuttle can be booked using smartphones, and the shuttle can pick up passengers from their doorstep, as a taxi does.

– *Open Data and Analytics for urban transportation*. Tracking the vehicles, the land transport authority reduced the rate of overcrowded buses by 92%.

Helsinki

Helsinki is constantly listed as one of the most affordable cities to live in, but in 2019 it was named Capital of Smart Tourism. Vapaavuori said [14]: "We are big enough to enable tests, demonstrations, and pilots in a systemic relevant way. But at the same time, we are small enough to make it happen and good enough to make it feasible. … we see the city as a platform, as an enabler, as a partner, not as a bureaucracy". One of the interesting solutions implemented in Helsinki is that ten years ago a metro station was built in Kalatasama, a district that was then "mostly wasteland and grim office buildings". With the opening of the metro station, conditions were created for the rapid settlement of the area, but on a "smart city" basis. The goal of this successful initiative was to disperse the city center and keep the city comfortable for life despite its expansion.

SMART CITIES AND IOV

The car is being an important factor in the lives of people for a long time, not only those who drive it or work in the automotive industry but also those who are exposed to its influence, whether it be the exhaust, noise, or physical endangerment. For traffic jams, solutions are found through projects based on the use of computer systems and simulations of different traffic cases. Thus, modern cars have become mobile platforms that supply drivers with a wealth of information about the condition of the vehicle and the state of the environment in which the vehicle moves, and even assume some of the functions of vehicle control. The application of modern information technologies encourages the establishment of new infrastructure consisting of networks of roads, railways, airports, stations, and ports connected by Internet-based systems. The efficiency and quality of transport are significantly influenced by intelligent systems that improve the mobility and safety of road users. By implementing an IoT solution, traffic regulation has the effect of increasing safety, thereby directly reducing the number of traffic accidents while increasing passenger satisfaction. Future solutions will be based on the implementation of smarter and more environmental-friendly vehicles and their connection to infrastructure facilities such as streets, signage, gas stations, parking lots, garages [11].

The term Internet-of-Vehicles (IoV) represents the paradigm of one of the directions for the development of smart traffic and an area that has been given special attention in recent years, both from a technical and technological point of view, for example [15], and from an ethical point of view, e.g. [16].

IoV involves the hybrid use of IoT devices, various wireless communication technologies, cloud and Internet services, and applications. This concept enables the collection and sharing of information about vehicles, infrastructure, and the environment. Moreover, IoV makes it possible to process, calculate, share, and publish information on information platforms available to most users today. On the other hand, based on this data, real-time monitoring, and management of the city's traffic-transport system, as well as the creation of BigData for the full range of multimedia and mobile Internet applications, are enabled.

The most important task of IoV architecture is to connect vehicles to heterogeneous wireless networks, as well as to interconnect them. In doing so, copies of the data generated on the vehicle itself are transmitted in different ways to the environment while retrieving data from the same environment. Many sensors, microcontrollers, RFIDs, and other technical solutions are built into the whole process. This plethora of data, vehicles, infrastructure objects interconnected using a distributed ad hoc vehicular network had created a new network and computing paradigm specifically designed for vehicles—the vehicular fog [15]. The urban vehicles fleet is evolving rapidly to the Internet cloud, and a network of autonomous vehicles (AUVs). In its path, the IoV architecture has many unresolved issues, primarily caused by the heterogeneity of networks and devices. One of the first solutions of a layered architecture is proposed in the paper [17]. This five-layer IoV architecture is shown in Figure 1. Given that it is explained in more detail in the original paper, only some basic characteristics of individual layers will be indicated here:

1. The Perception layer is characterized by a variety of sensors and devices connected to the network.
2. The Coordination layer is reflected in the virtual universal network coordination module for heterogeneous networks.
3. The third level is represented as the virtual cloud infrastructure, and it is the brain of IoV and responsible for the information received from layer 2 and decision making based on the critical analysis.
4. The application layer consists of smart applications and it is oriented to the end-users.
5. The fifth layer of the architecture, represented by the operational management module of IoV, is aimed at foresight strategies for the development of business models.

The interaction model of IoV network

The IoV network model should enable the efficient, safe, and reliable functioning of the IoV system, both by elements and as a whole. The way the model works has been analyzed in numerous pieces of literature, with each part broken down into details, but here it is convenient to use the model to be divided into hardware, software, and users. These components can be considered individually, but also unified as in the case of users, communications, and clouds that work closely together. This division of the IoV model emphasizes the functionality of its concept. Sensors and devices installed at the site of use are the first basic elements. The choice of sensors and devices depends on what one wants to accomplish, so they are very heterogeneous.

Software is what brings life to the system and makes it possible to achieve the goal. This includes all types of software, from drivers and communications software to user applications. Different types of devices or smart applications may individually implement one or more of the same or different types of wireless access connections, depending on the priority and preference for services.

The third basic element is the network of users whereby the user can be understood as a human participant in the traffic (driver, passenger, pedestrian) as well as the autonomous vehicle.

No.	Layers	Representation	Functionalities
5.	Business	Graphs, Flowchart, Table, Diagram	• Business model and investment designs • Resource usage and application pricing • Budget preparation, data aggregation
4.	Application	Smart applications for vehicles and vehicular dynamics	• Smart, intelligent services to end users • Service discovery and integration • Application usage data and statistics
3.	Artificial Intelligence	Cloud computing, big data analysis, expert systems	• Storing, processing, analysis of data • Analysis based decision making • Service management based on profit
2.	Coordination	Heterogeneous Networks: WAVE, WiFi, LTE	• Unified structure transformation • Interoperability provisions • Secure transportation of information
1.	Perception	Sensor and actuator of vehicles, RSU, personal devices	• Data gathering: vehicle, traffic, devices • Digitization and transmission • Energy optimization at lower layers

Figure 1. The five-layered architecture of IoV

Source: [17]

Different interactions can be established between these components of the IoV model. A systematic schematic presentation of these relationships is shown in Figure 2.

If looks at Figure 2, one can see the full variety of model factors. They vary in many characteristics, including the technology they use, response speeds, signal strength, the protocols they use, and their relevance to specific issues. If a communication network is considered, there are two types of communication. The intra-vehicular communications are focused on communications inside the vehicle supporting V&P devices, V&S, and Sensors and Actuators (S&A). The extra-vehicular communications are focused on communications between the vehicle and surroundings.

Most modern IoT networks are based on LPWAN (Low-Power Wide-Area-Network) which is designed to wirelessly connect the "things". LoRa (Long Range) is a spread spectrum modulation technique derived from Chirp Spread Spectrum (CSS) modulation technology. [19]

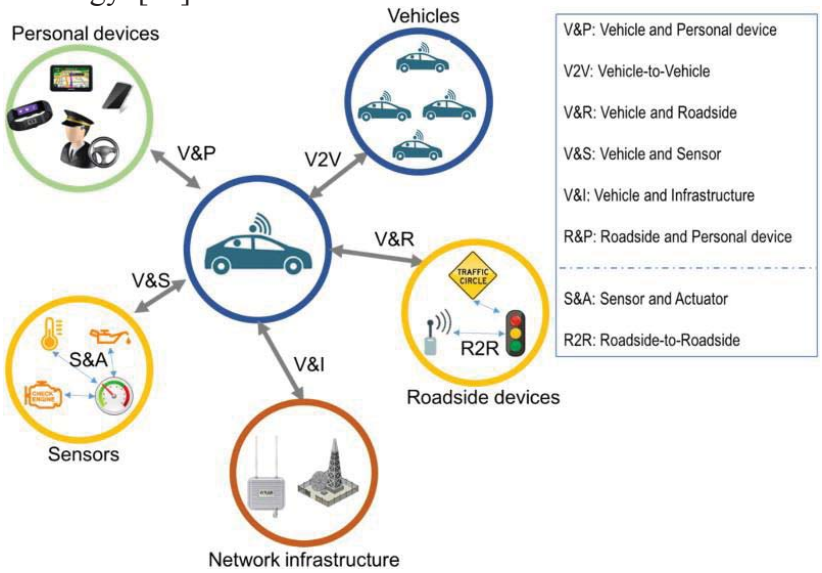


Figure 2. Device-to-device interaction model for IoV

Source: [18]

Many LPWA technologies allow communication over distances measured in hundreds of kilometers, but their flow rates are limited to a few kilobits per channel and second. Although much hope is being placed in 5G networks, 75% of the IoT market is expected to come from LPWA network solutions, and 25% to high-bandwidth low-latency 5G applications. [20] One of the main advantages of LPWAN is that such networks already exist and that it will take years of work to deploy 5G networks. Another advantage is that the LPWAN does not require massive infrastructure like in the case of 5G networks. The network can be formed based on small, very smart, and not very expensive devices.

IoV software

The software part of the IoV model includes software components that are embedded in sensors and devices and an application, user part. The first group is inevitably tied to the sensor and equipment manufacturer and as such is of little interest to end-users. The second group is much more interesting to the end-users and can be divided into two basic groups:

✓ *Security and management-oriented applications:* security, navigation, diagnostics, and telematics; and

✓ *Business-oriented applications:* insurance, car sharing, information and entertainment applications

✓ By their purpose, IoV security and management-oriented applications are intended for various security functions such as:

✓ *Traffic accidents prevention*. This group is a vehicle security M2M [The M2M system is a set of technologies that allow devices to communicate with each other over a wired or wireless network] communication system. Its function is to prevent traffic accidents by exchanging real-time information between different vehicles. Such a system would be very useful for highways and urban areas with high traffic density.

✓ *Emergency Call*: It is a system that activates in an emergency when it is necessary to contact emergency services such as police, firefighters, roadside assistance, as well as family or friends.

✓ *Navigation:* These applications related to navigation are services based on geo-referenced data. They are already known from GPS devices so far, but it will also be supplemented by data from vehicle video sensors and data from heterogeneous communication networks. There are no obstacles to the introduction of a system that would prevent the driver from driving the vehicle at a speed higher than permitted.

✓ *Diagnostics:* The application refers to vehicle diagnostics to protect it. In addition to real-time vehicle condition monitoring, one of the key operations of these applications is the management of vehicle condition data. It is cloud-based. The application in a timely manner indicates the need to repair or service vehicles.

✓ *Telematics:* This application gives the ability to remotely access parked vehicles using very secure telematics remote applications. Applications are based on precise remote monitoring, authentication, and authorization methods.

✓ *Smart traffic lights:* They are equipped with sensors, data processing, and communication devices. These traffic lights have information about the traffic load (e.g. intersections), as well as the intensity and density of traffic going in all directions. This information can be analyzed and sent to adjacent traffic lights or a central controller.

✓ Business-oriented IoV applications group can be classified as applications related to the economic and organizational aspects of transportation in smart cities. They can be oriented to:

✓ *Insurance:* The insurance-related applications are based on a statistical analysis of information including vehicle use, driver behavior, place of use, and duration of vehicle use.

✓ *Ridesharing*: This application is a special hybrid system of shared transport, also called modified passenger car use. Such applications are based on the concept of improving the use of a passenger car to meet the same transport needs in space and time and reducing the personal costs associated with transportation. Typical representatives of this subsystem are the common private car (Carpool), the common private minibus (Vanpool), and the common car (CarSharing). The application locates users who make the same or similar transportation requests and connects them to the car owner. This way a software optimizes the realization of the trip based on the aligning of the same transport requirements of different passengers. Undoubtedly, this approach runs counter to taxi carriers' will.

✓ *Infotainment*: Starting from the concept of connection of home, work and general mobility, this type of application implies the availability of different information while driving, and the synchronization of the onboard display with an office or home computer, smartphone, or other online devices.

Decision making

One of the most important functions of an IoV system is decision making. Due to the movement of vehicles in a changing environment, there is a constant danger to the safety of road users and a constant need for decision making. All data collected has a purpose and is expected to be used in real-time. To ensure that the right decision is made on various issues, it is necessary to create appropriate criteria, boundary conditions, and to ensure the possession of quality data. Given the diversity of traffic conditions, the criteria must be comprehensive and cover even the rarest expected situations. Along with the creation of technical solutions, appropriate legislation should be created, which should be adapted to the new conditions. One of the most logical questions is who is at fault in the event of an accident if the vehicle is autonomous? Until the system is perfected, the driver will often listen to the message "Put your hands on the steering wheel!". However, not all decisions are fateful. There are many decisions that IoV systems can make independently, without endangering traffic users. For example, vehicle and infrastructure data can be provided to the appropriate traffic safety and regulation platform, and the platform can create and forward commands to the traffic light system and driver alert system. This could reduce traffic congestion, fuel consumption, and reduce the emission of toxic gases into the atmosphere.

CONCLUSIONS

Population migration has always existed and will continue to exist. And it is good as long as the migration is small-scale and related to the personal desires of individuals. It is not good when it is massive and a consequence of the struggle to maintain a bare existence. There is a noticeable increase in the population in large cities as a result of the newcomers' hope that they will live better in the big city than in the place of their current life. Instead of providing a better living environment in a place where people are born, society does nothing, and people are moving to (big) cities. Because of the growing population in (big) cities and the difficult organization of life in new conditions, smart cities are a necessary orientation. For the city to survive at all, it must become "smart", and this requires major investments in all areas and especially in technology and technological development, but also in the way of thinking of the people who live in them. There is no

technical solution that can meet all the challenges in real-time. The challenges are numerous despite all the technological solutions based on IoT, IoV, M2M, 5G, LPWAN, and other technologies. Life in big cities can be expected to become increasingly uncomfortable. The solution could be found in the decentralization of large cities and the development of villages and towns in the interior.

BIBLIOGRAPHY

1. B. Gulan, "Stanovništvo u naseljima – selima Srbije na početku 2019. godine," 29 01 2019. [Online]. Available: https://www.makroekonomija.org/0-branislav-gulan/stanovnistvo-u-nasel%D1%98ima-%E2%80%93-selima-srbije-na-pocetku-2019-godine/
2. RZS, "Ključni pokazatelji," 2011. [Online]. Available: https://www.stat.gov.rs/sr-latn/oblasti/popis/popis-2011/
3. Population.City, "Beograd - Broj stanovnika," 2011. [Online]. Available: http://brojstanovnika.population.city/srbija/belgrade/
4. RZS, "Unutrašnje migracije - 2018," 28 06 2019. [Online]. Available: https://www.stat.gov.rs/sr-latn/vesti/20190628-unutrasnje-migracije-2018/?s=1806
5. UN, "68% of the world population projected to live in urban areas by 2050, says UN," 28 12 2019. [Online]. Available: https://www.un.org/development/desa/en/news/population/2018-revision-of-world-urbanization-prospects.html [Accessed 28 12 2019]
6. J. Subin and D. Matović, "Novosti istražuju i Srbija će imati "pametne gradove"," 20 May 2019. [Online]. Available: https://naslovi.net/2019-05-21/vecernje-novosti/novosti-istrazuju-i-srbija-ce-imati-pametne-gradove/23430914
7. HEREmobility, "Amsterdam's Smart City: Ambitious Goals, Collaborative Innovation," 2019. [Online]. Available: https://mobility.here.com/amsterdams-smart-city-ambitious-goals-collaborative-innovation [Accessed 28 12 2019]
8. B. v. '. Padje, B.-J. Knegt, J. Soetendal, R. Koreman, and R. v. d. Lans, "City Alerts," 2019. [Online]. Available: https://amsterdamsmartcity.com/projects/city-alerts
9. R. Kok, E. v. d. Veen, S. Balm, S. d. Rijke and M. Altenburg, "Mobility," 2017. [Online]. Available: https://amsterdamsmartcity.com/themes/mobility
10. Yonhap, "Mayor Unveils Plan to Transform Seoul into 'Smart' City," 13 3 2019. [Online]. Available: http://koreabizwire.com/mayor-unveils-plan-to-transform-seoul-into-smart-city/134009
11. T. Pećnik, "Primena IoT u saobraćaju i transportu," unpublished, Belgrade, 2020
12. Smart Nation Singapore, "OneService App," 2014. [Online]. Available: https://mobility.here.com/singapore-smart-city-holistic-transformation#pgid-153
13. HEREmobility, "Smart City Initiatives," 29 12 2019. [Online]. Available: https://mobility.here.com/singapore-smart-city-holistic-transformation
14. CGTN, "What makes Helsinki such a 'smart' city?," 28 Nov 2019. [Online]. Available: https://news.cgtn.com/news/2019-11-22/What-makes-Helsinki-such-a-smart-city--LPGwcllOdG/index.html
15. E.-K. Lee, M. Gerla, G. Pau, U. Lee, and J.-H. Lim, "Internet of Vehicles: From intelligent grid to autonomous cars and vehicular fogs," *International Journal of Distributed Sensor Networks,* vol. 12, no. 9, 6 Sep 2016.
16. R. Silva and R. Iqbal, "Ethical Implications of Social Internet of Vehicles Systems," *IEEE Internet of Things Journal,* vol. 6, no. 1, pp. 517-531, Feb 2019
17. O. Kaiwartya, A. H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C.-T. Lin and X. Liu, "Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects," *IEEE Access,* vol. 4, pp. 5356-5373, 2016

18. J. Contreras-Castillo, S. Zeadally, and J. A. G. Ibáñez, "A seven-layered model architecture for Internet of Vehicles," *Journal of Information and Telecommunication,* pp. 4-22, 02 Mar 2017
19. L. Slats, "A Brief History of LoRa®: Three Inventors Share Their Personal Story at The Things Conference," 08 Jan 2020. [Online]. Available: https://blog.semtech.com/a-brief-history-of-lora-three-inventors-share-their-personal-story-at-the-things-conference
20. J. Blackman, "LoRa shoots for 75% of IoT market, versus 25% for 5G; aims for stars with satellite constellation," 18 Jun 2019. [Online]. Available: https://enterpriseiotinsights.com/20190618/channels/news/lora-shoots-for-75pc-of-iot-market
21. HEREmobility, "Smart City Initiatives," 29 12 2019. [Online]. Available: https://mobility.here.com/singapore-smart-city-holistic-transformation

KEY SEGMENTS OF THE DIGITAL SHADOW ECONOMICS

ОСНОВНЫЕ СЕГМЕНТЫ ТЕНЕВОЙ ЦИФРОВОЙ ЭКОНОМИКИ

Охрименко Сергей
Доктор экономических наук, профессор
Академия Экономичексих Знаний Молдовы
e-mail: osa@ase.md

Бортэ Григорий
Кандидат экономических наук, доцент
Академия Экономичексих Знаний Молдовы
e-mail: grigori.borta@gmail.com

Abstract
This article highlights and discusses new segments of the shadow digital economy. Among them, such as cyber weapons, as the concentration of all the achievements of information and communication technologies at the level of counteraction between states; targeted attacks and ATR groups; attack on cryptocurrency exchanges; identity theft. Statistical data characterizing these segments of the shadow digital economy is analyzed.

Keywords: *shadow digital economics, information security, threats in information security, cryptocurrencies, cryptoexchanges.*

JEL Classification: *E26 F52 J46 H56*

ВВЕДЕНИЕ

Настоящая работа является логическим продолжением исследований теневой цифровой экономики (ТЦЭ), нашедших отражение в ряде публикаций авторов, в частности таких, как [2], [6], [7]. Одной из важных задач выступает не только определение категории ТЦЭ, но и ландшафта современных угроз. В частности, процессы цифровой трансформации экономики (например, реализация концепции «Индустрия 4.0») породили новые угрозы [4]:

- атаки становятся все более изощренными за счет автоматизации и использования методов искусственного интеллекта и машинного обучения;
- подключение огромного количества новых незащищенных устройств (промышленный интернет или интернет вещей, как сеть передачи данных между физическими объектами, которые оснащены встроенными средствами и технологиями взаимодействия друг с другом или с внешней средой). Хакеры используют для входа в сеть такие устройства как, видеокамеры, кофемашины и др.;
- в результате резко возрастает количество целей для атак.

Авторы изучили состав основных продуктов и услуг криминальной направленности, относящихся к ТЦЭ. Но их спектр постоянно изменяется, появляются новые сегменты, требующие исследования и описания. В данной статье будет рассмотрены следующие сегменты: кибероружие, как сосредоточение всех достижений информационных и коммуникационных технологий на уровне противодействия между государствами; целенаправленные атаки и АТР-группы; нападение на криптобиржи, кража личных данных.

КИБЕРОРУЖИЕ

Под кибероружием понимается вредоносное программное обеспечение, используемое в военных или разведывательных целях. В последнее время всплывает всё больше и больше случаев подобного использования программного обеспечения. Одна из основных характерных черт подобных атак - узкая направленность, в отличие от киберпреступников, стремящихся заразить как можно большее количество жертв. Чаще всего подобные разработки спонсируются или проводятся государственными учреждениями. Наиболее яркими примерами подобного программного обеспечения служат Stuxnet, Falme, Duqu, Gauss. Почти всегда в подобных вредоносных программах используются уязвимости нулевого дня.

К числу стран, официально объявивших о наличии специальных подразделений, чья деятельность связана не только с кибероборoной, но и кибератаками, являются следующие: США, Великобритания, Российская Федерация, Франция, Германия, Эстония, Иран, Израиль, Южная и Северная Корея, Китай. Австралия и др.

Основными событиями выступают следующие [5]:

1) 1982 – Взрыв на советском газопроводе в Сибири. По слухам, причина взрыва – «закладка» в программном обеспечении, которое использовалось в управляющей системе.

2) 1997 – Операция “Eligible Receiver”. Первые полноценные киберучения. Внутренняя операция американских спецслужб, в процессе которой были атакованы сервера других государственных институтов США.

3) 1998-2000 – Операция “Moonlight Maze”. Атакованы Пентагон, NASA, Департамент энергетики, исследовательские компании и университеты США.

4) 2003-2006 – Операция «Титановый дождь». Атакованы NASA, Lockheed Martin, Sandia National Laboratories, Redstone Arsenal. Точные масштабы нападения неизвестны, однако в нем подозревают китайских хакеров либо кого-то, кто использовал для этого расположенные на территории Китая компьютеры.

5) 2006 – Израиль использует киберсредства в ходе конфликта с группировкой Hezbollah.

6) 2007 – Множественные хакерские атаки на правительственные и военные структуры США, Германии, Индии.

7) Апрель 2007 – DDOS против Эстонии. Серия массированных DDoS-атак на эстонские государственные порталы началась 27 августа, сразу после решения правительства перенести статую бронзового солдата в Таллине. Данная атака привела к созданию в Эстонии Европейского центра по борьбе с киберугрозами. В организации нападения некоторые специалисты обвиняют структуры, близкие к движению «Наши».

8) Сентябрь 2007 – Операция Orchard. Израильская бомбардировка ядерного центра в Сирии. Кроме массированных авиа-ударов использовалась специальная, предварительно внедренная вредоносна программа, которая влияла на работу радаров.

9) 2008 – Массовые атаки и взломы правительственных и прочих Интернет-ресурсов Грузии во время операции «Принуждение к миру» в Южной Осетии.

10) 2009 – Операция «Аврора». Серия кибератак, инициированных в 2009 году структурами, близкими к Китайской народной освободительной армии, против американских интернет-гигантов, по большей части Google.

11) Нападение на Корею. Более 166 тыс. компьютеров были инфицированы вирусом, сделавшим их частью огромного ботнета, чей атакующий потенциал был

направлен против правительственных, финансовых и медийных сайтов Южной Кореи.

12) 2010 – Операция Myrtus. Червь Staxnet был обнаружен в Иране. Целью червя стали программируемые логические контроллеры. Эти устройства обслуживают моторы, работающие на крайне высоких частотах, которые установлены в Иране только на заводе по обогащению урана.

13) Атака на Бирму. Мощнейшая DDoS-атака на крупнейшего интернет-провайдера Бирмы началась незадолго до первых за 20 лет всеобщих выборов, впоследствии признанных фиктивными.

14) АЭС В БУШЕРЕ, ИРАН. По версии New York Times, компьютерный червь Stuxnet был разработан спецслужбами США и Израиля специально для саботажа иранской ядерной программы. По данным Symantec, вирусом оказалось заражено 58,85% компьютеров Ирана, 18,22% компьютеров Индонезии и 8,31% машин в Индии.

15) 2012 – Операция ABABIL. Общее название для серии кибератак на американские финансовые институты, инициированной группировкой Cyber fighters of Izz Ad-Din Al Qassam, названной в честь мусульманского проповедника.

16) 2013 – Атака «МЕССИИ». 1 июня государственными регуляторными органами Сингапура были приняты новые правила: в течение 24 часов все местные сайты с посещаемостью от 50 тыс. посетителей должны были удалить с серверов любые статьи, призывающие к «нарушению расовой либо религиозной гармонии» в стране. В ответ на это хакерская группировка «Анонимусы» инициировала атаку на государственные сайты Сингапура, в том числе сайт премьер-министра.

17) 2014 – Утечка данных из JPMorgan Chase. Крупнейший американский банк, один из старейших финансовых институтов на планете подвергся серьезной хакерской атаке, в результате чего более 83 млн счетов были скомпрометированы. По одной из версий, за нападением стояли русские хакеры, также атаковавшие другие банки США.

18) Операция CLEAVER. Согласно отчету компании Cylance, к массовой атаке на 50 объектов из 16 стран (в том числе Korean Air, Qatar Airlines, Pemex) оказались причастны иранские хакеры, тесно связанные с Корпусом стражей исламской революции.

С ростом киберугроз расходы в области кибербезопасности постоянно растут (в том числе расходы на брандмауэры и анализ угроз) со стороны правительств и частного сектора неуклонно растут, и по оценкам [1], стоимость приближается к 0,1% мирового ВВП. Некоторые исследователи утверждают, что существующую риски и издержки, связанные с облачными технологиями и 5G, перевешивают выгоды от цифровизации [9], [15].

Еще одним немаловажным аспектом является стоимость потерь от кибершпионажа. Например, по данным Центра стратегических и международных исследований (CSIS, https://www.csis.org), в 2014 году глобальные затраты на кибербезопасность составили до 575 млрд. дол. (или 0,8% от мирового ВВП). Для Европейского Союза стоимость оценивается в 0,41% ВВП или 55 млрд. дол. в год. По расчетам страховой компании Lloyd's срыв облачного сервиса может привести к значительным экономическим потерям, которые могут варьироваться от 4,6 млрд. дол. До 53,1 млрд. дол. Или 0,07% мирового ВВП [10]. Кибершпионаж очень дорого обходится Европейскому Союзу – как результат подобных действий - ежегодно теряются 55 млрд евро, 289000 рабочих мест находятся в опасности. Подобные существенные потери будут возрастать с расширением процессов цифровизации

(поколение 5G, Индустрия 4.0), по прогнозам ожидается появление в сети 26 000 000 000 новых устройств. Естественно можно предположить, что возрастут атаки на информационные системы и ресурсы, изменится их состав и количество.

ЦЕЛЕВЫЕ (ЦЕЛЕНАПРАВЛЕННЫЕ) АТАКИ

Проанализируем содержание данного термина. Специалисты по информационной безопасности по-разному трактуют термин advanced persistent threat (APT). Среди вариантов: «расширенные постоянные угрозы»; «продвинутые», «развитые», «сложные», «целевые», «целенаправленные» и «таргетированные» угрозы. Эксперты Positive Technologies определяют APT как хорошо организованную, тщательно спланированную кибератаку, направленную на конкретную компанию или целую отрасль. В ходе нее злоумышленник получает несанкционированный доступ к сети, закрепляется в инфраструктуре и надолго остается незамеченным. За такими атаками, как правило, стоят APT-группировки, имеющие значительные финансовые ресурсы и технические возможности [22].

В следующей таблице приведено описание целевых кибератак (ATP), нацеленных на интересы ЕС.

Таблица 1. Список целевых кибератак, нацеленных на интересы ЕС

Инцидент, угроза	*Предполагаемый правительственный спонсор*	*Год*	*Затрагиваемые интересы ЕС*	*Примечания*
APT 10	Китай	2017	Великобритания, Франция, Швеция, Финляндия	Китайская группа ATP 10 (или Red Apollo) осуществляет кражу информации, характеризующую интеллектуальную собственность и других конфиденциальных данных из нескольких информационных систем сервис-провайдеров относительно энергетических, финасовых, технологических и медицинских фирм
OPERATION BUGDROP	Россия	2017	Австрия	Американскими и европейскими СМИ сообщается, что операция BugDrop была спонсирована Россией для сбора информации в различных областях, включая данные о критической инфраструктуре, средствах массовой информации и научных исследованиях, включая аудиозаписи разговоров, скриншоты, документы и пароли
“OCEAN LOTUS”	Вьетнам	2015	Германия	Ocean Lotus – группа, поддерживаемая правительством Вьетнама, которая реализовала доступ для получения информации в целях ослабления конкурентных преимуществ (данные частного сектора, правоохранительных органов, кражи интеллектуальной собственности и мер по борьбе с коррупцией) иностранных компаний, проявляющих интерес к потребительским товарам из Вьетнама, производству, гостиничному бизнесу, технологической инфраструктуре и банковскому сектору

UPS	Китай	2015	Великобритания	Фишинговая операция, спонсируемая Китаем. Цель – информация аэрокосмических, оборонных, строительных, инженерных, технологических, телекоммуникационных и транспортных фирм.
EMISSARY PANDA	Китай	2015	Великобритания, Франция	Emissary Panda – китайская операция, направленная на фирмы авиакосмические, автомобильные, технологические и энергетические и другие сектора производства и обороны, а также получение политической и коммерческой информации о конкурентах, инноваций, финансовых, ценовых возможностях и планах развития
ÄXIOM	Китай	2014	Великобритания, Германия, Нидерланды, Бельгия, Италия	Китайская группа, нацеленная на организации, имеющие отношение к стратегическим технологиям, телекоммуникациям, инфраструктуре, экологической и энергетической политике для развития конкурентной борьбы и избавления от иностранных технологий в рамках специального плана
CARETO	Испания	2014	Великобритания, Франция, Испания, Германия, Польша	Возможно, спонсируется Испанией, и науелена на деятельность энергетических и нефтегазовых компаний, научно-исследовательские институты и частные инвестиционные компании. Создана и использовалась сложная программа, способная перехватывать и собирать важную информацию по каналам связи
CROUCHING YETI	Россия	2014	Испания, Германия, Франция, Италия, Ирландия, Польша	Осуществлял слежку за рядом предприятий различных секторов экономики (фармацевтика, автомобильная, сетевая инфраструктура, ИТ). Имел потенциал для совершения диверсий. Приписывается поддержке РФ
PEOPLE'S LIBERATION ARMY	Китай	2014	SolarWorld	Пять офицеров Народно-освободительной армии Китая были обвинены властями США в нацеливании предприятия металлургической, атомной и солнечной энергетики, в том числе на американскую дочернюю компанию немецкой фирмы SolarWorld. Цель – кража информации для использования в конкурентных целях
PEOPLE'S LIBERATION ARMY 61398	Китай	2013	Великобритания, Франция, Бельгия, Люксембург	Подразделение 61398 или APT1, было нацелено на деятельность 141 компаний в 20 основных отраслях, в том числе ИТ, транспорт, технологии, финансовые услуги, инжиниринг, химикаты, энергетика и здравоохранение, которые связаны со стратегическими приоритетами Китая

COMPROMISE OF EADS (AIRBUS) AND THYSSENKRUPP	Китай	2013	EADS/Airbus ThyssenKrupp	Целью была компания ThyssenKrupp из-за позиции основного игрока в мире производства стали. Кража интеллектуальной собственности у EADS (сейчас Airbus), а также планов проектирования, аэродинамических расчетов и смет
NITRO ATTACKS	Китай	2011	Великобритания, Германия, Чехия, Нидерланды, Финляндия, Франция	Спонсируемые Китаем атаки Nitro касались деятельности компаний по разработке и производству химических веществ и интеллектуальной собственности (проектная документация, формулы и производственные процессы)

Источник: Hosuk Lee-Makiyama [1]

ATP-команды по странам:
Китай: ATP41, ATP40, ATP31, ATP30, ATP27, ATP25, ATP24, ATP23, ATP22, ATP21, ATP20, ATP19, ATP18, ATP17, ATP16, ATP15, ATP14, ATP12, ATP10, ATP9, ATP8, ATP7, ATP6, ATP4, ATP3, ATP2, ATP1.
Северная Корея: ATP38, ATP37.
Россия: ATP29, ATP28.
Вьетнам: ATP32.
Неопределенные: ATP5.

Приведенные примеры нелегальных действий и продуктов далеко не исчерпывают всего многообразия. Данный набор постоянно совершенствуется и обновляется с завидной скоростью. В связи с этим, разработка реестра подобных продуктов является весьма актуальной и окажет существенную помощь разработчикам программного обеспечения, персоналу, отвечающему за поддержку информационных систем.

Следует отметить многообразие атак, направленных на разные информационные объекты. В качестве основного объекта следует рассматривать организации кредитно-финансовой сферы. Основной тренд последних лет – использование для компрометации информационных систем и сетей инструментов, предназначенных для проведения тестирования на проникновение. В качестве такого инструмента использовался прежде всего набор программ Cobalt Strike, разработанный американской компанией Strategic Cyber, LLC. В то же время, анализируя способы совершения различных атак, специалисты ФинЦЕРТ обоснованно предполагают наличие иных преступных групп, использующих похожие инструменты. Большинство атак с использованием Cobalt Strike, наблюдавшихся в 2016 – 2017 гг., реализовали одну из двух схем: конечной целью были либо банкоматы, либо процессинг платежных карт.

Типовая схема целевой атаки на кредитную организацию выглядит следующим образом:

1. Производится массовая рассылка электронных писем, содержащих вредоносные вложения, на адреса организаций кредитно-финансовой сферы.
2. В случае запуска вредоносного вложения из письма на компьютере получателя, проявившего неосторожность, происходит скрытное внедрение программ, чаще всего – загрузчика.
3. После скачивания загрузчика на компьютере устанавливается компонент Beacon – основной инструмент из набора Cobalt Strike. Атакующий получает возможность удаленного доступа к зараженному компьютеру.

4. Атакующий проводит исследование доступных с зараженного компьютера сегментов сети и пытается установить доступ к контроллеру домена сети с целью последующего получения паролей администраторов. Для получения пароля могут быть использованы возможности специальных инструментов (Mimikatz и другие).

5. После получения доступа к контроллеру домена и администраторских паролей атакующий проводит поиск в сети интересующих серверов и компьютеров. Прежде всего ищется компьютер или сервер, с которого есть доступ в подсеть, где находятся банкоматы или иные сегменты сети, например, в сегмент процессинга платежных карт.

6. На банкоматах устанавливается программное обеспечение, взаимодействующее, предположительно, через программный интерфейс XFS и обеспечивающее выдачу денежных средств по команде, подаваемой удаленно. После получения контроля над банкоматами к процессу привлекаются соучастники, занимающиеся получением денежных средств. Их задача – обеспечить присутствие около банкоматов в условленное время для получения денег. После успешной выдачи денежных средств программное обеспечение с банкоматов, как правило, удаляется.

7. В случае получения доступа к процессингу платежных карт привлекаются соучастники, занимающиеся оформлением на подставных лиц платежных карт атакованной организации. Данные карты консолидируются в руках лиц, занимающихся получением денежных средств. Их задача – обеспечить снятие денежных средств в банкоматах непосредственно после того, как балансы и лимиты карт будут повышены в системе процессинга. В процессе получения денег соучастниками оператор может при необходимости продолжать поднимать лимиты по снятию или балансы карт.

8. В случае получения доступа к компьютерным средствам сегмента платежной системы Банка России (АРМ КБР) или системы переводов SWIFT производятся платежи на заранее подготовленные счета, с которых денежные средства далее переводятся и обналичиваются по стандартным для компьютерной преступности схемам.

НАПАДЕНИЕ НА КРИПТОБИРЖИ

Относительно новым направлением является атака на криптобиржи, кража криптовалют и отмывание денежных средств. Высокая рыночная капитализация отдельных криптовалют привлекает хакеров. В качестве примера используем данные, приведенные в таблице 2.

Таблица 2. Криптовалюты по состоянию на 8 мая 2018 года

№ п\п	*Наименование криптовалюты*	*Стоимость (в млрд. дол.)*
1.	Bitcoin	160
2.	Ethereum	75
3.	Ripple	32
4.	Bitcoin Cash	28
5.	EOS	15
6.	Litecoin	9
7.	Cardano	8
8.	Stellar	7,4
9.	IOTA	6,6
10.	TRON	5,5
11.	NEO	5,1
12.	Dash	3,7
13.	Monero	3,6
14.	Ethereum Classic	2,3
15.	Verge	1,1
16.	Zcash	1,1
17.	Decred	0,62

Источник: CoinMarketCap website (https://coinmarketcap.com/)

По состоянию на 23 декабря 2020, года лидерами являются следующие криптовалюты, таблица 3.

Таблица 3. Текущие данные о стоимости основных криптовалют

Название	*Тикер*	*Цена (USD)*	*Рын.кап.*
Биткоин	BTC	23.570	439,57B$
Эфириум	ETH	609,25	69,76B$
Tether	USDT	0,9997	20,47B$
Рипл	XRP	0,31428	14,57B$
Лайткоин	LTC	105,212	7,07B$
Bitcoin Cash	BCH	291,12	5,46B$
Chainlink	LINK	11,82	4,74B$

Источник: Ведущие криптовалюты. https://ru.investing.com/crypto/

Одной из относительно новых видов атак является организация нападения на криптообменники. Специалисты Group-IB провели анализ атак на криптовалютные биржи за последние два года и выявили общие потери в сумме 882 млн $. В отчете указывается, что в 2019 году криптовалютные биржи станут для агрессивных хакерских групп новой целью и их усилия будут перенесены с атак на коммерческие банки. Но в качестве целей выдвигаются не только биржи-криптообменники, но и криптовалютные компании, организующие запуск ICO, сбор средств и предусматривающие продажу токенов частным инвесторам.

ТОП 10 КРИПТОВАЛЮТ ПО КАПИТАЛИЗАЦИИ

Капитализация рынка криптовалют превысила $400 млрд. [18]. Наибольшее внимание инвесторов и трейдеров приковано к тем криптовалютам, которые имеют самую высокую капитализацию. Несмотря на то, что сравнение криптовалют по данному показателю некоторые считают не полностью объективным, именно капитализация является главным фактором, определяющим интерес к отдельной монете со стороны не только покупателей, но и кибермошенников. Для сравнения

приведем данные по 10 криптовалютам по капитализации на начало октября 2020 г., которые представлены в следующей таблице.

Таблица 4. 10 ведущих криптовалют по капитализации на октябрь 2020 г.

Название криптовалюты	*Тиккер*	*Текущая рыночная стоимость*	*Капитализация*
Bitcoin	BTC	$10 610	$196,4 млрд
Ethereum	ETH	$340	$38,3 млрд
Tether	USDT	$1,00	$15,6 млрд
Ripple	XRP	$0,24	$11,1 млрд
Bitcoin Cash	BCH	$219,01	$4,05 млрд
Binance Coin	BNB	$27,45	$3,9 млрд
Polkadot	DOT	$3,81	$3,2 млрд
Chainlink	LINK	$8,80	$3,08 млрд
Crypto.com Coin	CRO	$0,14	$3,02 млрд
Litecoin	LTC	$45,89	$3,01 млрд

Источник: Капитализация криптовалют: Особенности и как влияет на трейдинг [17]

Group-IB обнаружила, что более 10 % средств, привлеченных во время ICO, были украдены. Речь идет о периоде с 2017 года по сентябрь 2018 года. Более половины украденных у ICO средств были связаны с фишинговыми атаками. Целью хакерских групп была не только сама виртуальная валюта, но и списки инвесторов, заинтересованных в ICO, для реализации в будущем таких действий, как шантаж или целевые фишинговые атаки. Примеры успешных атак на криптообменники и соответствующие потери приведены в следующей таблице.

Таблица 5. Примеры успешных атак на криптообменники в 2017-2018 г.г

Дата	*Наименование проекта*	*Страна*	*Группа*	*Потери в криптовалюте*	*Потери в млн $*
Февраль 2017 г.	Bithumb	Южная Корея	-	-	7
Апрель 2017 г.	YouBit	Южная Корея	-	-	5,6
Апрель 2017 г.	Yapizon	Южная Корея	Lazarus	3,816 BTC	5,3
Апрель 2017 г.	Ether Delta	-	Неизвестна	-	0,225
Август 2017 г.	OKEx	Гонконг	Неизвестна	-	3
Сентябрь 2017 г.	Coinis	Южная Корея	Lazarus	-	-
Декабрь 2017 г.	YouBit	Южная Корея	Lazarus	17 % всех активов	-
Январь 2018 г.	Bitstamp	Luxemburg	Неизвестна	18.000 BTC	5
Январь 2018 г.	Coincheck	Япония	Lazarus	532.000.000 NEM	534
Февраль 2018 г.	Bitgrail	Италия	Неизвестна	17.000.000 NANO	170
Июнь 2018 г.	Bithumb	Южная Корея	Lazarus	-	32
Июнь 2018 г.	Coinrail	Южная Корея	Неизвестна	-	37
Июнь 2018 г.	Bancor	-	Неизвестна	-	23
Сентябрь 2018 г.	Zaif	Япония	Неизвестна	-	60
				Итого	882

Источник: Report: Cryptocurrency Exchanges Lost $882 Million to Hackers [14]

Анализ данных, приведенных в таблице, позволяет сделать предварительные выводы. Во-первых, из 14 событий (с февраля 2017 г. по сентябрь 2018 г.) 7 успешных атак были реализованы в Южной Корее, 2 в Японии и по 1 атаке в Гонконге, Люксембурге и Италии. То есть из 14 атак 10 приходятся на Юго-Восточную Азию (71%).

Во-вторых, единственной криминальной группой, которой приписываются успешные атаки, является Lazarus (5 атак из 14, то есть 36%). Хакерская

группировка Lazarus (она же Hidden Cobra) получила известность после успешной атаки на информационные ресурсы Sony Pictures Entertainment (2014 год). Ее деятельность связывают с Северной Кореей (КНДР) и ей приписывают ряд успешных инцидентов, таких как, эпидемия Wannacry, атаками на коммерческие банки в Мексике и Польше и другими фишинговыми атаками.

В-третьих, основной криптовалютой выступает биткойн (BTC), но встречаются и другие альтернативные криптовалюты. В частности, криптовалюта NEM и NANO. 26 января 2018 года японская криптобиржа Coincheck стала жертвой крупной хакерской атаки взлома, в результате чего потеряла 523 миллиона монет NEM на сумму около $534 миллионов. Взлом коснулся только NEM. Поскольку причиной кражи стало отсутствие мер безопасности на самой бирже Coincheck, команда разработчиков NEM отказалась провести хардфорк, чтобы вернуть потерянные средства.

Увеличение интереса к криптовалютам породило развитие массовых атак на данные сервисы. Так, С 2016 по 2017 годы число скомпрометированных учетных записей пользователей криптобирж увеличилось на 369%. В январе 2018 года количество инцидентов выросло на 689% по сравнению со среднемесячным показателем 2017 года. Эксперты Group-IB провели анализ краж 720 пользовательских учетных записей 19 крупнейших криптовалютных бирж и установили, что лидерами по количеству жертв кибератак стали США, Россия и Китай (табл.6).

Таблица 6. Распределение жертв криптобирж по странам

№ п\п	*Страна*	*% украденных активов*
1	США	34,3
2	Россия	10,5
3	Китай	5,0
4	Индонезия	4,5
5	Германия	3,6
6	Украина	2,8
7	Иран	2,8
8	Словакия	2,6
9	Гонконг	2,6
10	Вьетнам	2,4
11	Турция	2,4
12	Другие	11,1

Источник: Число взломанных аккаунтов на биткоинбиржах в начале 2018 года выросло на 689% [21]

Эксперты Group-IB отмечают, что киберпреступники используют те же инструменты, использовавшиеся при атаках на коммерческие банки, ориентируют их на проведение взлома криптобирж, электронных кошельков и получения доступа к личным данным пользователей. В отчете «2018 Криптовалютные биржи. Анализ утечек учетных записей пользователей» [8] указано, что по меньшей мере 5 из 19 криптобирж стали жертвами целенаправленных атак: Bitfinex, Bithumb, HitBTC, Huobi (табл.7).

Таблица 7. Утечки и жертвы целенаправленных кибератак

Название биржи	*Год*	*Торги 31.01.18 (в $)*	*Торговые пары*	*Число утечек*	*Инциденты с биржей*
Binance	2017	2 222 672 484	252	39	Нет
Bit-Z	2016	236 374 114	69	2	Нет
Bitfinex	2012	1 881 119 042	103	48	Да
BitHumb	2013	1 783 489 020	12	1	Да
Bitstamp	2011	514 697 740	14	48	Да
Bittrex	2014	743 909 464	261	112	Нет
BTCC	2011	103 530 000	4	9	Нет
CEX.io	2013	53 713 354	23	95	Нет
Coinone	2014	222 211 947	9	3	Нет
Gate.io	2017	103 092 086	226	4	Нет
GDAX	2012	926 158 460	12	2	Нет
Gemeni	2014	474 980277	3	19	Нет
HitBTC	2014	494 363 548	421	83	Да
Huobi	2013	1 256 939 172	171	10	Возможно
Kraken	2011	884 409 505	45	61	Нет
KuCoin	2017	157 142 723	212	2	Нет
OKEx	2014	2 701 097 580	422	5	Нет
Poloniex	2014	383 900 716	99	174	Да
Wex.nz	2017	69 440 237	35	3	Нет

Источник: Short Guide on Shadow it Digital Footprinting, Continuous Monitoring & Digital Risk Protection [16]

В апреле 2019 года, криптовалютная биржа Binance сообщила о том, что хакерам удалось за один день вывести более 7 тыс. биткойнов, а также похитить часть данных ее пользователей. Сумма украденных хакерами средств превышает $40 млн. Биржа подверглась «крупномасштабному взлому», причем все средства — более 7 тыс. биткойнов на сумму, превышающую $40 млню – были выведены в несколько этапов и переведены на один кошелек. Binance, одна из крупнейших в мире онлайн-сервисов обмена цифровых валют, была основана в 2017 году в Гонконге. Предоставляет платформу для торговли более чем 100 разных видов криптовалют. В начале 2018 года Binance была крупнейшей криптобиржей по объему капитализации собственной криптовалюты BNB. Ее капитализация составляет $2,9 млрд (7 место в мире). В первом квартале 2019 года прибыль Binance выросла на 66% по сравнению с аналогичным отчетным периодом 2018 года.

Хакеры провели трансакцию так, что она не вызвала подозрений у системы защиты Binance, и та сработала лишь после завершения операции. Средства были выведены с так называемого горячего кошелька биржи, который всегда подключен к сети интернет, в отличие от «холодного кошелька», который работает автономно. В «горячих кошельках» хранится около 2% имеющихся у криптобиржи запасов биткойна. Кроме того, хакерам, по-видимому, удалось похитить часть данных клиентов биржи, в частности коды двухуровневой авторизации, необходимые для входа в пользовательский аккаунт на сайте Binance [20].

Хакерские атаки на криптобиржи превращаются в норму. Так, по данным отчета аналитической компании Chainalysis [11], получили распространение рискованные и незаконные сервисы, в том числе такие, как P2P-обмены, микшерные сервисы, высоко рискованные биржи и игровые площадки, даркнет-рынки, связанные с мошенничеством, похищением и отмыванием средств. Количество атак в 2019 году почти удвоилось по сравнению с 2018 годом (6 и 11, соответственно), а

потери сократились с 875,5 млн. дол до 282,6 млн.дол. Самый большой взлом в 2019 году был осуществлён против сингапурской криптобиржи Coinbene, которая потеряла $105 млн. в токенах ERC-20. Далее идут Upbit, Binance и BITPoint, у которых украли криптовалют на $49 млн., $40 млн. и $32 млн. соответственно.

При содействии криптобиржи Binance удалось задержать трех мошенников, предлагавших киберпреступникам отмывать добычу от шифровальщиков-вымогателей через два десятка «криптообменников» [19]. Киберполицейские Украины при поддержке операторов криптобиржи Binance нейтрализовали банду кибермошенников, которые за два года отмыли около $42 млн через два десятка криминальных «обменников» – точек обналичивания криптовалют. Киберполицейские Украины при поддержке операторов криптобиржи Binance нейтрализовали банду кибермошенников, которые за два года отмыли около $42 млн через два десятка криминальных «обменников» – точек обналичивания криптовалют.

Группа, состоявшая из трех человек начала деятельность в 2018 г. Злоумышленники активно рекламировали свои услуги на подпольных форумах, предлагая, в частности, конвертацию криптовалютных средств, полученных нелегальным образом (то есть, через кибератаки, вымогательство и т. д.), в реальные деньги. Судя по объему отмытых таким образом средств, услуги группировки пользовались большим спросом.

Следует выделить еще одну, немаловажную особенность криптовалют - получение взяток криптовалютой уже несколько лет пользуется огромной популярностью у чиновников и юристов. Такие сделки могут отслеживаться, но ни фактически, ни юридически их нельзя привязать к человеку. То есть формальных доказательств для следствия и суда априори получить невозможно. Более того, криптовалюта сразу оказывается за пределами государства, и конфисковать ее практически невозможно. Но при наличии интернета они все время остаются в распоряжение хозяина. Это своеобразная подушка безопасности для задержанных.

КРАЖА ЛИЧНЫХ ДАННЫХ

Кража личных данных включает такие действия, как перехват идентификационных данных, кредитных карт, логинов и паролей.

В мае 2018 года Европейский Союз ввел обновлённые правила обработки персональных данных, установленные Общим регламентом по защите данных (Регламент ЕС 2016/679 от 27 апреля 2016 г. или GDPR – General Data Protection Regulation) [13]. Данный регламент, имеющий прямое действие во всех 28 странах ЕС, призван заменить рамочную Директиву о защите персональных данных 95/46/ЕС от 24 октября 1995 года. Важным нюансом GDPR является экстерриториальный принцип действия новых европейских правил обработки персональных данных. Новый регламент предоставляет резидентам ЕС инструменты для полного контроля над своими персональными данными. В частности, ужесточается ответственность за нарушение правил обработки персональных данных: по GDPR штрафы достигают 20 миллионов евро или 4% годового глобального дохода компании.

Регламент определяет персональные данные, как любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу (субъект данных), по которой прямо или косвенно можно его определить. К такой информации относится в том числе имя, данные о местоположении, онлайн идентификатор или один, или несколько факторов характерных для физической,

физиологической, генетической, умственной, экономической, культурной или социальной идентичности этого физического лица. Данное определение широкое и достаточно четко дает понять, что даже IP адреса также могут быть персональными данными.

Общий подход к обработке персональных данных сформулирован в виде 6 основных принципов:

1) **Законность, справедливость и прозрачность.** Персональные данные должны обрабатываться законно, справедливо и прозрачно. Любую информацию о целях, методах и объёмах обработки персональных данных следует излагать максимально доступно и просто.

2) **Ограничение цели.** Данные должны собираться и использоваться исключительно в тех целях, которые заявлены компанией (онлайн-сервисом).

3) **Минимизация данных.** Нельзя собирать личные данные в большем объёме, чем это необходимо для целей обработки.

4) **Точность.** Личные данные, которые являются неточными, должны быть удалены или исправлены (по требованию пользователя).

5) **Ограничение хранения.** Личные данные должны храниться в форме, которая позволяет идентифицировать субъекты данных на срок не более, чем это необходимо для целей обработки.

6) **Целостность и конфиденциальность.** При обработке данных пользователей компании обязаны обеспечить защиту персональных данных от несанкционированной или незаконной обработки, уничтожения и повреждения.

Специалисты по информационной безопасности высказывали противоречивые мнения относительно эффективности использования данного регламента. В первую очередь, никто не ставит под сомнение благие намерения законодателей или необходимость того, чтобы компании были более осторожны с конфиденциальной информацией, которой они обладают о клиентах, пациентах и других людях, с которыми они регулярно общаются. Несмотря на то, что положения в GDPR действительно помогают повысить эффективность защиты персональных данных, они также создали новые возможности для использования хакерами и похитителями личных данных этих данных [3].

GDPR установил набор руководящих принципов для управления сбором и хранением данных о потребителях и частной собственности. Многое из этого относится к личной информации, предоставляемой физическими лицами. Участниками этого процесса может быть банковское учреждение, страховая компания, инвестиционная служба или медицинское учреждение. Основная цель заключается в обеспечении надлежащей защиты и исключения возможности третьей стороной несанкционированного использования личной информации сотрудников, клиентов и пациентов этих организаций. Данный регламент устанавливает ключевые области безопасности данных: согласие на сбор и хранение личных данных; уведомление в случае взлома данных; шифрование данных, которое защищает личную информацию в случае нарушения; доступ к личной информации для проверки точности (целостности) и для установки ограничений на предполагаемое использование. Некоторые положения в рамках GDPR были отозваны (это относилось к необходимости в дополнительном персонале для защиты данных за пределами обычной ИТ-команды).

Продолжаются между специалистами в печати дискуссии относительно возможности создания адекватной системы информационной безопасности на базе минимальных стандартов, отвечающей требованиям GDPR. Высказываются мнения,

что хакеры продолжат поиск возможностей вторжения в сеть, используя технологии искусственного интеллекта для поиска уязвимых точек, а также анализ и отслеживание их на предмет возможных кибератак. Нет никаких сомнений, что хакеры пристально изучают новый регламент на предмет поиска «узких» мест и готовят «сюрпризы» службе информационной безопасности. В частности [3], предлагается проанализировать возможные действия хакеров, получивших название «обратного вымогательства». В основе данной схемы лежит использование механизма шифрования данных у пользователя (программа-шифровальщик) и вымогательства денежных средств (в различных криптовалютах, в основном в биткойнах) для восстановления данных. Подобные действия подробно описаны в специальной литературе. Но последовательность действий несколько другая, отличная от технологии вымогательства.

Суть данного действия заключается в следующем:

- хакер проникает в сеть любыми доступными средствами для получения и сбора информации о списках клиентов, которые обеспечены защитой новыми правилами GDPR;
- полученные данные обещают опубликовать публично, что приведет к нарушению регламента GDPR и сделает ответственной организацию за нарушение данного регламента. Соответственно, организацию ждет огромный штраф, который значительно превышает требуемый выкуп.

Второе действие сводится к массовой рассылке фишинговых писем, в которых предлагаются услуги бесплатных консультаций для объяснения GDPR, треннингов и разработку политики безопасности. В случае, если пользователь проходит по указанной ссылке, не исключено, что сайт заражен шпионским программным обеспечением или содержание письма автоматически рассылается коллегам абонента. Невнимательность пользователя может быть самой большой угрозой кибербезопасности.

В январе 2020 года юридическая фирма DLA Piper опубликовала обзор данных о нарушениях, связанных с реализацией GDPR в части утечки персональных данных [12] в 28 странах-членах ЕС, а также Норвегии, Исландия и Лихтенштейна. Приведем основные положения данного отчета.

С 25 мая 2018 года (время ввода GDPR в действие) по 20 января 2020 года в общей сложности было отмечено 160921 случай нарушения данного закона, получивших уведомление надзорными огранами по заащите данных в рамках Европейской Экономической Зоны. За период с 25 мая по 27 января 2019 года в среднем было отмечено 247 уведомлений о нарушениях в день. За период с 28 января 2019 года по 20 января 2020 количество сообщений в день о нарушениях составило уже 278 или рост на 12,6%. Отмечается четкая тенденция роста, хотя подробная информация об утечках не публикуется. Лидерами утечек персональных данных признаны Нидерланды, Германия и Великобритания. Общее количество нарушений персональных данных приведено в следующей таблице.

Таблица 8. Общее количество нарушений персональных данных

№ п\п	Страна	Общее количество нарушений персональных данных, зарегистрированных по юрисдикции за период с 25 мая 2018 года по 27 января 2020 года	Количество нарушений персональных данных, уведомленных по юрисдикции с 28 января 2019 года по 27	Количество нарушений персональных данных, уведомленных по юрисдикции с 25 мая 2018 года по 27	Рейтинг уведомлений о нарушениях в расчете на душу населения	Общая стоимость штрафов GDPR, наложенных с 25 мая 2018 года на 17 января 2020 года в евро
1	Нидерланды	40647	25247	15400	147,2	460 000
2	Германия	37636	25036	12600	31,12	24 574 525
3	Великобритания	22181	11581	10600	17,79	320 000
4	Ирландия	10516	6716	3800	132,52	-
5	Дания	9806	6706	3100	115,43	360 000
6	Польша	7478	5278	2200	13,74	947 345
7	Швеция	7333	4833	2500	48,14	53 639
8	Финляндия	6355	3938	2500	71,11	51 100 000
9	Франция	3459	2159	1300	3,2	-
10	Норвегия	2824	2004	820	37,31	406 210
11	Италия	1886	1276	610	2,05	11 550 000
12	Словения	1845	1105	740	52,55	-
13	Испания	1698	1028	670	2,08	1 381 060
14	Австрия	1644	1964	580	12,1	18 107 700
15	Бельгия	1332	912	420	7,88	39 000
16	Венгрия	749	479	270	4,87	198 000
17	Чехия	720	430	290	4,03	291 717
18	Румыния	668	408	260	1,9	329 500
19	Люксембург	545	345	200	56,97	-
20	Исландия	338	313	25	91,15	-
21	Мальта	239	139	100	31	35 500
22	Греция	232	162	70	1,5	550 000
23	Литва	222	118	105	4,18	67 500
24	Эстония	188	121	67	9,74	-
25	Латвия	173	117	55	6,13	168 930
26	Кипр	94	59	35	4,8	151 900
27	Лихтенштейн	30	15	15	39,18	-
28	Болгария	-	-	-	-	3 156 500
29	Португалия	-	-	-	-	424 000
30	Словакия	-	-	-	-	132 600

Рассчитано по DLA Piper GDPR data breach survey: January 2020 [12].

ЗАКЛЮЧЕНИЕ

За последние несколько лет киберпреступность перешагнула через многие технические и программные преграды и перешла из узкоспециализированной ниши в один из наиболее значительных стратегических рисков, стоящих сегодня перед всем миром. Развитие цифровых форм мошенничества (криптовалюты и ICO, заражение вирусом-вымогателем, установка приложения на смартфон, фишинг и др) во многом способствует развитие технического прогресса.

Какие прогнозы представляют ведущие исследовательские и консалтинговые компании в области теневых ИТ [16]?

По прогнозам исследовательской и консалтинговой компании, Gartner к 2020 году 30% нарушений в информационной сфере будет вызвано теневыми ИТ.

В отчете консалтинговой компании Frost & Sullivan говорится, что более 80% респондентов признают, что используют неутвержденные (теневые) приложения в своей работе.

Исследования, проведенные компанией IDG, свидетельствуют что распространение теневых ИТ ежегодно увеличивается на 5% и составляют около 30% ИТ-бюджетов предприятий.

Исследователи Gartner показали, что Shadow IT составляют от 30 до 40% расходов на ИТ в целом.

Исследования Everest Group зафиксировали, что доля теневых ИТ составляет 50% и более в расходах на ИТ в целом.

БИБЛИОГРАФИЯ

9. Lee-Makiyama H. *Stealing Thunder.* ECIPE, No. 2/18. https://bit.ly/38FuJvs
10. Ohrimenco S., Borta G. *Chapter 8. Challenges for Digital Transformation in the Manufacturing Industry.* Socio-Economic Development. Interdisciplinary Ecosystems Perspective. The Jubilee Book Dedicated to Professor Kazimierz Zielinski. Cracow University of Economics, 2020, Poland, Cracow. – 330 p. ISBN 978-83-8175-233-6.
11. Willis S. *Is GDPR the new hacker scare tactic?* https://bit.ly/3rxcelw
12. Батранков Д. *Первый NGFW с машинным обучением.* https://bit.ly/3mKIjCY
13. Овчинский В., Ларина Е. *Кибервойны XXI века. О чем умолчал Эдвард Сноуден.* https://bit.ly/3mQ45Ft
14. Охрименко С., Бортэ Г. *Новое наполнение науки секьюритологии.* Nauka i praktyka bezpieczeństwa, Wydawnictwo EAS, Kraków, Poland. 2019. P. 112-147. ISBN 978-83-61645-34-4.
15. Охрименко С., Бортэ Г. *Тень цифровой экономики.* Годишник, Том CXXI, Академично Издателство „Ценов", Стопанска Академия "Д. А. Ценов". № 121, 2018. С.79-131. ISSN 0861-8054.
16. Юсуфов Р. *2018 Криптовалютные биржи. Анализ утечек учетных записей пользователей.* https://bit.ly/3poQ9nt
17. *2017 Data Breach Investigations Report.* https://vz.to/3aKNi4q
18. *A Lloyd's emerging risk report.* https://bit.ly/3rtjizK
19. *Crypto Crime Report. Decoding increasingly sophisticated hacks, darknet markets, and scams. January 2019.* https://bit.ly/34LqPQL
20. *DLA Piper GDPR data breach survey: January 2020.* https://bit.ly/3rw67hC
21. *General Data Protection Regulation. GDPR.* https://bit.ly/37RkaGs, https://bit.ly/3pjaQkG
22. *Report: Cryptocurrency Exchanges Lost $882 Million to Hackers.* https://bit.ly/37QWoKV
23. *Risk Nexus. Overcome by Cyber Risks? Economic Benefits and Costs of Alternate Cyber Futures.* https://bit.ly/3nSl0bF
24. *Short Guide on Shadow it Digital Footprinting, Continuous Monitoring & digital risk protection.* https://bit.ly/2WOrRqW
25. *Капитализация криптовалют: Особенности и как влияет на трейдинг.* https://bit.ly/3rtjkaQ
26. *Капитализация рынка криптовалют превысила $400 млрд, но этого все равно мало.* https://bit.ly/34IEw2I

27. *На постсоветском пространстве нейтрализована банда, отмывшая десятки миллионов долларов от кибервымогательства.* https://bit.ly/2KTYrVE
28. *Хакеры похитили более 7 тысяч биткойнов с криптобиржи Binance.* https://bit.ly/38yA8Vq
29. *Число взломанных аккаунтов на биткоинбиржах в начале 2018 года выросло на 689%.* https://bit.ly/2WOud8Z
30. *Что такое целевая атака: признаки, объекты и последствия.* https://bit.ly/3aIp8aw

BIG DATA ANALYTICS IN SUPPORT OF INFORMATION SECURITY

Popov Veselin
PhD, Associate Professor
"D.A.Tsenov" Academy of Economics, Svishtov
e-mail: v.popov@uni-svishtov.bg

Emilova Petya
PhD, Associate Professor
"D.A.Tsenov" Academy of Economics, Svishtov
e-mail: p.emilova@uni-svishtov.bg

Abstract
Along with the many opportunities that Big Data provides to users (business users and individuals), it brings many threats to society, businesses and individuals. At the same time, Big Data Anapytics has established itself as an effective tool in many areas of modern information processing, including the area of information security. Big Data technologies used in security systems are able to detect threats in advance.
By providing tools for collecting and analysing large amounts of digital information generated from different sources or recorded by different devices, BDA helps to detect and define patterns and trends of malicious behaviour, search for methods to track cybercriminals, predict and stop potential cyber-attacks.
This report focuses on the problems and challenges of protecting Big Data in these two aspects.

Keywords: *Big Data, Big Data Analytics, Information Security*

JEL Classification: *D80*

INTRODUCTION

The globalization of business and the increasing use of cloud and mobile services have brought with them significant challenges in information security and the need for new tools (other than traditional ones) to protect and detect malicious activities in corporate networks.

Big Data Analytics (BDA) has established itself as an effective tool in many areas of modern information processing, including information security. By providing more data and applying various analytical techniques, with BDA all real and potential risks can be analyzed very quickly, more alternatives for protection and counteraction can be assessed, more accurate forecasts for the future development can be made, more expert opinions can be collected. With this tool, IS security professionals can quickly and cost-effectively perform complex simulations and test multiple possible security scenarios.

This report explores the opportunities and challenges of Big Data and Big Data Analytics in terms of information security.

BIG DATA – SOURCES, FEATURES, PROTECTION, PLATFORMS

In the literature, the term "Big Data" refers to huge aggregates of information that are stored, transmitted and processed in computer systems. Today, the main sources for generating Big Data are social media, a huge variety of smart devices, video, digital images, sensors and records of commercial transactions (Techopedia). Apart from being huge, these sets of information are also complex, which is why traditional processing applications cannot handle them.

According to the National Institute of Standards and Technology (NIST, 2018), Big data are those data in which the volume, required speed of data processing or presentation

limits the possibilities for effective analysis with traditional relational approaches or requires significant horizontal scaling to ensure efficient processing. This created the need for a new generation of software applications and tools.

Big Data differs from traditional databases in four main characteristics related to: the volume of the data set; the speed of data generation and transmission; the diversity of data in the form of different types of structured and unstructured data; the complexity of the structure, behaviour and permutations of datasets when different critical factors are at work.

One of the most serious challenges for Big Data platforms is the protection that must be implemented at every stage of the platform's life cycle and uses a combination of *traditional* security tools, *new* tools and technologies, as well as *intelligent security monitoring processes*.

The Big Data lifecycle includes four stages: data organization, processing, data warehouse maintenance, processing, and production.

Data organization includes the creation and/or access to data. Big Data is a collection of various types of data that come from different sources. According to sources, Big Data is of three types: data generated by humans – text, photos, video; data generated by machines - computers operating documents, databases, multimedia, GPS, RFID, the so-called smart "homes"; and data generated by various digital devices (objects).

For example, user-generated data includes CRM data, data such as emails, telephones, SMS or social media posts, and more. There is a lot of transaction data and data stored in different databases. There is also a huge amount of data generated by custom software and sensors. All data transited from sources to the platform must be protected.

Storage in a data warehouse. Security tools such as encryption, user authentication, intrusion protection are used for protection. These security tools must operate in a distributed platform with many servers and branch nodes. Security tools must protect log files and analytics tools when they operate on the platform.

Many organizations use cloud services to secure a data storage solution. Cloud technologies also allow companies to use pre-built Big Data solutions, or quickly create or deploy powerful server complexes without significant hardware acquisition costs. In addition to advantages, new technologies pose challenges to protection.

Analytical processing (analysis and results) of different types of data is the essence of Big Data. The results obtained from this processing are directed to applications, reports, and dashboards are the target of attacks. Therefore, encryption of results, access control and traffic are extremely important.

The classic technologies used for protection in Big Data are: encryption, user access control, intrusion detection and counteraction, physical protection. Encryption protects data both when it is stored in repositories and when it is transited. It should be noted that encryption must work with different types of data and with different analytical tools, relational and non-relational databases, special file systems, etc. User access control is a key tool for protection at the network level. It is important for the Big Data platform; it must be very precise and based on well-defined policies. Intrusion detection and response systems are also important for the Big Data platform as they contribute to the timely detection of intrusion attempts. Physical protection is related to the protection of the building and rooms of the data centre of the organization or the cloud provider.

Hundreds of software tools and complex platforms are available on the Big Data processing *software market*. Some of them have a long history, while others have appeared recently. Large enterprise software solution manufacturers, such as Oracle, IBM, SAS,

SAP, Teradata, Microsoft and others, dominate this market. Their Big data products are characterized by being integrated with complex business management solutions.

Successful products are also offered by smaller software companies specializing in Big data such as Tableaau, RapidMiner, Pentaho, Alteryx, Alpine and others.

Open source products such as Apache Hadoop, MapReduce, GridGain, Storm and others are also available on the market. Some open source software solutions are often included in commercial vendor projects.

The best software tools for processing Big data, according to their purpose, functions performed and implemented level of protection are (import.io, 2018):

- for data storage and management – Haddop, Cloudera, MongoDB, Talend;
- for data cleaning – OpenRefine, DataCleaner;
- to extract knowledge from data – RapidMiner, IBM SPSS Modeler, Oracle data mining, Teradata, FramedData, Kaggle;
- for data analysis – Qubole, BigML, Statwing;
- for data visualization – Tableau, Silk, CartoDB, Plot.ly, Datawrapper;
- for data integration – Blockspring, Pentaho;
- data languages – R, Python, RegEx, XPath;
- for data collection – Import.io.

BIG DATA ANALYTICS FOR INFORMATION SECURITY

From a structural point of view, the information protection process includes three phases: *prevention – detection – response*. The BDA has a huge potential for the strategies and activities of the second phase – the phase of detecting crimes and potential threats.

The analysis of Big data is significantly more complex than that used in traditional databases. Big data have large volumes, non-aggregated, in different formats and their processing is difficult to do in the memory of only one computer. Big data processing includes mechanical processes and algorithms. The methods used for Big data analysis are of two main types - *responsive and predictive analysis* (Huang & W. Chaovalitwongse, 2015).

The response analysis aims to produce statistics on current and historical data and to provide information on what happened and why it happened. It includes methods such as statistical modelling, trend reporting, visualization, association and correlation analysis.

Predictive analysis focuses on the use of known data (training data), which include input data properties (attributes) and response values (target models) to build a predictable model (solution) to make predictions for invisible data (test data). It uses methods such as vector machines, linear regression / classification, nonlinear regression (generalized linear model), decision tree, Bayes theory, neural networks and others.

Big Data technologies used in security systems are able to detect threats in advance. For example, they can detect atypical behaviour on the network, predict an attack, and analyse the sources of an attack.

Big Data creates conditions for efficient and effective application of some fraud detection techniques. In the specialized literature, they are divided into two main groups: statistical techniques and techniques using *artificial intelligence*. Table 1 presents examples of these techniques.

Table 1. Examples of Big Data Analytics techniques

Statistical techniques
1. Techniques used in data pre-processing to detect, validate, correct errors, fill in missing and inaccurate data.
2. Calculation of various statistical parameters such as averages, valves, efficiency indicators, probability distribution, etc.
3. Models and probability distribution of different business activities.
4. Processing of user profiles.
5. Analysis of time-dependent data series.
6. Clustering and classification to detect possible models / schemes and dependencies / associations in data groups.
7. Combining algorithms to detect anomalies in the behavior of transactions or users
Techniques using artificial intelligence
1. Data mining
2. Expert systems.
3. Automatic pattern recognition
4. Machine learning techniques
5. Neural networks

Source: (BajpaiI & Arushi, 2018)

CHALLENGES

Big Data Working Group, defines four aspects of Big data protection, which are: infrastructure security; data confidentiality; data management, integrity and reactive security (Cloud Security Alliance, 2013). Each of the areas is associated with many problems. For example, infrastructure security has the following issues:

- Availability of single-layer protection - companies must include multi-layered defence within the company's defence strategy, which addresses both internal and external security threats..
- Data transfer across multiple devices, which requires additional levels of security and monitoring to ensure that data is not captured along the route from one device to another.
- Rapid development of big data technology and its supporting infrastructure (such as cloud services), which must be able to process data from an infinite number of points with speed, security and reliability.

The infrastructure must include security measures to keep information at every stage of the process.

In fact, in addition to enhancing business intelligence, Big Data provides an opportunity to enhance information security. This increases the existing problems and challenges that require attention and await solutions.

The main problems with Big Data security are related to: threats to data security; privacy risks; the need to confirm the authenticity; there is no technology to protect the confidentiality of big data.

These Big Data security issues require addressing many challenges, the most important of which are:

a) Acceptance of protection as a top priority for Big Data platforms, which will focus the attention of managers and developers in this direction.

b) Introduction of reactive and proactive protection.

c) The physical protection of devices and servers that contain sensitive information must be managed with special care and isolated from other devices.

d) Application protection is as important as device protection. In this regard, the protection of Data mining solutions is of particular importance. These solutions are the basis of Big Data platforms, contribute to the discovery of patterns of behaviour and development trends and on this basis offer business strategies. This importance of Data mining solutions requires that they be protected not only from external threats, but also from internal individuals who abuse their privilege to access sensitive information

e) High level of access control to be provided by encrypted authentication and to determine which individual can see what data.

f) Use of real-time protection tools. These tools generate a huge amount of information. The problem here is to ignore unimportant signals so that employees can focus on the real violations.

g) Data warehousing management. For the Big Data architecture, it is typical for data to be stored at multiple levels, depending on its importance to the business and the cost of storing it.

h) Carrying out a detailed audit, which can help determine when missed attacks can occur, what were the consequences, what to change in the current system.

i) Use of distributed systems. For faster analysis, most Big Data platforms actually distribute the huge amount of data processing work across many systems.

CONCLUSIONS

Along with the many opportunities that Big Data provides to consumers (business users and individuals), it brings with it many threats to society, business and individuals. At the same time, the BDA has established itself as an effective tool in many areas of modern information processing, including information security. This report addresses the challenges and challenges of Big Data protection in these two aspects.

BIBLIOGRAPHY

1. Bajpai, A., & Arushi, A. (2018). Big Data Analytics in Cyber Security. *International Journal of Computer Sciences and Engineering, 6*(7).
2. Cloud Security Alliance. (2013). *Expanded Top Ten Big Data Security and Privacy Challenges.* Retrieved from Expanded top Ten Big Date Security and Privacy Challenges: https://downloads.cloudsecurityalliance.org/initiatives/bdwg/Expanded_Top_Ten_Big_Data_Security_and_Privacy_Challenges.pdf
3. Huang, S., & W. Chaovalitwongse, W. (2015). *Computational Optimization and Statistical Methods for Big Data Analytics: Applications in Neuroimaging.* INFORMS TutORials. Retrieved from Computational Optimization and Statistical Methods for Big Data Analytics: Applications in Neuroimaging: http://faculty.washington.edu/artchao/INFORMS_Tutorials_2015-Web.pdf
4. import.io. (2018). *All the best big data tools and how to use them.* Retrieved from import.io: https://www.import.io/post/all-the-best-big-data-tools-and-how-to-use-them/
5. NIST. (2018). *Big Data Information.* Retrieved from NIST: https://www.nist.gov/el/cyber-physical-systems/big-data-pwg
6. Techopedia. (n.d.). *Big Data Analytics.* Retrieved from Techopedia: https://www.techopedia.com/definition/28659/big-data-analytics

MODELS AND METHODS FOR GOVERNAMENTAL CYBER RISK MANGEMENT

MODELE ȘI METODE DE GESTIONARE A RISCURILOR CIBERALE GUVERNAMENTALE

Valeriu Cernei
Doctorand, Academia de Studii Economice a Moldovei
e-mail: valeriu.cernei@bsd.md

Abstract
The subject of cyber security risk management of state organizations is one that cannot lose its relevance given the fact of the continuous development of information technologies. The Republic of Moldova has demonstrated significant progress in the field of ICT, especially in the development of services for citizens, as well as to business and government to government, through the implementation of the interoperability platform. Thus, Cyber Security risk management processes and activities are to be carefully planned, implemented and monitored. The paper presents a generalized view of the approach and proposes certain tools and methods aiming to facilitate the implementation of a Government wize risk management process.

Keywords: *Risk Management, Cyber Security, Governement, ICT, KRI, approach*

JEL Classification: *C63, D81*

INTRODUCERE

Subiectul gestiunii riscurilor de securitate cibernetică este unul ce nu-și poate pierde actualitatea dat fiind faptul dezvoltării vertiginoase și continue a tehnologiilor informaționale. Apar noi vulnerabilități sau își modifică forma vulnerabilitățile vechi, și, prin urmare, se analizează noi riscuri inerente.

Domeniul gestiunii riscurilor TIC și a celor de Securitate cibernetică prezintă procese și activități ce trebuie cu o mare atenție planificate, realizate și monitorizate.

Conducătorii de toate nivele conștientizează faptul că procesul de gestiune a riscurilor, inclusiv a celor de Securitate cibernetică, reprezintă o sursă consistentă de informare cu scopul elaborării deciziilor corecte. Totodată, ei înțeleg, că procesul trebuie organizat și derulat cu o maximă responsabilitate și transparență, altfel, deciziile elaborate pot afecta negativ întreaga organizație.

Subiectul este de o și mai mare importanță odată cu orientarea serviciilor statale către cetățeni. Implementarea sistemelor informaționale ce au obiectivul de a ușura interacțiunea dintre stat si cetățeni, stat și persoane juridice, dintre instituțiile statului duce la faptul expunerii participanților unor riscuri inerente informaționale (TIC) și de Securitate cibernetică semnificative.

REZULTATELE CERCETĂRII

Republica Moldova, în ultimii 10 ani, a progresat semnificativ în digitizarea și automatizarea serviciilor pentru cetățeni și a activităților interne de colaborare inter-instituțională, inter-departamentală, s.a.m.d. Totodată, funcțiile de asigurare a securității cibernetică și analiza riscurilor, precum și cele de creștere a nivelului de conștientizare în domeniul securității cibernetice, nu au fost cumva tratate/dezvoltate și instituționalizate comensurabil, sau, dacă acest lucru s-a întâmplat, atunci activitățile respective au purtat un caracter sporadic, fără o coordonare consistentă și planificată la nivel statal.

Nivelul de maturitate a domeniului de Securitate al sectorului guvernamental a fost și este în continuare diferit: unele instituții alocă resurse și implementează mecanisme consistente de Securitate, altele, abordează subiectul superficial și cazual. Dacă ar fi să realizăm o grupare, atunci organizațiile guvernamentale ce posedă un nivel de maturitate sporit ar reprezenta mai puțin de 10 % din numărul total, inclusiv al instituțiile în care statul are calitate de fondator sau acționar.

Platforma interguvernamentală de comunicare (implementată de către Agenția pentru Guvernare Electronică) presupune că instituțiile de Statului sunt conectate și alimentează platforma cu date, astfel, fiind asigurate servicii dintr-o singură sursă pentru cetățeni. În acest caz, se poate admite obiectiv, că unele Instituții pot alimenta platforma cu date eronate/neveridice/etc, fapt ce implică riscuri de Securitate semnificative, inclusiv riscuri ce țin de protecția datelor cu caracter personal.

Autorul, pe parcursul ultimilor ani, a prestat servicii comerciale de audit al securității informaționale pentru mai multe Instituții de stat. O analiză generalizată a nivelului de maturitate a Instituțiilor statului din punct de vedere al securității cibernetice relevă mai multe concluzii, dintre care:

- Nivelul mediu de maturitate per instituții guvernamentale de nivel superior este evaluat ca fiind intre 1 si 2, pe o scara de la 0-5 (0-inexistent, 5 - optimizate).
- Funcția de ofițer de securitate cibernetică sau nu este instituită sau nu este completată (lipsa cadrelor în domeniu, necăutând la faptul instituirii specialităților corespunzătoare în cadrul instituțiilor de învățământ superior, licență și master).
- Doar câteva instituții au abordat subiectul securității informației într-un mod complex, prin adoptarea și implementarea unui sistem de management al securității cibernetice.

În anul 2017 a fost aprobată HG 201 Cerințe minime de securitate cibernetică. Este de menționat că HG respectivă include expres cerințe privind gestiunea riscurilor cibernetice. Necăutând la faptul că procesul de gestiune a riscurilor de securitate este unul central implementării și menținerii unui sistem de management al securității informației, nicio instituție de stat nu a abordat subiectul într-un mod comprehensiv, fiind stabilit și urmat un proces în sensul larg.

Este evident că, în condițiile digitizării și centralizării serviciilor publice, este crucială o abordare centralizată și foarte bine coordonată a aspectelor de securitate a informației și, corespunzător, cele de gestiunea riscurilor cibernetice.

Pe lângă metodologia propriu-zisă ce trebuie dezvoltată, este necesar de a asigura un suport considerabil de implementare etapizată. Implementarea etapizată presupune crearea / validarea mediilor protejate și includerea graduală a unor medii informaționale adiționale, ca rezultat al activității de analiza a riscurilor și, ce este mai important, de tratare corespunzătoare a acestora.

Elaborarea unei metodologii de analiza a riscurilor cibernetice cu scopul de a fi adaptată și propusă spre implementare in instituțiile Statului este foarte importantă. Metodologia trebuie să vizeze evaluarea riscurilor, identificarea măsurilor de minimizare, planificarea activităților de tratare a riscurilor, aplicarea indicatorilor de corecție calculați în funcție de situația reală pentru perioadă analizată, etc. În sine, procesul de gestiune a riscurilor este interconectat și se alimentează cu informații și date rezultate din alte procese, cum ar fi gestiunea incidentelor, gestiunea schimbărilor, gestiunea continuității, s.a.m.d. Pentru a asigura un proces eficient de gestiunea riscurilor va fi necesar de a asigura și derularea eficientă a respectivelor procese.

Pornind de la axioma că ”tot ce nu poate fi măsurat, nu poate fi îmbunătățit”, nu mai puțin important este necesitatea dezvoltării unui sistem de parametrizare și raportare,

cu gruparea pe diferite resurse informaționale, după componentă, după sursă, nivelul riscului și altele.

Metodologia poate fi elaborată în baza instrumentelor MS Office: Excel și Word la prima etapă. Pentru a asigura maximum funcționalități utile și fezabile, instrumentele respective pot fi create și ținând cont de rezultatele analizelor instrumentelor de Risc Management existente pe piață, care prezintă mai multe neajunsuri cum ar fi rigiditatea de configurare adaptare, efort sporit de localizare, complexitatea, lipsa specialiștilor si, nu în ultimul rând, prețul sporit de achiziție și licențiere.

Din punct de vedere al abordării activităților, acestea trebuie structurate în mai multe etape, atât practice cât și de cercetare, rezultatul reprezentând instrumente fezabile și concluzii relevante - rezultat al activităților analitice. Astfel, se conturează câteva etape de realizare ce sunt prezentate în continuare:

- **Evaluarea situației privind gestiunea riscurilor la nivel statal**. Activitatea presupune organizarea unei serii de ședințe și întâlniri cu persoane cheie din cadrul organizațiilor statale. Pentru a asigura rezultate cât mai relevante, este necesar de a selecta organizații de nivel 1 (Ministere și Agenții de stat), nivel 2 (Agenții și Companii fondate sau administrate de către structuri guvernamentale de nivel 1) si chiar 3 (Agenții și organizații subordonate celor de nivel 2). Pentru a asigura că selecția și, corespunzător, rezultatele sunt relevante, va fi necesar de a elabora criteriile de selecție a instituțiilor. Un criteriu evident la momentul scrierii curentului referat poate fi nivelul organizației conform HG201 privind cerințele minime de securitate cibernetică, precum și cantitatea de date furnizate către platforma guvernamentală.
- **Analiza bazei legale privind gestiunea riscurilor TIC și de securitate cibernetică a Republicii Moldova.** Respectiva activitate presupune analiza detaliată a cadrului legal în domeniu. Ca rezultat vor fi înaintate recomandări de îmbunătățire a bazei normative și legale statale
- **Evaluarea situației privind gestiunea riscurilor de securitate cibernetică în instituțiile comerciale**. Autorul își propune să realizeze o analiza a mediului comercial din punct de vedere al proceselor aferente gestiunii riscurilor de securitate.
- **Analiza comparativă stat versus comercial în R. Moldova.** Analiza comparativă in raport cu un sistem de referință precum și cu mediul comercial, poate oferi o înțelegere mai bună a situației curente precum și facilita selectarea strategiei de implementare a proceselor aferente securității informației, specific gestiunii riscurilor de securitate.
- **Analiza principalelor instrumente de gestiune a riscurilor existente la nivel local și internațional**. Pe piață există o multitudine de soluții ce, parțial sau integral, automatizează activitățile aferente gestiunii riscurilor. Acestea reprezintă instrumente valoroase si complexe. Totodată, în R. Moldova nu au fost identificate cazuri de implementare a astfel de sisteme. În scopul lucrării, analiza respectivelor sisteme va avea o valoare semnificativă din punct de vedere al organizării proceselor și a funcționalităților specifice. Totodată va fi realizată analiza comparativă a diferitor metodologii de analiza a riscurilor calitative și relevarea aspectelor de localizare
- **Elaborarea metodologiei de gestiunea riscurilor la nivel de Instituții de Stat.** Este considerat că, aderarea la o metodă cantitativă a riscurilor, va fi mult prea greoaie de implementat și menținut, în special în situația lipsei de experți în domeniu. Cunoștințele și experiența acumulată de-a lungul anilor vor fi sistematizate, dezvoltate și îmbogățite cu rezultatele cercetării aspectelor specifice cu scopul elaborării unei metodologii viabile, ușor de implementat și menținut.
- **Elaborarea conceptului de implementare graduală a metodologiei la nivel statal**. Metodologia elaborată urmează să stea la baza conceptului de implementare graduală.

După cum a fost specificat anterior, se recomandă a asigura o abordare etapizată de implementare, fapt ce presupune crearea a cel puțin 3 zone de implementare: zona securizată, zona tampon, zona cu risc înalt. Instituțiile de stat vor fi grupate conform unor criterii elaborate și pre-aprobate. Ulterior, fiecare instituție va trebui să satisfacă anumite cerințe pentru a fi atribuite zonei cu nivel de securizare mai înalt. Totodată, va fi necesar de a stabili principiile de monitorizare a modului de menținere a nivelului curent.

- **Elaborarea instrumentarului de înregistrare, calcul și evidența a riscurilor informaționale/cibernetice.** În cadrul activității respective autorul își propune a sistematiza cunoștințele acumulate în rezultatul cercetării și a elabora instrumentele de automatizare a procesului. În scopul lucrării procesul urmează a fi automatizat cu ajutorul instrumentelor MS Excel și MS Word. Ulterior, odată ce metodologia va fi implementată și ajustată conform situației reale, aceasta urmează a fi automatizată in baza tehnologiilor moderne.
- **Propunerea unui program de studiu prind gestiunea riscurilor cibernetice utilizând tehnici neformale de educare în domeniu**. Autorul își propune a elabora un curs de studiu, ce urmează a fi propus instituțiilor de învățământ. Acest lucru este important pentru a asigura experți pregătiți de a menține procesele de gestiune a riscurilor în instituțiile de stat.

Rezultatele cercetării pot avea un impact semnificativ în procesul de consolidare cibernetică a statului. Efectul va fi unul benefic pentru fiecare dintre instituțiile statale, comerciale, precum și instituțiile de învățământ.

CONCLUZII

Procesul de gestiune a riscurilor reprezintă unul dintre instrumentele cheie în elaborarea deciziilor. În condițiile curente și cele viitoare, când tehnologiile se dezvoltă cu o progresie geometrică, este crucial de a asigura, pentru analiza, informație relevantă și actuală. Un proces de gestiune a riscurilor consistent ne permite, nu doar să anticipam potențialele evenimente nedorite, dar și să învățăm din experiența anterioară, analizând și contrapunând diferiți indicatori de risc.

BIBLIOGRAFIE

1. ISO 31000, *Risk management – Guidelines*
2. HOTĂRÎRE Nr. 201 din 28.03.2017 privind *Cerințe minime obligatorii de securitate cibernetică*
3. Levi Gundert, The Risk Business (2020) - *What CISOs Need to Know About Risk-Based Cybersecurity*
4. Лившиц Илья Иосифович (2018) *Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами*
5. Ванюрихин Ф.Г. (2019), *Модели и методы динамического управления рисками предприятий.*

THE PASSWORDLESS MANAGER

Țurcan Nicolae
Master in Economics
Computer Security University of Oklahoma, Norman, USA
e-mail: nicolae@ou.edu

Schneider Tobias
Master in Economics
Computer Security University of Oklahoma, Norman, USA
e-mail: tobias.schneider-1@ou.edu

Abstract
Password managers are common software solutions to store secure and valuable information like banking credentials, passwords or personal information. Our goal is to design a password manager using a new approach to manage private data. We analyze problems of existing solutions, propose our own design and technique, and finally implement a solution. Our application does not store passwords in any form on the memory but instead generates them on the fly by processing the user input and other variables combined with a key derivation function. Finally, we elaborate limitations of our approach and suggest future work.

Keywords: *security, managers, password, system design, security analysis*

JEL Classification: *C63*

INTRODUCTION

A password manager is a computer program which stores and administrates secret data like passwords on a computer, smartphone or in web applications. These programs originate from the problem that users need secure passwords on their system and many websites. There is a high security risk of using the same usernames and passwords for different services, as a single stolen password would allow access to all services. Therefore, many different passwords are needed. To protect these accounts from unauthorized access, many and long passwords are needed. A possible solution to tackle this problem is using a password manager to store the valuable information in an encrypted format.

Some password manager utilize a master key to encrypt the private data. The security of a master password approach depends on the strength of the mostly user chosen passphrase. If an attacker is able to obtain the master key all saved passwords are rendered vulnerable. The password database, also called vault is stored on the file system and has to be encrypted. Also, the used encryption algorithm must be implemented flawlessly to avoid security problems which are risk to exploitation by hackers.

In 2014, more than five million Gmail logins were leaked. A password manager company named LastPass conducted an analysis of that data and came up with the following findings [8]:

- Top 10 most-used passwords were 123456, password, 123456789, 12345, qwerty, 12345678, 111111, abc123, 123123, 1234567.
- Top 10 most-used words in passwords were password, qwerty, love, monkey, dragon, hello, iloveyou, abcd, welcome, July.

	LastPass	Dashlane	1Password	KeePass
Customizable encryption algorithm	✗	✗	✗	✓
Customizable KDF	✗	✗	✗	✓
Multi-platform	✓	✓	✓	✓
Open source	✗	✗	✗	✓
Multi-factor authentication	✓	✓	✓	✓*
Password metrics	✓	✓	✓	✓
Breach alert	✓	✓	✓	✗
No data leaks	✗[1]	✓	✓	✓
External third-party storage	✗	✗	✗	✓
Password sharing	✓	✓	✓	✗*
Password generator	✓	✓	✓	✓
Password changer	✓	✓	✗	✗
Privacy respecting	✓	✗	✓	✓
Beginner friendly	✓	✓	✓	✗
Subscription restricted features	✗	✗	✗	✓

Figure 1. Overview of popular password managers

– 92.96% of the passwords were 1-10 characters in length The above statistics suggest that average users are not aware of how insecure their password choices or do not realize how many other people tend to use the same combination. This piece of knowledge makes the job of hacking a particular password much easier for those who are interested of stealing such personal information. Therefore, a secure master key is essential for the security of the saved passwords.

Instead of storing the encrypted passwords on the file system we propose a new approach which avoids the use of a vault. We generate passwords on the fly by calculating a function which takes a combination of user name, website, master key and a counter as input. Chapter II presents related work to our research. Chapter III explains our system, used algorithms and password generation in detail. In chapter IV we propose our application by explaining the user interface and implementation details. Also, chapter V contains a security analysis of our approach and possible attacks. Chapter VI summarizes the results of our research.

RELATED WORK

We decided to explore the most popular password managers in order to come up with a hypothesis as to why people do not tend to use password managers more often. The paper presenting SAFEPASS, which is a password manager, has summed up the main features of four of the most popular password managers. [1]

As it can be seen in the table above, only KeePass provides customizability regarding the encryption algorithm used for storing a password. This feature might be of interest for people with encryption knowledge and who desire to take control over how their passwords can be encrypted, perhaps mixing the algorithms for different instances. On the other hand, KeePass is the manager that is the least beginner friendly when compared to LastPass, Dashlane, and 1Password.

	Bookmarklet	Extension	Website	Credential Encryption: Master Key Derivation	Credential Encryption: Encrypted Fields	Collaboration
LastPass	✓	✓	✓	KDF(mp,mu,5000,32)	usernames and passwords	✓
RoboForm	✓	✓	✓	×		×
My1login	✓	×	✓	MD5(ph_{even})+MD5(ph_{odd})	usernames and passwords	✓
PasswordBox	×	✓	×	KDF(mp,mu,10000,32)	passwords only	✓
NeedMyPassword	×	×	✓	×		×

mu: master username mp: master password
ph: passphrase $ph_{even(odd)}$: characters at even (odd) positions of ph
KDF(p,s,c,l) is a key derivation function [23], which derives key of length l octets for the password p, the salt s, and the iteration count c.

Figure 2. Encryption schemes of popular password managers

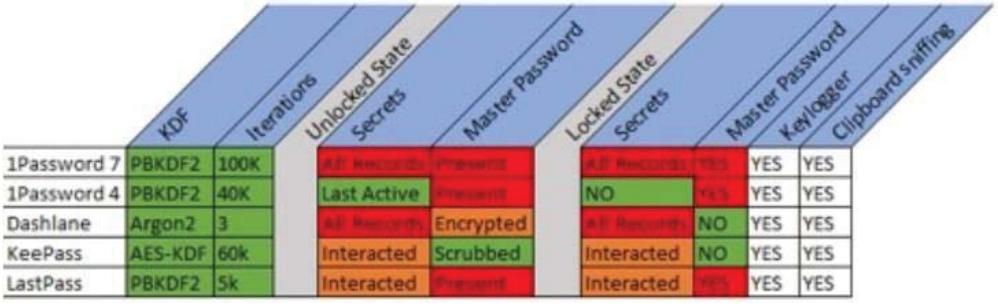


Figure 3. Summary of password managers security items

A study from 2014 analyzed five popular password man- agers: LastPass, RoboForm, MyLogin, PasswordBox, and NeedMyPassword. It concluded that all five managers had critical vulnerabilities, and with four of them arbitrary user credentials could be stolen [2].

The study also provided guidance and mitigations to avoid the vulnerabilities. The goal of our password manager is to follow this guidance in order to avoid critical vulnerabilities.

Additionally, that study presented the following table that provides a summary of certain features for those five password managers.

The above table shows that not all password managers combine the bookmarklet, extension, and website format for user interaction. We choose to keep our password manager as simple as possible to avoid misuse and prevent security issues. In 2019, Independent Security Evaluators (ISE) have con- ducted an analysis four major password managers: 1Password, Dashlane, KeePass, and LastPass. The main focus of the anal- ysis was to explore the sanitization of sensitive information stored by the password managers [3]. The following figure summarizes their findings.

The red in the figure above displays security violations of proposed security guidelines by ISE. The conclusion of the study was that each password manager analyzed failed to implement proper sensitive information sanitization for various reasons. The most urgent concern outlined was when a password manager was put into a locked state and sensitive information was not sanitized.

More work related to password managers has been done in the past. For instance, a solution that created a password manager for the Firefox browser using cloud-based storage was outlined in 2014 [4]. Since this solution does not target Chrome as its primary browser, the fact that our password manager will primarily be developed for Chrome will

setus apart. Two more cloud-based password solutions were outlined in the papers that presented Passpet [5], and Password Multiplier [6].

Passpet and Password Multiplier represent for the most part solutions that solely help in generating passwords, hence our password management capabilities will offer a different approach to solve the password problems.

A password manager named Master Password is the most similar application compared to ours [11]. The main idea is the provision of passwords only when the user needs to. If a user selects a website the tool generates the password. This application still stores a version of the hashed master key on the file system to allow the user to login. Even if the passwords are erased after the generation the hash of the master key is still saved on the memory.

Based on the above observation, we decided to come up with a solution that will offer a combination of features that is not currently present on the market. In particular, our password manager will be secure, beginner friendly, appealing to people who require more customizability, secure according to ISE guidelines.

SYSTEM DESIGN

This chapter explains the main idea of our approach. The system design is fundamental for the security of the applica- tion. Criterias for the chosen encryption, password generation and functionality are explained in detail.

A. *System Overview*

As our aim is to not store any passwords in neither en- crypted nor unencrypted form on the memory so we propose a new take on a password manager. If the we do not utilize a password database we have to generate the passwords by processing information the user inputs and data which does not have to be necessarily private. This way we can store the name of the website on the computer but every other information is secret and supplied by the user to generate the password for the requested web page.

Figure 4 shows the concept of our system. The name of the user, the website and the counter are combined into a message string. This message is part of the input for the password generation function. The user input is displayed on the left and consists of three inputs variables:

- **Master key:** The passphrase which is used to gain access to the application. Usually, the hash of the master key is stored and compared with the hashed input of the user. As we do not store the key on the file system the passphrase has to be correct or a wrong password will be generated.
- **User name:** The name of the user does not have to be secret but the number of possible inputs increases if the user name remains unknown.
- **Website:** The name or URL of a web page. The list of websites is saved in the application and is not secret.

Additionally, we use a counter which increments every time a new password is generated. Otherwise would the input for the generation of a new password for the same website result in the same passphrase.

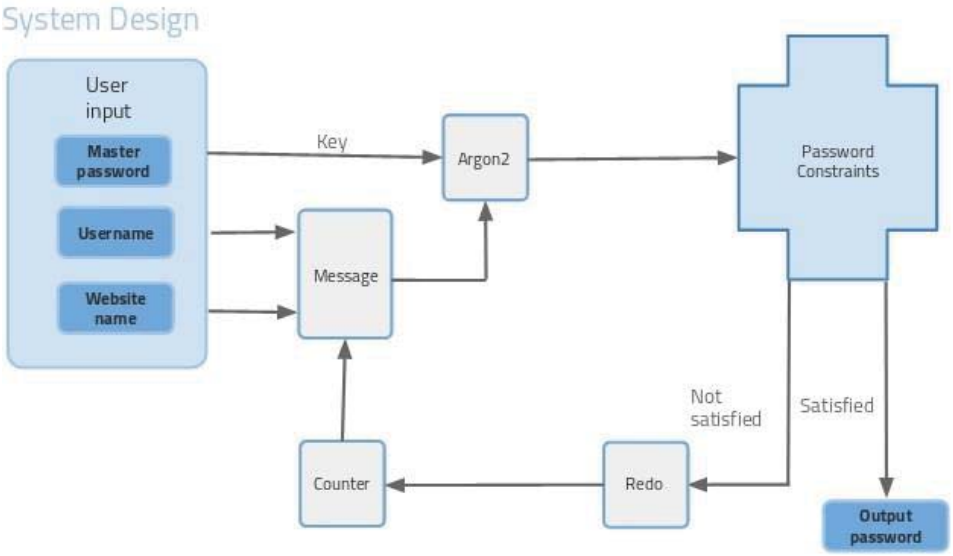


Figure 4. System Design

The function for the password generation must meet several requirements to be suitable for our use case. We use a hash function H for this purpose. The most important requirement is the one-way property. If an attacker is able to obtain the password $H(m)$ it must be computationally infeasible to find the original message m.

We use a key derivation function (KDF) for the password generation. Such a function repeats the hash process many times to make password cracking more difficult. The KDF derives a key from a secret value which would be the com- bination of master password and message in our case. The advantage of such a function compared to a simple hash function is the slow down of the computation to aggravate brute-force and dictionary attacks. The number of iterations indicates how often the hash function is calculated. The result of the previous function is the input for the next calculation. The number of iterations should be high enough to slow down the calculation process to a reasonable time. The usual input for a key derivation function is the string to hash, a salt and the number of iterations for the sub-function. The use of a salt prevents an attacker from precomputing rainbow tables of a dictionary or random words.

To choose a key derivation function fitting our purposes we examine different available solutions. The PBKDF2 [https://www.ietf.org/rfc/rfc2898.txt] (Pass- word Based Key Derivation Function 2) is used for deriving a key from a password. It possible to specify the hash algorithm, length of the key and the number of iterations. A disadvantage is that it can be implemented in hardware with a small curcuit and little RAM very cheap. The HKDF (HMAC- based Extract-and-Expand Key Derivation Function) is used to derive keys of a fixed length for further crpytographic usage [https://tools.ietf.org/html/rfc5869].

Another KDF is argon2 [https://tools.ietf.org/html/draft-irtf-cfrg-argon2-03] which was selected as winner of the Password Hashing Competition in 2013. The algorithm creates a big vector in the memory to avoid the cracking by specialized hardware which usually has a small memory. We select argon2 as key derivation function due to its security features compared to the other algorithms.

We define some constraints for the generated password to meet the requirements requested by most modern websites:

- Minimum length is 8 characters
- Contain at least one uppercase letter
- Contain at least one number

– Contain at least one special character

Finally, if the derived password complies with the required quality it is shown to the user in the interface. This password is used for the website which was selected by the user before.

B. *Secure Master Key*

In 2006, a study of 49 undergraduates has shown that the majority had three or fewer user passwords and passwords were reused twice [7]. Over time, password reuse has only increased because students created more accounts but did not come up with more passwords. This study is particularly inter- esting because students are the ones to adopt new technology the quickest, but even they did not adopt the use of password managers at a broad scale.

RoboForm has performed a survey which polled 1,000 random people in the US and UK about password security practices [9]. The following are some of the results they came up with:

- ✓ Only 27% never have their browser remember their passwords
- ✓ 42% write their passwords down, 10% save them in a document, 23% always use the same password, 25% use personal information, 5% enter as numbers on mobile device, 37% use phrases consisting of numbers and letters, 8% use a password manager.
- ✓ 12% use more than 11 passwords, 29% use between 6 and 10 passwords, and 59% use up to 5 passwords.
- ✓ 63% have forgotten a password or had a password com- promised in their professional life.
- ✓ 53% have forgotten at least a password for work in the past month.

The fact that only 27% never have their browser remember passwords might sound odd to some, however, browsers do not provide secure spaces for storing such information. For instance, a paper from University of California that analyzed the security of password manager database formats concluded that the way Google Chrome stores its users' passwords does not provide neither secrecy nor integrity [10].

Only 8% use password managers, meaning that users are overall still reluctant to use such kind of tools for password storage. Password managers solve the problem that people need to remember different passwords for several accounts. The user has to remember one master key to access all data. In many cases, the master key consists of a 12 to 16 character long, hard to remember passphrase. Since the security of such a system depends on the strength of the master key it is of highest priority to choose a strong pssword.

A possible solution to tackle the difficulty of remembering such a master key is the use of the Diceware passphrase [http://world.std.com/~reinhold/diceware.html]. This approach makes use of a list containing 7776 words of different length. Our application allows the user to generate such a password for his master key. In detail, the roll of five dices results in one word. We make use of a passphrase of six Diceware words so basically we roll the dice 65 = 30 times. The resulting password is a combination of these words, for example *PelicanTrustingUnmovableGemAstronautRipcord*.

Another argument for the usability is the following scenario. If the user inputs a wrong master key or flips a character the system generates the password based upon the wrong input and the computed passphrase is useless. After the login attempt the user recognizes that his password is false and tries to find the error in his usual master key for example *Sr0 pR7m&3K!*. It is difficult to find the error in such strings compared to a Diceware phrase. The problem is that the user is not notified while entering the false

password remains in both cases.

The advantage of using a Diceware password is the con- catenation of simple words. Such a phrase compared to a random combination of letters, digits and special characters is easy to remember. To compare the security of both options we calculate the entropy of both approaches. The entropy is a measurement for the set of random information in a system. Define password $p1$ as a 12 character random sequence of letters, numbers and some special chars (86 characters in total) and $p2$ as a Diceware password of 6 words. Calculate the entropy H as follows:

$$H(p1) = log2(8612) = 77.1\ bit\ H(p2) = log2(77766) = 77.5\ bit$$

As the entropy of both passwords is almost the same we conclude that the strength of both passwords is equal. Therefore, we provide the possibility to random a master key using Dicewords.

APPLICATION

This section presents the application and its workflow. Figure 5 shows the window that a first time user will be prompted with. The left hand side displays the application's name and a short summary of what it does. It also contains three navigation buttons: Register, Login, and Incognito. The right hand side presents a basic login form. In case the user does not have an account yet, he can create it using the register option on the left hand side of the application. After a successful registration, user's name and master password are hashed and stored in a local file for future login checks. In case the user does not want any of these to be stored anywhere, he can choose the Incognito option on the left hand side.

Figure 6 presents the window that logged in users are presented with. By default, logged in users are presented with the classic mode of our application. The left hand side offers information about the classic mode. The right hand side displays some social media presets that when clicked generate the according name in the website name section (i.e. if the Facebook logo is clicked, Facebook will be filled in the website name section). Otherwise, the user can manually type in the website for which he wants to generate a password. The blue label at the button will be the region where the generated password will appear.

Figure 7 is an example of how a generated password use case works. By either pressing the Instagram logo or manually typing it in, the user is presented with a generated password inside the blue label. This password has been generated by using the existed hashed of the user's name and password and combined with the website name provided. In case the user inputs the same website name in this section again, the same password will be generated. This way, the user can recover the already generated password without having to store it anywhere.

Figure 8 displays the incognito mode of Passwordless. The left hand side provides an explanation of the mode. The right hand side, just like in the classic mode, contains the social media logo shortcuts to fulfill the website name section. Incognito mode additionally requires the user to input the name and the master password because it does not use any stored information to generate the password.

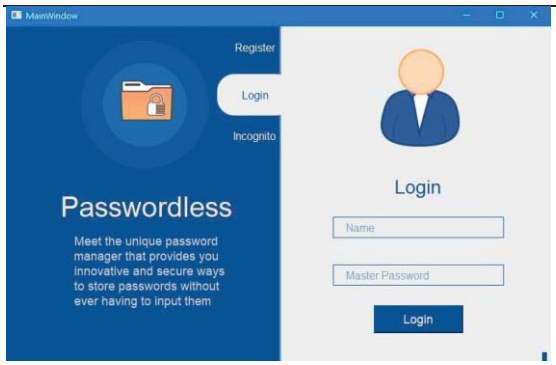


Figure 5. Default login page

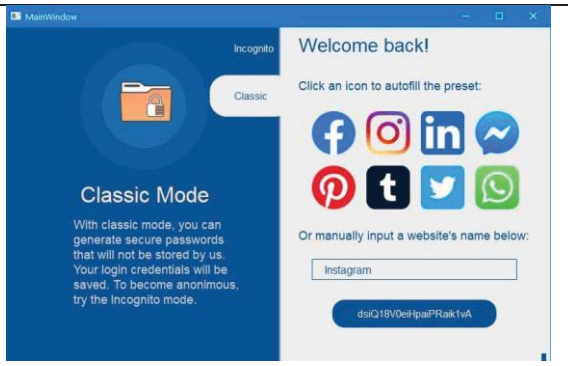


Figure 7. Classic Mode with generated password

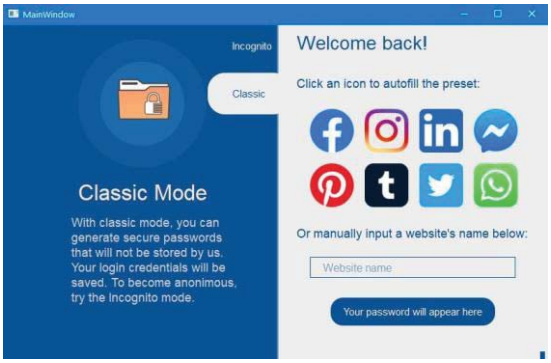


Figure 6. Classic mode

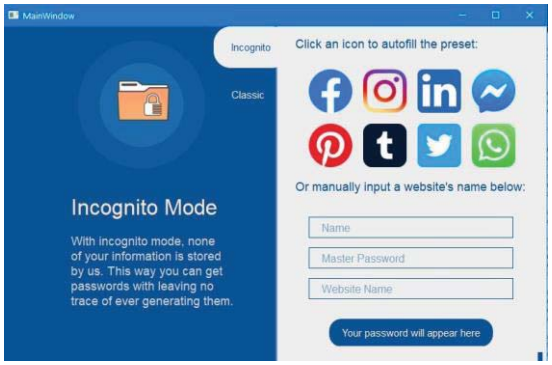


Figure 8. Incognito Mode

After typing in the name and the master password, while the user is inputting the website name the blue label will begin generating a password. As mentioned before, this mode calculates the passwords on the fly and does not use any stored data and does not store any of its results.

While developing the application, one of our goals was mak- ing sure that the application is easy to understand and usable. This is the reason why we decided to divide the interface into two pieces, the left piece explaining the current state of the application and the right piece focusing on user interaction. This way, the users do not have to search for specific button to understand what each application state entails. The usability was enhanced by using a simple minimalist design and limited interaction fields so that the user is not overwhelmed.

SECURITY ANALYSIS

The security of our system is a top priority target as flaws in the implementation result in risk of compromised user accounts. In this chapter we analyze the security of our application and propose challenges and limitations we currently deal with.

A. *Is our system design secure?*

It is necessary that the cryptographic operations in our system do not leak any information or are insecure in its execution. We assume that the input of the user is not intercepted by malicious software or other attacks. Since the hashing of the string combination of password, user name, website and counter is a safe operation the system itself is inherently secure. Security vulnerabilities in our application are more subject to errors in the implementation, memory leaks or attacks using video cameras.

The attacks on several password managers exploiting mem- ory leaks in 2019 revealed security issues affecting even pop- ular applications [3]. The authors were able to extract secrets from the memory during a locked state. Due to the compexity of this attack

we did not implement any countermeasures since the attack is very complex, uses tools we do not have access to and requires more research into memory leakage on Windows systems.

Another way to recieve the master key is without using exploiting security vulnerabilities in the actual application. Spying on a users keyboard is a simple yet effective way to get the master key. This attack only requires a camera with a high resolution to detect the keystrokes.

Our system provides no security measures against malware or malicious software. Since we do not store the master password in any form it is not possible for any application to read out the key. Malware specialized on stealing store data is uneffective in our case.

B. *Challenges and Limitations*

As for every common password manager the user has to remember the master key. If the user forgets the passphrase it is impossible to access the passwords. We do not provide any recovery options as the master key is not saved on the file system. By providing the opportunity to make use of a Diceword password we aim to minimize the risk of forgetting the master key.

If a new user utilizes our application it is necessary to change the passwords for all existing accounts. If a new website is added to our list the system calculates a password for it. There is no way to simplify that step because our system generates passwords based upon the name of the website amongst other things. The time required increases the more accounts the user applys new passwords to. After this initialization step the password manager is ready for further usage.

Another limitation which includes other common password managers as well is the risk of compromising the master key. If the user notices critical activities on registered accounts it is necessary to change the password on every site which is stored in the application. This step is time-consuming but not avoidable by any security measure.

A further problem is the use of the application in an unsafe environment. If the computer is infected by a keylogger the master key can be obtained. Other common password manager face the same problem. This problem has to be tackled by the user of the computer and is not part of our research.

CONCLUSION

Finally, we were able to implement our approach that does not store passwords in any format on the filesystem. We use a key derivation function to generate passwords and propose a user friendly interface to complete our password manager. With the use of Diceware keys we enable the user to obtain a secure and easy to remember passphrase. Besides some existing challenges like initial password creation for all accounts is the passwordless solution practicable. Future work should focus on a more detailed analysis of our approach regarding security and the design of attacks on the proposed application.

BIBLIOGRAPHY

1. Hakbilen, O., Perinparajan, P., Eikeland, M., and Ulltveit-Moe, N. (2018). SAFEPASS-Presenting a Convenient, Portable and Secure Pass- word Manager. In ICISSP (pp. 292-303).
2. Li, Z., He, W., Akhawe, D., and Song, D. (2014). The emperor's new password

manager: Security analysis of web-based password managers. In 23rd USENIX Security Symposium (USENIX Security 14) (pp. 465- 479).
3. Bednarek A. (2019). https://www.ise.io/casestudies/password-manager- hacking/
4. Zhao, R., and Yue, C. (2014). Toward a secure and usable cloud-based password manager for web browsers. Computers and Security, 46, 32- 47.
5. Yee, K. P., and Sitaker, K. (2006, July). Passpet: convenient password management and phishing protection. In Proceedings of the second symposium on Usable privacy and security (pp. 32-43). ACM.
6. Halderman, J. A., Waters, B., and Felten, E. W. (2005, May). A convenient method for securely managing passwords. In Proceedings of the 14th international conference on World Wide Web (pp. 471-479). ACM.
7. Gaw, S., and Felten, E. W. (2006, July). Password management strategies for online accounts. In Proceedings of the second symposium on Usable privacy and security (pp. 44-55). ACM.
8. Gott A. (2014, September). The Scary Truth About Your Passwords: An Analysis of the Gmail Leak. https://blog.lastpass.com/2014/09/the- scary-truth-about-your-passwords-an-analysis-of-the-gmail-leak.html
9. Couillard K. (2015, September). Password Security Survey Results. https://roboform-blog.siber.com/2015/03/06/password-security-survey- results-part-1
10. Gasti, P., and Rasmussen, K. B. (2012, September). On the security of password manager database formats. In European Symposium on Re- search in Computer Security (pp. 770-787). Springer, Berlin, Heidelberg.
11. Billemont M. (2019). https://masterpassword.app/

CONTROL AND PROTECTION OF INFORMATION IN THE COMPANY

КОНТРОЛЬ И ЗАЩИТА ИНФОРМАЦИИ В КОМПАНИИ

Шишманов Красимир
Доктор экономических наук, профессор
Экономическая Академия имени Д.А.Ценова (Свиштов, Болгария)
e-mail: k.shishmanov@uni-svishtov.bg

Abstract
The control and protection of the information is expressed in the possibility for an information system of the organization to ensure during the implementation of activities, its normal functioning, preventing events, expression of data in the products, modification or loss of data that represents some value for it. Read, due to the reason for these events, accidental actions or changes may be taken, which result in non-compliance with labor discipline, low qualification of the staff or the provided unauthorized access to the system.

Keywords: *information security, protection of information, control and protection of the information, protection of information system.*

JEL Classification: *D81, P47, C45*

ВВЕДЕНИЕ

Системы контроля и защиты информации от физического уничтожения или несанкционированного доступа к ней имеют первостепенное значение для информационной системы любой организации, независимо от области ее применения. Главной особенностью защищаемой информации являются ограничения, которые организация накладывает на ее распространение и использование.

Процессы, происходящие в современных организациях, можно отнести к очень сложным и высокотехнологичным. Они включают в себя различные действия по обработке и обмену информацией, отклонение которых от заранее заданного функционального алгоритма приведет к значительным потерям или невозможности дальнейшего функционирования. Параметры ответственных технологических процессов касаются контроля входящих потоков информации, хранения результатов и выработки управленческих решений. Для обеспечения их готовности и безопасности предъявляются особые требования к способу контроля и защиты информационных, административных, управленческих и коммуникационных ресурсов.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Современное функционирование корпоративных систем предполагает большое количество разнообразных средств, методов и форм сбора, обработки и передачи информации, что значительно увеличивает их уязвимость. Основными факторами в этом отношении являются:

- ✓ резкое увеличение объема информации, которая собирается, обрабатывается при исполнении служебных обязанностей;
- ✓ необходимость хранить и обрабатывать информацию разного назначения и разной принадлежности;

- ✓ увеличение количества используемых технических средств (в том числе мобильных) и усложнение взаимосвязей между ними в процессе работы;
- ✓ усложнение организации работы и технологии взаимодействия отдельных сотрудников;
- ✓ резкое расширение круга пользователей, имеющих прямой доступ к ресурсам корпоративной информационной системы;
- ✓ увеличение и усложнение обмена данными между отдельными пользователями, в том числе на больших расстояниях.

Защищенная информация используется корпорацией и различными другими системами. При этом у защищаемой информации есть свои особенности:

- Есть возможность ограничить доступ к ней. Доступ к корпоративной информации должны иметь только отдельные сотрудники или специально уполномоченные лица;
- Чем важнее информация, тем серьезнее ее защита. В зависимости от ее ценности и важности, определяются и различные степени доступа и секретности;
- Защищенная информация должна приносить пользу ее владельцу и оправдывать затраты на ее защиту.

Опасения по поводу правильного функционирования системы существуют в трех направлениях. Первое – возможность изменения или уничтожения (частично или полностью) данных (т.е. нарушение их физической целостности), второе – неправильное использование данных и нарушение последующих технологических процессов, третье – возможность несанкционированного предоставления информации, т.е. утечка информации.

Физическая потеря данных в информационных системах во многом зависит от технологии обслуживания. В этом отношении наиболее сильное негативное влияние оказывает низкая квалификация некоторых сотрудников и отсутствие достаточных знаний в области компьютерной обработки данных.

Основными потенциально возможными каналами утечки информации являются:

- ✓ запоминание или копирование информации в процессе функционирования информационной системы;
- ✓ несанкционированное подключение к информационной системе;
- ✓ несанкционированный доступ к информации с помощью специальных устройств;
- ✓ изменение алгоритма работы системы;
- ✓ загрузка и использование сторонних программ вне общей технологии системы;
- ✓ проникновение сторонних программ - «вирусов»;
- ✓ использование незаконных технических средств (перехват электромагнитных волн и др.).

Существует множество разнообразных форм и методов контроля и защиты информации. Однако они должны работать синхронно и охватывать все элементы информационной системы. В связи с этим следует стремиться сочетать надежное аппаратное (техническое) и программное обеспечение с соответствующими организационными мерами.

При рассмотрении и анализе процессов контроля и защиты информации, очень трудно (а в большинстве случаев, невозможно) отличить функции контроля от

защиты. Если необходимо контролировать только функции управления, можно представить несколько типов элементов управления.

1. В зависимости от времени обращения виды контроля полностью соответствуют его основным формам и могут рассматриваться как **предварительный, текущий, последующий**.

При функционировании информационной системы под предварительным контролем понимается **контроль входной информации**, под текущим - **контроль при обработке** и под последующим - **контроль результирующей информации**.

- **Контроль входной информации (предварительный) -** выполняется перед выполнением каждой операции. Его основная цель - устранить предпосылки, которые могут привести к ошибкам. Выполняется по первичным документам, из которых вводится информация в технических средствах и по операциям ввода. Цель состоит в том, чтобы предотвратить ввод неверной информации в компьютер.
- **Контроль при обработке (текущий) -** осуществляется при выполнении операций. Здесь основную роль играет контроль, который встроен в программные продукты и функционирует непрерывно, взаимодействуя с основной программой. Текущий контроль развивается и проявляется параллельно с явлениями и процессами своего объекта, что раскрывает его оперативный характер, а предварительный контроль носит ярко выраженный превентивный (защитный) характер. Профилактика тоже находит место в текущем контроле, но с момента начала развития. Может найти применение в качестве «стопора» негативного развития и предотвращения накопления негативных эффектов. Функция «стопор» выполняет систему запретов и предупреждений, которая является неотъемлемой частью структуры любого современного программного продукта.
- **Контроль итоговой информации (последующий)** - целью этого контроля является устранение ошибок, допущенных к настоящему времени при обработке данных, и проверка вывода полученной информации. Для каждой технологической операции автоматизированной обработки данных применяются разные методы контроля.

Необходимо указать, что восприятие того или иного способа контроля зависит от типа используемых технических средств, технических носителей, типа и характера обрабатываемой информации, т.е. виды контроля используются в зависимости от конкретных условий и целесообразности.

2. В зависимости от технологии контроля, он может быть:

Автоматизированный (программное управление) - методы и средства управления являются неотъемлемой частью программного продукта. Он состоит из специальных операций, используемых при работе программного продукта. Эти операции устанавливаются программистами для управления действиями конечных пользователей Защита от случайных ошибок (непреднамеренное нажатие клавиши или сработавшая процедура). Наиболее важные из них являются:

- Инструкция по устранению ошибок;
- Вспомогательные тексты;
- Предупреждающие тексты;
- Инструкции по предыдущим и следующим операциям;
- Использование механизма альтернативного выбора;
- Использование механизма специально подготовленных номенклатурных полей;

- Контроль размера и формата данных;
- Контроль количества выполняемых операций;
- Контроль достижения заранее установленных лимитов.

Визуальный – пользователь осуществляет визуальный контроль над входной и выходной информацией, отслеживая работу программного продукта.

Каждая система защиты информации в корпорации должна одновременно отвечать некоторым общепринятым требованиям и иметь свои особенности.

Основные виды защиты информации являются следующие: спрятать, декомпозиция, дезинформация, разделение, страхование, отчетность, и шифрование.

Маскировка – это основной вид защиты, реализуемый на практике, и один из основных организационных принципов защиты информации. Максимально ограниченное количество пользователей, имеющих доступ к информационной системе, размещение и хранение информации в недоступных местах, а также ее секретность являются - основными средствами этого метода. Засекречивание информации на практике означает принадлежность к особой группе - секретная информация, с разной степенью секретности. В большинстве случаев она имеет различное значение для своего владельца и имеет к нему особый контролируемый доступ. Скрытая информация обычно исключает массовый доступ к информации, а также каналы ее утечки.

Декомпозиция – это вид защиты, который предполагает разделение секретной информации на степени секретности. Во время декомпозиции доступ к защищенной информации организуется, дифференцируется и регулируется. На практике это означает, что каждому отдельному пользователю предоставляются индивидуальные права на доступ к определенной информации, необходимой для выполнения определенных операций. Разграничение доступа может производиться на основе функциональных возможностей или на основе степени секретности информации. Декомпозиция как метод защиты информации является особым случаем сокрытия, потому что, если пользователю не разрешен доступ к информации, которая ему не нужна для выполнения своих официальных обязательств, это скрытая информация.

Дезинформация – это вид защиты информации, заключающийся в целенаправленном распространении заранее подготовленной ложной информации об истинном назначении отдельных объектов или продукции, фактическом состоянии организации или любой из сфер их деятельности.

Разделение - это вид защиты информации, который характеризуется тем, что разделяет защищаемую информацию на части с условием, что их очень сложно, а иногда и невозможно объединить, и добиться значимого результата.

Хранение новой информации – защищенная информация может использоваться повторно в течение неограниченного времени и большим количеством пользователей. Он обладает свойством не разрушаться и не терять своего объема, а в зависимости от использования может даже увеличиваться, т.е. для создания новой информации. Новая информация, в свою очередь, не имеет гарантии защиты и может создавать объективные предпосылки для уязвимости. Вновь созданная информация должна пройти обязательную проверку, прежде чем она будет сохранена и станет частью информационного ресурса организации.

Отчетность – это также один из важных методов защиты информации, обеспечивающий возможность в любой момент в процессе работы системы получать данные о состоянии защищаемой информации и ее пользователях.

Шифрование – это метод защиты информации, выражающийся в ее преобразовании с использованием различных кодов и алгоритмов. Шифрование использует набор символов и систему правил для преобразования информации в форму, недоступную для пользователей. Использование этой информации связано с обязательными операциями по ее декодированию. Шифрование информации может производиться как техническими, так и программными средствами.

Реализация этих основных типов защиты связана с разработкой комплекса организационных средств защиты информации, которые необходимо предоставить, чтобы повлиять на их реализацию. Наиболее важными из них являются:

- **наличие внутренней документации**, устанавливающей правила работы с компьютерным оборудованием и конфиденциальной информацией;
- **подписание дополнительных соглашений** к трудовым договорам сотрудников, в которых указана ответственность за разглашение или неправомерное использование секретной информации;
- **проведение инструктажей** и периодических проверок персонала;
- **разграничение сфер ответственности**, исключая, по возможности, ситуации, когда наиболее важные файлы данных доступны одному из сотрудников;
- **организация работы в общих программах,** которые в процессе своего функционирования осуществляют внутренний контроль;
- **организация хранения данных таким образом,** чтобы важные файлы не хранились вне сетевых устройств;
- **внедрение программных продуктов,** защищающих данные от копирования или уничтожения любым пользователем, включая высшее руководство организации;
- **составление планов восстановления системы** в случае отказа по любой причине.

Все эти комплексные меры должны входить в компетенцию ИТ-отдела компании и, в частности, службы безопасности. Если в компании нет такого отдела, можно пригласить внешнего специалиста по безопасности. Он может провести аудит ИТ-инфраструктуры компании и дать ценные советы о том, как защитить ее от внешних и внутренних угроз.

ВЫВОДЫ

В заключение можно сделать вывод, что для достижения надлежащего и полного контроля и защиты информации в корпоративной информационной системе, подход должен быть рассмотрен до ее создания и внедрения, а потом реализован последовательно. При организации информационной системы применяются как определенные базовые принципы, так и определенные организационные меры, направленные на создание необходимой среды, обеспечивающей безопасность корпоративных ресурсов.

Во-первых, необходимо интегрировать систему контроля и защиты информации. Целостность системы выражается в наличии единых целей ее функционирования, наличии информационных связей между элементами системы, иерархии ее отдельных функциональных единиц;

Во-вторых, система контроля и защиты информации должна обеспечивать безопасность информации и отстаивать интересы участников информационного процесса;

В-третьих, методы и средства, используемые системой управления информационной безопасностью, должны быть «прозрачными» для авторизованных пользователей. Желательно, чтобы они не создавали дополнительных неудобств, связанных с процедурами доступа к данным и их обработки;

В-четвертых, система контроля и защиты информации обязана обеспечивать информационные связи между элементами в ней, их совместное и согласованное функционирование, обеспечивать связи с внешней средой, в которой корпоративная информационная система представлена как единое целое;

В-пятых, необходимы упрощенные подходы к контролю и защите информации. Сложная система правил для полной безопасности столкнется с серьезными проблемами при ее реализации и нагрузкой на общение между сотрудниками. Правила контроля и защиты должны быть простыми в применении, а потребители, в свою очередь, должны осознавать их необходимость.

В-шестых, необходима четкая стратегия контроля и защиты. Сотрудники должны быть знакомы с четко определенными методами и средствами контроля и подчиняться им. Перед внедрением корпоративной информационной системы необходимо разработать правила работы для подготовки персонала. Программа контроля и защиты информации должна содержать все основные элементы, физические, программные и технические средства защиты, план работы с персоналом, план восстановления и т. д.

БИБЛИОГРАФИЯ

1. Галатенко П.К. Стандарты информационной безопасности, Москва, ИНТУИТ, 2006. 264 с. ISBN 5-9556-0053-1
2. Герасименко В. А. Защита информации в автоматизированных системах обработки данных, Енергоатомиздат, Москва 1994. 400с.
3. Мельников В. В. Защита информации в компьютерных системах. Финансы и статистика, Москва 1997. 368 с. ISBN 5-279-01631-4.
4. Шишманов К. Автоматизирани системи за контрол и защита на информацията. АИ Ценов, Свищов, 2008. 143 с. ISBN: 978-954-427-797-0
5. Highland H.J. Microcomputer security: Data protection techniques. Computers & Security, Volume 4, Issue 2, June 1985, Pages 123-134. ISSN: 0167-4048

FOREIGN EXPERIENCE OF DEFENDING THE FREEDOM OF BELIEF AND THEIR FREE EXPRESSION

ЗАРУБЕЖНЫЙ ОПЫТ ОТСТАИВАНИЯ СВОБОДЫ УБЕЖДЕНИЙ И ИХ СВОБОДНОГО ВЫРАЖЕНИЯ

Чирков Евгений
Доктор политических наук, доцент
Комратский государственный университет
e-mail: chirkove@mail.ru

Abstract
Paper describes the international experience of the ensurance of the freedom of convictions and their free expression. It is determined that the most effective among the bodies, created by the UN and the Council of Europe which have created some institutions for the protection of people, is the European Court of Human Rights. However, all of them are only the additional institutions for the national courts of the protection of the convention rights and freedoms.

Keywords: *freedom of belief, the UN Committee on Human Rights, Council of Europe, the EU Charter of Fundamental Rights.*

JEL Classification: *K38*

ВВЕДЕНИЕ

Права и основные свободы человека на протяжении как минимум полувека были не только компетенцией государства, но и стали делом всего мирового сообщества с того момента, когда в ряде важных международных договоров они были закреплены как общие стандарты прав и свободы личности. Еще после Первой мировой войны Лига Наций сделала попытку создать механизм защиты прав отдельных людей, который оказался довольно слабым. Важнейший критерием степени цивилизованности современного общества считается обеспечение государственной властью прав и основных свобод человека в стране. Таких прав и основных свобод человека, включая свободу убеждений и их свободное выражение, которые ученые относят к универсальным правам и свободам, то есть таким, которые принадлежат всем людям без исключения, независимо от их принадлежности к определенной национальности, религиозным, языковым, культурным или другим группам (сообществам), гарантируются Конституциями многих демократических стран по всему миру и являются ядром ряда международных соглашений.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Каждая страна в мире, взявшая на себя обязательство реализовывать нормы международных договоров в области прав человека и основных свобод, должна сделать их приоритетом в национальном законодательстве. Нормы, содержащиеся в международных договорах, обязательны для законотворчества развитых стран, являющимися международными стандартами, которые необходимо внедрять в реальную жизнь не только в законотворческом процессе, а что не менее важно вовремя правоприменения. Источники международных прав (международный договор, международный обычай, общие принципы права, судебные решения

доктрины известных экспертов, законотворческие решения международных форумов и тому подобное) являются основой национальных законодательных систем в различных сферах общества, в частности, в обеспечении свободы убеждений и их свободного выражения.

Странам, которые не так давно стали на путь создания правового, демократического и социального государства, безусловно необходимо очень много претворять в жизнь касательно положения о свободе убеждений и их свободного выражения, признанного международным сообществом стандартов, национального законодательства и, соответственно, создание эффективных механизмов их реализации в нормах, которые будут носить не только декларативный характер, но также оказывать мощное влияние на правительства тех государств, которые присоединятся к соответствующим международным договора и возьмут на себя ответственность перед мировым сообществом за внедрение международных стандартов в обеспечении свободы убеждений и их свободное выражение стране. По мнению Александру Сосна, содержание понятия «свобода мысли и слова» заключается в том, что никто не может запретить человеку следовать своим мыслям, отображать объективную реальность в их собственном восприятии, публично выражать эти материализованные в речи отображения, как взгляды и убеждения [3].

Впервые право на свободу убеждений и свободу их выражения было закреплено в провозглашенной ООН в 1948 г. Обшей Декларации прав человека (статья 19), в которой содержится суть свободы убеждений и их свободного выражения: «Каждый человек имеет право на свободу убеждений и на свободное их выражение; это право включает свободу беспрепятственно придерживаться своих убеждений и свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ» [5]. Однако, как отмечают ученые, закрепленное в Декларации права и свободы, включающие свободу убеждений и их выражения не является абсолютными, поскольку п. 2 ст. 29 Декларации допускает их ограничение «... каждый человек подлежит только таким ограничениям, которые установлены законом исключительно с целью обеспечения надлежащего признания и уважения прав и свобод других и обеспечения справедливого требований морали, общественного порядка и общего благосостояния в демократическом обществе» [5]. Следует отметить, что Декларация, являющаяся резолюцией и потому в соответствии с Уставом ООН, имеющая не обязательный, а рекомендательный характер, стала основой деятельности ООН, поскольку ее из-за массовых нарушений, провозглашенных в ней прав человека в период до и во время Второй мировой войны, было формализовано первое согласованное на международном уровне признание прав человека.

Следующим шагом международного сообщества касательно развития прав человека и основных свобод было принятие Советом Европы 1950 г. Конвенции о защите прав человека и Основных свобод. Следует отметить, что для стран, стремящихся к членству в Совете Европы, обязательным условием является ратификация и имплементация норм Конвенции в национальном законодательстве, что является юридически обязательным условием для них.

Рассматривая положения Декларации касательно свободы выражения взглядов, мы видим, что с одной стороны, в ст. 10 Конвенции, провозглашается право каждого «… на свободу выражения своих взглядов. Это право включает свободу выражать свои взгляды, получать и предоставлять информацию и идеи без вмешательства государственной власти и независимо от государственных границ», а с другой стороны, определяется и конкретизируется предостережение, когда в его

обеспечение имеет право вмешиваться государство: государству предоставляется право принимать такие формальности, условия, ограничения или санкции, которые установлены законом и необходимы для демократического общества, национальной безопасности, территориальной целостности или общественной безопасности, с целью предотвращения беспорядков или преступлений, для защиты здоровья или моральных устоев, для защиты репутации или прав других особ, для предотвращения раскрытия конфиденциальной информации или для поддержания авторитета и беспристрастности суда [3]. Таким образом указываются три причины, по которым государство может принять меры, предусмотренные законом: причина (указанные предостережения) должна быть предусмотрена законом; преследовать одну из указанных целей и считаться необходимым в демократическом обществе.

Одним из главных достижений Конвенции стало создание Института контроля в рамках Совета Европы в соответствии со ст. 19 - Европейского суда по правам человека (Страсбург). Государства-члены, участвующие в Совете Европы должен признать юрисдикцию Европейского суда по правам человека, обязательные для толкования и применения Европейской Конвенцией о правах человека и протоколы к ней в случаях нарушений в стране положения этих соглашений. Подача жалоб в Суд по правам человека возможна в случаях, если все возможности защиты в стране исчерпаны. Суд, рассматривая дела о нарушении положений ст. 10 Конвенции разъяснил, что свобода выражения взглядов как один из основополагающих столпов демократического общества, включает в себя не только определение взглядов посредством высказываний, а также с помощью рисунков, печатных СМИ, теле- и радиовещания, спектаклей, фильмов, электронных систем, рекламных акций, совершаемых с намерением выразить позицию или предоставить информацию. В своих решениях Европейский суд по правам человека может потребовать от конкретного государства – члена Совета Европы, пересмотреть определенные судебные решения, рекомендовать изменить нормы национального законодательства, нарушающие права конкретных лиц.

Впоследствии между странами во время имплементации ст. 19 Всеобщей декларации возникли определенные недопонимания: некоторые страны обвиняли других в запрете своим гражданам права на свободное получение и распространение информации, на что в ответ от них получили обоснование законности защиты своих граждан от пропаганды войны, фашизма, насилия, порнографии, что имеют место быть за рубежом [2, с. 29–30]. По этой причине Генеральная Ассамблея ООН в 1966 г. приняла Международный пакт о гражданских и политических правах (вступил в силу в 1976), в ст. 19 которого, сохраняя общее право придерживаться своих взглядов, право искать, получать и распространять информацию и идеи различных аспектов в любой форме (устной, письменной) была добавлена норма про то, что использование этих прав накладывает особые обязанности и особую ответственность на человека.

Кроме того, ст. 20 Международного пакта о гражданских и политических правах устанавливает для государств-членов запрещающие для них законы любой формы пропаганды войны и разжигания национальной, расовой или религиозной ненависти, если они представляют собой разжигание дискриминации, вражды или насилия в отношении людей. Для контроля правильного соблюдения Международного пакта о гражданских и политических правах в соответствии со ст. 28 создан Комитет ООН по правам человека (Нью Йорк, Женева), который имеет право рассматривать заявления от физических лиц, которые стали жертвами

нарушений прав, закрепленных в МПГПП[2], в частности права, предусмотренного ст. 19. Однако, как и в Европейском суде по правам человека, важным аспектом деятельности Комитета является то, что лицо должно исчерпать все средства правовой защиты в своей стране, прежде чем отправлять претензию в Комитет ООН по правам человека.

Комитет осуществляет контроль за выполнением государствами своих обязательств в форме рассмотрения отчетов государств об исполнении постановлений МПГПП, принятии индивидуальных жалоб граждан на нарушения их прав.

В последние годы наблюдается тенденция по изучению комитетами ситуации в государствах не только на основании отчетов, подготовленных и предоставленных государственными органами, а также информации о статусе неправительственных правозащитных организаций в стране, которые во многих случаях являются независимыми и их видение ситуации часто отличается от видения ситуации представителями органов государственной власти. Это конечно способствует более глубокому и всестороннему изучению положения дел в рассматриваемой стране. Комитеты отправляют сообщения о соблюдении государствами соответствующих постановлений МПГПП для подготовки годового отчета о положении дел человека в мире для Генеральной Ассамблеи ООН. В системе ООН, в соответствии с Факультативным протоколом № 1 к МПГПП, работает также защита прав человека в форме принятия заявлений от граждан. Таким способом правовой защиты можно воспользоваться непосредственно пострадавшим от нарушений прав человека или их представителям, если страна проживания ратифицировала и МПГПП, и настоящий Протокол. Так, граждане Республики Молдова, ратифицировавшей МПГПП в 1990 г. [8] и Факультативный протокол к Международному пакту о гражданских и политических правах в 2007 году с обоснованными заявлениями и оговорками. При ратификации Протокола молдавский парламент постановил, что «до полного восстановления территориальной целостности Республики Молдова положения Протокола применяются только на территории, фактически контролируемой властями Республики Молдова» [7], вправе обращаться с индивидуальными заявлениями на нарушение прав, гарантированных Пактом и Протоколом к ООН, в Комитет по правам человека.

В системе органов ООН с 1993 г. осуществляет деятельность Специальный докладчик по вопросам продвижения и защиты прав человека, включая свободу убеждений и их выражения, который обладает важными специальными полномочиями, включая анализ полученных сообщений с целью выявления тенденций, подготовки регулярных отчетов, написания обращений и писем с целью привлечения внимания международного сообщества к отдельным направлениям политики и практики, что влияют на положение дел, касающихся уважения права на свободу выражения убеждений. Обычно Специальный докладчик изучает сообщения, отправленные ему из различных источников - Правительства, международных, региональных, национальных и местных неправительственных организаций, ассоциаций всех регионов мира, чтобы обращать внимание Совета по правам человека и Верховного комиссара ООН по правам человека на такие ситуации и случаи, касающиеся права на свободу мнений и их свободного выражения, которые вызывают особо серьезную обеспокоенность.

[2] МПГПП - Международный пакт о гражданских и политических правах

Во время Саммита глав государств и правительств в 2005 г. в г. Нью-Йорке было решено создать еще один орган ООН в области прав человека - Совет ООН по правам человека (СПЧ), в рамках выполнения которого в 2006 г. 60 сессия Генеральной Ассамблеи Организации Объединенных Наций приняла резолюцию 60/251 [6]. Согласно резолюции, главной целью СПЧ является продвижение всеобщего уважения и защиты всех прав человека и основных свобод для всех без каких-либо исключений и на справедливой и равной основе (п. 2); она видела ситуацию, связанную с нарушением прав человека, включая грубые и систематические нарушения, и дать им свои рекомендации, а также способствовать эффективной координации и интеграции деятельности, связанной с правами человека, в рамках системы Организации Объединенных Наций (п. 3). Основой этой системы являются принципы универсальности, беспристрастности, объективности и избирательности, конструктивного международного диалога и сотрудничества с целью содействия поощрению и защите всех прав человека, включая свободу убеждений и их свободного выражения (п. 4), уникальной особенностью является непосредственный доступ членов СПЧ к информации через связь с Правительством и другими заинтересованными сторонами, в частности, действующие в области человеческих прав в тесном сотрудничестве с правительствами, региональными организациями, национальными правозащитными учреждениями и гражданским обществом (п. 5 h). Более того, в Совете на основе принципа равных подходов и критериев для всех стран без исключения действует механизм универсального периодического обзора (УПО), с помощью которого проводится обзор выполнения всеми государствами-членами ООН своих обязательств в области прав человека, что позволило решить ряд проблем нарушений прав человека в течение первого цикла (2006–2011 гг.). В мае 2012 г. начался второй цикл универсального периодического обзора.

В Договор ЕС в соответствии с изменениями, внесенными в Лиссабонский договор, вступивших в силу в 2009 г., была внесена поправка, согласно которой Хартия Европейского Союза об основных правах [4, с. 302–314] с 1 декабря 2009 г. стала юридически обязательным документом для всех стран ЕС (с определенными оговорками относительно отдельных стран - Великобритании, Польши, Чехии). В первой части ст. 11 Хартии «Свобода выражения своих убеждений и свобода информации», как и статья 10 Европейской конвенции защиты прав человека и основных свобод закреплено: «Каждый имеет право на свободу выражения мнения. Это право включает свободу придерживаться своих взглядов, получать и делиться информацией и идеями без вмешательства органов государственной власти и независимо от государственных границ». Во-второй части, помимо собственной свободы, должен быть гарантированы плюрализм и разнообразие: «придерживаться свободы и плюрализма СМИ». Таким образом, важный аспект позитивных обязательств государств поощрения свободы выражения убеждений лежит в необходимости развития плюрализма и обеспечения равного доступа к информации для всех.

Некоторые ученые считают Хартию «более современным инструментом для защиты прав человека по сравнению с Конвенцией, которая была принята более полувека назад ... содержит не только права особенного и политического характера, а также процессуальные гарантии этих прав… регулирует экономические, социальные права и некоторые права четвертого поколения… учитывает научно-технический прогресс и, устанавливает права, связанные с биомедициной и

воспроизведением» [9]. Вне всяких сомнений, Хартия содержит гораздо больший перечень прав и свобод человека, учитывая вызовы современного состояния гражданского общества. Однако возникают разумные сомнения относительно процессуальных гарантий этих прав, потому что в Хартии не предусмотрен контрольный механизм, как например, Европейский суд, созданный в соответствии с Европейской Конвенцией.

В мире существует разветвленная система из нескольких десятков универсальных и региональных международных органов по правам человека с разным количеством компетенций [1], в частности, наиболее известная из них: система защиты прав человека (квази-суд и конвенционные органы); региональный: европейская система защиты прав человека, африканская система защиты прав человека, американская система защиты прав человека; система национальной защиты прав человека и другие механизмы. Наиболее обширной и всеобъемлющей является система защиты прав человека (см. рис.1).

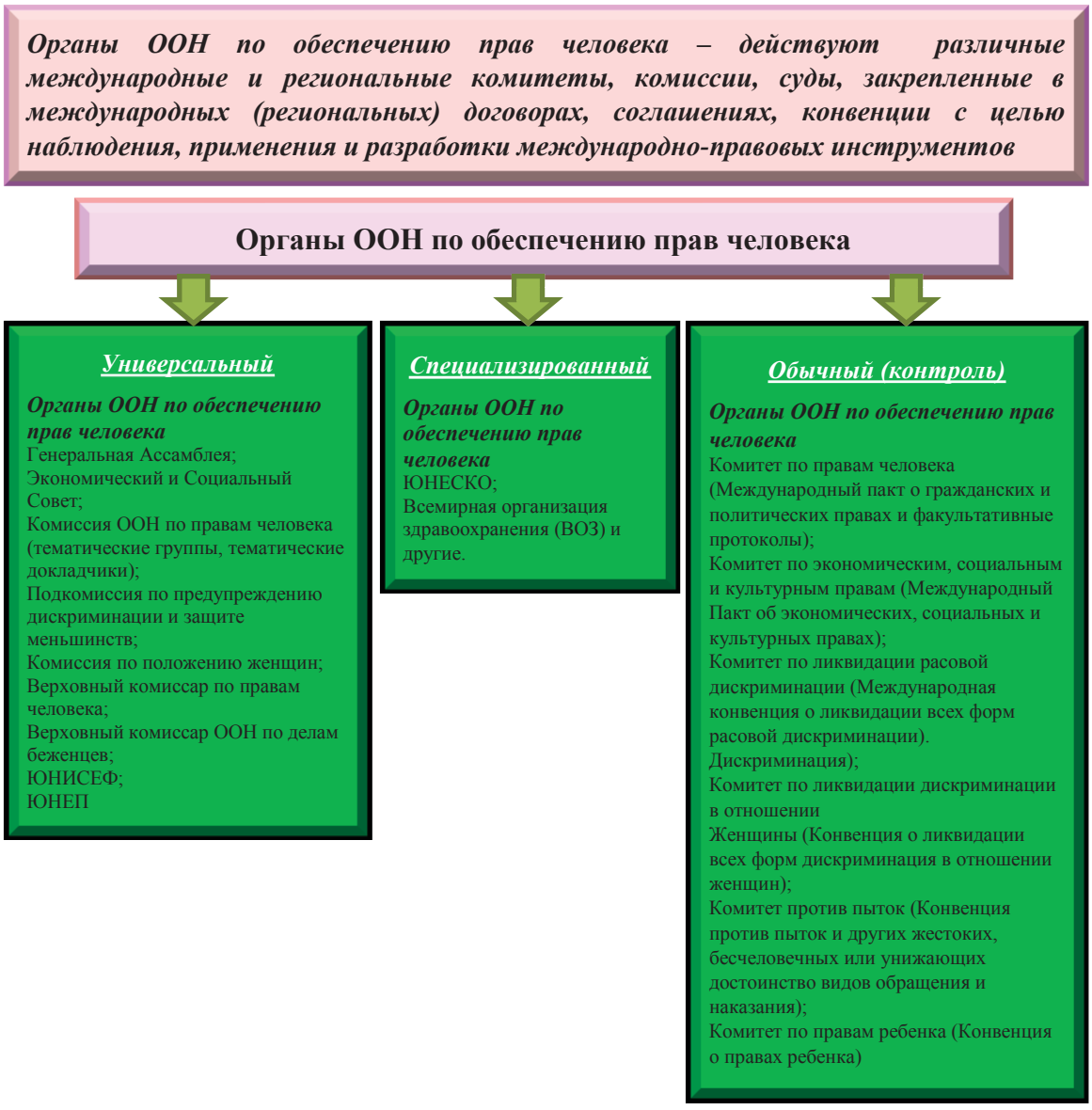


Рисунок 1. Органы ООН по обеспечению прав человека

ВЫВОДЫ

Итак, рассмотрев международные системы, касательно обеспечения свободы убеждений и их свободного выражения, мы можем констатировать, что наиболее эффективным органом является европейский Суд по правам человека. Однако следует отметить, что, как и Комитет ООН по правам человека, и Специальный докладчик по вопросам поощрения и защиты прав человека, и Совет ООН по правам человека и др. органы являются лишь дополнением к национальным судам Института защиты конвенционных прав и свобод, поскольку что обращение в международные органы возможно только после исчерпания всех средств правовой защиты в своей стране. Таким образом, в соответствии с актуальными вызовами относительно свободы убеждений и их свободного выражения в государствах необходимо разработать комплексный подход, который включал бы следующие элементы: внедрение международных стандартов в национальное законодательство; создание действенного механизма их поддержки; реформирование органов государственной власти, судебной власти, прокуратуры и правоохранительных органов, в основу деятельности которых следует вложить такие демократические принципы как: верховенство закона, разделение властей, законность, открытость, принцип избирательности основных органов государственной власти, плюрализм, неприкосновенность прав граждан.

БИБЛИОГРАФИЯ

1. Буриан А. Характеристика дипломатической службы Республики Молдова. В: Московский журнал международного права. 2003, № 4.
2. Рихтер А.Г. Международные стандарты и зарубежная практика регулирования журналистики: учеб. пособ. / А.Г. Рихтер. - Изд. ЮНЕСКО. - М., 2011.
3. Сосна, Александру. Конвенция о защите прав человека и основных свобод. Европейский суд по правам человека / Сосна Александру; науч. ред.: Захария Сергей; Ин-т демократии. – Комрат: Institutul pentru Democraţie, 2017 («MITRA-GRUP» S.A.). – 328 p. Bibliogr.: p. 235-254 (381 tit.). – Referinţe bibliogr. în subsol. – Изд. при поддержке Европейского Союза. – 5000 ex. ISBN 978-9975-3126-9-1.
4. Хартия основных прав европейского союза (принята в г. Ницце) 07.12.2000) // Московский журнал международного права. - 2003. - № 2.
5. Всеобщая декларация прав человека [Электронный ресурс]. - Режим доступа: https://www.un.org/ru/universal-declaration-human-rights/index.html
6. Резолюция, принятая Генеральной Асамблеей / 60/251. Совет по правам человека [Электронный ресурс]. - Режим доступа: http://www.elibrary.humanrightshouse.org/library/doc1/arh/11.pdf
7. Руководство по правам человека для государственных служащих/ авт.: Анатолий Мунтяну, Светлана Русу, Ольга Вакарчук; пер. с рум.: Валентин Рябцов; Офис Народного Адвоката. – Изд. 2-е, перераб. и доп. – [Кишинэу.] Arc, 2016 (Типогр. „Bons Offices“), - 328 стр. ISBN 978-9975-61-951-6[Электронный ресурс]. - Режим доступа: https://rm.coe.int/16806f12b9
8. Формирование современной молдавской государственности и отношения с национальными меньшинствами [Электронный ресурс]. - Режим доступа: https://regnum.ru/news/polit/1454307.html
9. Хартия основных прав европейского союза [Электронный ресурс]. - Режим доступа: https://ava.md/2019/07/07/hartiya-evropeyskogo-soyuza-ob-osnovnyh/

BACKUP AND RECOVERY STRATEGIES AND THEIR ROLE IN BUSINESS CONTINUITY

STRATEGII DE BACKUP ȘI RECUPERARE ȘI ROLUL LOR ÎN CONTINUITATEA AFACERII

Zgureanu Aureliu
Doctor în științe fizico-matematice, conferențiar universitar
Academia de Studii Economice a Moldovei
e-mail: zgureanu.aureliu@ase.md

Abstract
IT disaster recovery is one of the most important component of business continuity process. Companies need it for recovering disrupted systems and networks and resume normal operations every time when disruptions occure. Disaster recovery becomes more important from day to day because it allows minimizing any negative impacts to company operations. Disaster recovery is a business continuity process that ensures access to the software, hardware, and data required to resume normal business operations in the event of a natural or human-induced disaster. Implementation of a good distaer recovery plan begins with choosing the best strategies for this goal. The correlation of the business continuity, disaster recovery and the best strategies in this field are analysed in this paper.

Keywords: *backup, recovery, disaster, business continuity, strategy.*

JEL Classification: *H12, M15*

INTRODUCERE

În IT, un dezastru poate fi orice problemă neașteptată care duce la o încetinire, întrerupere sau o eroare într-un sistem cheie sau o rețea. Aceste probleme pot fi cauzate de dezastre naturale (adică incendii, cutremure, uragan, etc.), erori tehnologice, acte rău intenționate, diverse tipuri de incompatibilități sau chiar de simple erori umane. Probabilitatea ca un astfel de dezastru să aibă loc poate crește odată cu dezvoltarea organizației și a infrastructurii sale IT, a concurenței neloiale și a multor altor factori. Totodată, cea mai bună apărare orientată spre evitarea urmărilor dezastruoase ce pot apărea în astfel de situații constă în planificarea continuității afacerii și a recuperării datelor în caz de dezastru, folosind cele mai bune practici și strategii care ghidează organizațiile în prevenirea și/sau gestionarea mai bună a evenimentelor perturbatoare imprevizibile.

Ținând cont de ultimele date statistice, o organizație nu poate să-și permită riscul confruntării cu un dezastru IT fără a fi pregătită de astfel de scenarii, deoarece urmările perturbărilor catastrofale ale datelor organizației, și implicit a reputației sale, o poate costa foarte mult, până chiar și la pierderea afacerii. Institutul Ponemon și IBM Security în raportul *Cost of a Data Breach Report* pentru anul 2020 [1] a constatat că costul mediu al unei încălcări de date la nivel global este de 3,86 milioane de dolari (3,90 în 2019 și 3,86 în 2018). Același raport pentru anul 2018 arată că 65 la sută dintre clienții cărora le-au fost compromise datele au spus că și-au pierdut încrederea într-o organizație, iar unul din trei a ales să-și întrerupă relația cu organizația afectată. În acest context recuperarea datelor capătă o conotație specială și devine una dintre elementele de bază ale Managementului continuității unei afaceri.

Standardul ISO/IEC 27031:2011: Tehnologia informației - Tehnici de securitate - *Linii directoare pentru disponibilitatea tehnologiilor de informare și comunicare pentru continuitatea afacerilor* specifică recuperarea dezastrelor IT ca capacitatea elementelor

TIC ale unei organizații de a-și susține funcțiile critice de afaceri la un nivel acceptabil într-o perioadă de timp prestabilită după o întrerupere. În același document este definit și Planul de continuitate a afacerii (BCP -Business Continuity Plan) și Planul de recuperare în caz de dezastru TIC (ICT DRP – Disaster Recovery Plan) [2].

Planul de continuitate a afacerii reprezintă un set de proceduri documentate care ghidează organizațiile să răspundă, să recupereze, să reia și să restabilească la un nivel predefinit de funcționare în urma întreruperii. În mod normal, aceasta acoperă resursele, serviciile și activitățile necesare pentru a asigura continuitatea funcțiilor critice ale afacerii.

Planul de recuperare în caz de dezastru TIC este un plan clar definit și documentat care recuperează capacitățile TIC atunci când apare o perturbare (uneori acesta se mai numește plan de continuitate TIC).

Astfel, recuperarea resurselor IT în caz de dezastru este un set standard de politici și proceduri pe care o afacere sau o organizație le pune în aplicare și le urmează pentru a se proteja pe sine și personalul său în fața unui dezastru. Planurile de recuperare în caz de dezastru pot ajuta compania să asigure securitatea angajaților, a hardware-ului și software-ului, restaurarea sistemelor și a elementelor conexe continuității afacerii. DRP-urile pot include măsuri preventive, măsuri corective și măsuri detective pentru a preveni cât mai mult posibil dezastrele care ar putea afecta întreprinderile, reducând în același timp, într-un mod cât mai fiabil posibil, impactul unui dezastru.

Măsurile preventive sunt acele măsuri care diminuează riscul și previn apariția unui dezastru IT, iar exemplele de aceste măsuri includ backup-ul datelor în cloud, efectuarea de audituri de securitate de rutină etc. Măsurile detective ajută la descoperirea potențialelor amenințări, de exemplu, actualizarea software-ului antivirus, instalarea software-ului de monitorizare server/rețea etc. Măsurile corective conțin pașii necesari pentru restabilirea rapidă a sistemelor IT lovite de dezastru. Toate aceste măsuri sunt importante în realizarea procesului de recupearre IT și deaceea trebuie tratate cu responsabilitate maximă.

CONTINUITATEA AFACERILOR

Continuitatea afacerii (BC - Business Continuity) este procesul de minimizare a riscului de perturbare. Mai precis, continuitatea afacerii înseamnă efortul necesar pentru a reduce probabilitatea unui incident perturbator și pregătirea organizației pentru a continua livrarea celor mai esențiale produse și servicii, dacă ar avea loc o perturbare.

Un proces de continuitate a afacerii ar trebui să implice la două lucruri:

- înțelegerea riscurilor legate de perturbările cu care se poate confrunta afacerea;
- încrederea executivilor în capacitatea organizației de a reacționa și de a se recupera.

Acesta poate fi numit nivelul corect de reziliență. Continuitatea afacerii este, de asemenea, cunoscută sub numele de planificare a continuității, reziliență organizațională sau management al continuității afacerii.

Continuitatea afacerii se bazează pe parcurgerea a câtorva pași fundamentali [3]:

a) în primul rând, este necesar de a identifica produsele sau serviciile critice care trebuie protejate;
b) apoi, trebuie identificate riscurile pentru produsele sau serviciile respective; acestea sunt cel mai adesea resursele necesare livrării, în special persoane, tehnologii, facilități, echipamente și terțe părți;
c) odată ce resursele sunt identificate, este necesar de a implementa strategii care protejează resursele cheie (cum ar fi munca la distanță, procesele manuale sau facilități alternative);
d) în continuare, pot fi documentate planurile de continuitate a afacerii care prezintă modul de implementare a strategiilor de recuperare;

e) în cele din urmă, se efectuează exerciții și teste pentru a confirma că planurile și strategiile funcționează conform așteptărilor.

Există o serie de discipline legate de continuitatea afacerii, inclusiv:

- *managementul situațiilor de urgență* - este o disciplină axată pe probleme specifice instalației care implică siguranța vieții și protecția proprietății;
- *recuperarea în caz de dezastru*, cunoscută și sub numele de *recuperare în caz de dezastru IT* - este o disciplină axată pe protejarea și recuperarea tehnologiei și a datelor;
- *managementul riscului* - continuitatea afacerii este un tip special de proces de management al riscului; alte procese de gestionare a riscurilor includ conformitatea și securitatea informațiilor;
- *managementul crizelor* - acest efort se concentrează pe răspunsul executiv la perturbări și este o parte cheie a continuității afacerii.
- *comunicarea în situații de criză* - acest efort se concentrează pe aspectul de comunicare când reacționăm la un dezastru și merge mână în mână cu gestionarea crizelor.

De ce am avea nevoie de conceptul „continuitate a afacerii”? Continuitatea afacerii ajută la protejarea unei organizații, indiferent de dezastrul care poate apărea. Și acest lucru este important în lumea din ce în ce mai imprevizibilă de astăzi! Fie că este vorba de perioade de nefuncționare neprogramate ale tehnologiei, de o întrerupere a lanțului de aprovizionare, de un dezastru natural sau de un eveniment provocat de om, organizațiile de toate dimensiunile recunosc că trebuie să fie pregătite pentru aproape orice. Majoritatea organizațiilor construiesc un plan de continuitate a afacerii din unul dintre cele trei motive:

- clienții o cer (cel mai frecvent în modelul B2B);
- autoritățile de reglementare o cer (cel mai frecvent în domeniul bancar și energetic);
- consiliul de administrație sau directorii superiori o cer (recunoscând responsabilitatea lor fiduciară).

Toate aceste grupuri solicită continuitatea afacerii ca o modalitate de a proteja organizația pe termen lung.

Continuitatea afacerii este reglementată la nivel internațional de standardul ISO 22301, care la nivel național este înscris în registrul de Stat al standardelor sub numele „SM EN ISO 22301:2020. *Securitate și stabilitate. Sisteme de management al continuității activității. Cerințe*” [2]. Există patru beneficii esențiale ale afacerii pe care o companie le poate obține prin implementarea acestuia:

1. Respectarea cerințele legale. Există din ce în ce mai multe țări care definesc legi și reglementări care necesită respectarea continuității afacerii. Și dincolo de interesele guvernamentale, întreprinderile private (de exemplu, instituțiile financiare) solicită, de asemenea, furnizorilor și partenerilor să implementeze soluții de continuitate a afacerii. Și vestea bună este că ISO 22301 oferă un cadru și o metodologie perfectă pentru a sprijini respectarea acestor cerințe - prin reducerea efortului administrativ și operațional, precum și a penalităților care trebuie plătite.

2. Obținerea unui avantaj de marketing. Dacă o companie este certificată ISO 22301 și concurenții ei nu, respectiva companie va avea un avantaj față de aceștia atunci când vine vorba de clienții care sunt sensibili la păstrarea continuității operațiunilor lor și la livrarea produselor și serviciilor lor. În plus, o astfel de certificare poate ajuta și la obținerea de clienți noi, facilitând demonstrarea apartenenței la cei mai buni din industrie, ceea ce duce la creșterea cotei de piață și la profituri mai mari.

3. Reducerea dependenței de peronal. De cele mai multe ori, activitățile critice ale unei companii se bazează doar pe câțiva oameni greu de înlocuit - situație demonstrată dureros când acești oameni părăsesc organizația. Directorii care sunt conștienți de acest lucru pot face uz de practicile de continuitate a afacerii pentru a deveni mult mai puțin

dependenți de acei angajați ai săi (fie datorită soluțiilor implementate pentru o eventuală înlocuire a acestora, fie prin documentarea sarcinilor conexe), ceea ce înseamnă că se poate preveni o mare durere de cap atunci când cineva părăsește organizația.

4. Prevenirea daunelor la scară largă. Într-o lume a serviciilor și tranzacțiilor în timp real, fiecare minut de stagnare costă bani - mulți bani. Și, chiar dacă afacerea nu este atât de sensibilă la perioade mici de indisponibilitate, incidentele perturbatoare o vor costa. Prin implementarea practicilor de continuitate a activității conforme ISO 22301 se obține un fel de poliță de asigurare. Fie prin prevenirea incidentelor perturbatoare, fie prin capabilitatea de recuperare mai rapidă - compania va economisi bani. Și, cel mai bun lucru dintre toate este că investiția în ISO 22301 este mult mai mică decât economiile pe care le va realiza compania.

RECUPERAREA DATELOR ÎN CAZ DE DEZASTRU

După cum am menționat mai sus – una dintre discipline legate de continuitatea afacerii este *recuperarea în caz de dezastru* – cunoscută și sub numele de recuperare în caz de dezastru IT.

Secțiunea A.17 din anexa A la ISO/IEC 27001 are ca obiectiv pentru o organizație încorporarea continuității securității informațiilor în sistemele sale de gestionare a continuității activității. Pentru a susține acest lucru, această secțiune oferă controale legate de procedurile de continuitate a afacerii, planuri de recuperare și redundanțe [5].

Cu toate acestea, la fel ca toate standardele sistemului de management, ISO 27001 descrie doar ceea ce trebuie realizat, însă nu și cum. Nici ISO/IEC 27002 - colecția de bune practici pentru ISO 27001- nu ajută prea mult în acest sens [8].

Însă familia ISO/IEC 27000 are standarde suplimentare care vizează domenii specifice, iar unul dintre ele este ISO/IEC 27031, care acoperă disponibilitatea tehnologiei informației și comunicațiilor pentru continuitatea afacerii (sau IRBC - ICT Readiness for Business Continuity) și ne ghidează cu privire la ce trebuie să luăm în considerare atunci când dezvoltăm continuitatea afacerii pentru IT - de obicei, aceasta se numește „recuperare în caz de dezastru”. Implementarea ISO/IEC 27031 devine tot mai actuală odată ce tot mai multe activități ale companiilor moderne au devenit dependente de tehnologiile informației și comunicațiilor, iar erorile și defecțiunile IT devin din ce în ce mai critice.

În acest context, standardul ISO/IEC 27031 abordează modul de utilizare a ciclului PDCA (Plan-Do-Check-Act) pentru a pune în aplicare un proces sistematic de prevenire, prezicere și gestionare a incidentelor de perturbare a serviciilor TIC sau a celor care au potențialul de a perturba aceste servicii [3]. Procedând astfel, acest standard ajută la susținerea atât a managementului continuității afacerii, cât și a managementului securității informațiilor. Prin natura sa, ISO/IEC 27031 este un standard perfect pentru realizarea controlului A.17.2.1 din ISO/IEC 27001 (disponibilitatea mijloacelor de prelucrare a informației) [5].

Este adevărat că termenul de recuperare în caz de dezastru nu este un termen oficial ISO și, în consecință, sensul său nu este universal acceptat. Cu toate acestea, majoritatea profesioniștilor IT identifică acest termen cu capacitatea de a recupera infrastructura IT în caz de perturbare. Prin urmare, ISO 27031 este cel mai potrivit dintre standardele ISO anume în acest scop.

Este necesar aici de precizat unele diferențe esențiale între ISO 27031 și ISO 22301. În primul rând, ISO 22301 acoperă continuitatea afacerii în ansamblu, considerând orice tip de incident ca o sursă potențială de perturbare (de exemplu, boală pandemică, criză economică, dezastru natural etc.) și utilizând planuri, politici și proceduri pentru a preveni, reacționa, și recupera după perturbările cauzate de acestea. Aceste planuri, politici

și proceduri pot fi clasificate în două tipuri principale: cele pentru continuarea operațiunilor, dacă afacerea este afectată de un eveniment de perturbare și cele pentru recuperarea infrastructurii IT, în cazul în care sunt perturbate tehnologiile IT.

Prin urmare, ne putem gândi la ISO 27031 ca la un instrument pentru implementarea părții tehnice a ISO 22301, oferind îndrumări detaliate cu privire la modul de a face față continuității elementelor TIC pentru a ne asigura că procesele organizației vor oferi clienților rezultatele așteptate [2]-[3].

ISO 27031 recomandă șase categorii principale care necesită a fi luate în considerare la planificarea continuității afacerii cu referință la elementele care implică TIC și care pot răspunde la întrebările principale care apar în procesul de asigurare a continuității [2]:

1. *Abilități și cunoștințe*: strategiile de recuperare includ luarea în considerare a abilităților tehnice specializate și a cunoștințelor necesare pentru a opera serviciile IT până la, în timpul și după o perturbare; strategiile care includ considerări privind abilitățile și cunoștințele se concentrează pe asigurarea faptului că niciun individ nu deține abilități sau cunoștințe specializate care ar fi necesare pentru a opera sistemele IT ale organizației.
   Aici trebuie luate în considerare:
   - informațiile care sunt necesare pentru a rula serviciile IT critice;
   - persoanele care dețin aceste informații;
   - modul în care pot fi încorporate aceste informații în cunoștințele organizaționale și puse la dispoziție cu ușurință;
   - modul în care organizația face disponibile aceste informații în caz de dezastru.
2. *Echipamente*: strategiile de recuperare includ reducerea riscului asociat cu operarea sistemelor TIC bazate pe un singur echipament; strategiile care includ considerări privind echipamentele asigură utilizarea sistemelor IT chiar dacă echipamentul primar devine inoperabil.
   Pentru aceasta este necesar de avut în vedere:
   - condițiile care ar trebui să le respecte dispozitivele și infrastructura pentru a minimiza riscurile de perturbare sau timpul de recuperare;
   - locul unde ar trebui amplasate astfel de facilități.
3. *Tehnologia*: strategiile de recuperare includ luarea în considerare a cerințelor tehnice necesare pentru a îndeplini cerințele de recuperare ale organizației, în special Obiectivul Timpului de Recuperare (RTO) și Obiectivul Punctului de Recuperare (RPO); strategiile mai includ considerări tehnologice care implică asigurarea faptului că hardware-ul și software-ul și datele pot fi recuperate în timpul solicitat de organizație.
   Aceste considerări ar trebui să includă:
   - tehnologiile cele mai importante pentru afacere - sisteme de asistență, cum ar fi alimentarea, răcirea, personalul, asistența furnizorului și conectivitatea WAN;
   - cerințele de recuperare, de exemplu, RTO, RPO, dependența de alte tehnologii, etc.
4. *Date*: strategiile de recuperare includ luarea în considerare a modului de protejare a datelor solicitate de organizație.
   Strategiile privind datele includ:
   - securitatea, validitatea și disponibilitatea datelor solicitate de utilizatorii finali;

- datele necesare pentru a restabili activitățile comerciale și în ce perioadă de timp (de reținut că RTO și RPO pentru serviciile IT sunt diferite de RPO și RTO pentru date);
- controalele de securitate (de exemplu, controlul accesului) care trebuie să existe în permanență pentru a securiza datele.

5. *Procese*: strategiile de recuperare includ luarea în considerare a modului de susținere a proceselor necesare pentru a monitoriza, opera și recupera sistemele IT pentru a satisface cerințele afacerii; strategiile care iau în considerare procesele identifică procesele IT necesare înainte, în timpul și după o întrerupere a sistemelor IT și anume:
   - procesele pe care le avem la dispoziție pentru a face față unui incident sau dezastru;
   - modul în care procesele necesare pentru a crea elemente din categoriile 1-4 funcționează împreună pentru a furniza serviciile comerciale necesare (de exemplu, comunicații, aplicații, acces utilizator etc.).
6. *Furnizori*: strategiile de recuperare includ luarea în considerare a modului de informare și implicare a furnizorilor care sunt necesari pentru recuperarea și operarea sistemelor TIC.

   Aceste strategii definesc:
   - furnizorii implicați în operarea și recuperarea sistemelor TIC înainte, în timpul și după ce a avut loc o întrerupere;
   - consumabilele (de exemplu, copii de software și piese de schimb hardware) esențiale pentru continuitatea IT, modul în care se pot asigura furnizorii companiei că pot susține cerințele de continuitate a afacerii acestei companii.

STRATEGII DE BACKUP ȘI RECUPERARE

Backup-ul este procesul de creare a unei copii a datelor din sistemul ce trebuie protejat. Această copie se utilizează pentru recuperare în cazul în care datele originale ale organizației sunt pierdute sau corupte. De asemenea, putem utiliza o copie de rezervă pentru a recupera copii ale fișierelor mai vechi, dacă ele au fost șterse din sistem. Multe companii și organizații își protejează datele critice cu ajutorul copiilor de rezervă, făcându-le una dintre componentele cheie ale planului de recuperare în caz de dezastru și ale strategiei de continuitate a afacerii.

Recuperarea este foarte importantă pentru companii, deoarece ele sunt foarte dependente de date. La fel cum o persoană nu poate supraviețui fără aer, apă și alimente, întreprinderile nu pot supraviețui fără date. În conformitate cu raportul anual al phoenixNAP pentru anul 2020 [4], 40-60% dintre întreprinderile mici care pierd accesul la sistemele operaționale și la date fără un plan de recuperare în caz de dezastru își pierd afacerea pentru totdeauna, iar companiile care se pot recupera fac acest lucru la un cost mult mai mare și la un interval de timp mai extins decât companiile care aveau un plan clar de backup și recuperare în caz de dezastru. În același timp 96% dintre companiile care au implementată o soluție de recuperare în caz de dezastru și-au recuperat complet operațiunile.

Odată cu creșterea atacurilor malware și a creșterii costului unei încălcări a securității datelor, securitatea cibernetică a devenit o prioritate de afaceri. Cu toate acestea, chiar și cu măsuri de securitate înăsprite, încălcările au crescut cu 67% în ultimii 5 ani. Drept urmare, nevoia de a avea o strategie solidă de backup a devenit mai importantă ca niciodată. Pentru a fi cu adevărat protejate, organizațiile trebuie să formeze un plan bine definit, care să ajute la recuperarea rapidă și fără probleme a datelor pierdute și să garanteze continuitatea afacerii atunci când toate măsurile preventive eșuează.

O strategie cuprinzătoare pentru recuperare este o parte esențială a conceptului de securitate cibernetică a unei organizații. Ea poate fi definită ca un plan al administratorului pentru a se asigura că datele organizaționale critice sunt copiate și disponibile pentru restaurare în cazul unei situații de pierdere a datelor. O strategie de backup, împreună cu un plan de recuperare în caz de dezastru, constituie unul dintre pilonii de bază în continuitatea afacerii și poate ajuta o organizație să reziste unui atac cibernetic și să se recupereze cu daune minime sau chiar nule pentru afacere, reputație și date.

Abordările care vin să stabilească o strategie în acest sens pot fi diferite de la companie la companie, însă acestea pot fi generalizate prin patru pași, necesari pentru dezvoltarea unei strategii solide de backup, propuși de Matt McDermott, directorul de management al produselor (inclusiv backup-ul) pentru Office 365 și anume [6]:

1. *Determinarea datelor care trebuie copiate*. Pornind de la ideea că toate datele ar trebui să fie copiate, nivelul de protecție a datelor ar varia în funcție de cât de important este să recuperăm un set de date sau altul. Obiectivul timpului de recuperare (RTO) al organizației, care reprezintă *durata maximă acceptabilă necesară pentru ca o organizație să recupereze datele pierdute și să revină la funcționalitatea acceptabilă*, ar constitui un punct de referință fiabil atunci când ne formăm strategia de backup. Este recomandat ca aplicațiile și datele se fie evaluate și grupate în:
   - existențial-critice pentru ca afacerea să supraviețuiască;
   - critice pentru ca organizația să funcționeze;
   - optime pentru performanță pentru ca organizația să prospere;

   Odată identificate toate datele pertinente, este necesar de a acoperi nivelul de protecție corespunzător.
2. *Determinarea frecvenței cu care trebuie făcută o copie de rezervă a datelor*. Frecvența cu care facem o copie de rezervă a datelor companiei ar trebui să fie aliniată cu obiectivul punctului de recuperare (RPO) al organizației, care este definit ca *perioada maximă admisibilă între momentul pierderii datelor și ultima copie de rezervă utilă a unei stări bune cunoscute*. Astfel, cu cât datele sunt salvate mai des, cu atât este mai probabil să respectăm RPO-ul declarat al acestei organizații. Ca regulă generală, copiile de backup trebuie efectuate cel puțin o dată la 24 de ore pentru a îndeplini standardele acceptabile ale majorității organizațiilor.
3. *Identificarea și implementarea unei soluții adecvate de backup și recuperare*. Pe baza cerințelor organizației trebuie de identificat o soluție de backup adecvată ca parte a strategiei de backup. Iată câteva aspecte de luat în considerare la identificarea soluției de backup și recuperare:
   - tipurile de backup: backup complet, backup diferențial (în care sunt copiate numai adăugările/modificările) și backup incremental (în care se modifică diferența de la cel mai recent backup incremental);
   - unde se va păstra backup-ul: backup fizic/local (în care datele sunt copiate la fața locului utilizând un hard disk extern, o unitate USB, etc.) sau backup cloud/remote (unde datele sunt salvate în afara locației într-un mediu de stocare cloud);
   - caracteristici necesare organizației: ușurința de realizare a backup-ului (opțiuni automatizate și/sau la cerere), restabilirea flexibilității (între utilizatori, bazat pe căutare, punctual), scalabilitatea (gestionarea licențelor și utilizatorilor), ușurința de utilizare (o interfață utilizator intuitivă și recuperarea self-service), experiența după cumpărare (asistența gratuită și spațiu de stocare nelimitat), recomandări solide (evaluări pozitive ale clienților, certificări de securitate și conformitate).
4. *Testarea și monitorizarea sistemului.* Odată ce sistemul backup este instalat, el trebuie testat, atât pentru a verifica dacă atât backup-ul, cât și restaurarea au fost realizate cu

succes. Trebuie de verificat backup-ul și restaurarea referitor la diferite tipuri de artefacte – conturi, e-mailuri, documente, site-uri etc. Dacă soluția de backup acceptă backup-ul utilizatorului final – este necesar de a informa și educa utilizatorii despre modul de folosire a acestuia. La fel este important să fie monitorizată performanța copierii de rezervă și să fie verificate în mod regulat jurnalele referitor la pierderea de date.

Aici trebuie de mai menționat regula frecvent menționată când vine vorba de backup-ul datelor, și anume strategia (sau regula) 3-2-1, care este utilizată ca protocol de bază și la care se mai adaugă alte caracteristici pentru a se asigura un nivel optim de securitate. Această regulă include:

- asigurarea că avem 3 copii ale datelor;
- stocarea copiilor pe 2 dispozitive separate;
- păstrarea unei copii într-o locație la distanță.

În ultimul timp devine actuală și versiunea 3-2-2 a acestei reguli, în care ultimul punct se completează cu 2 copii în loc de una, păstrate în locații diferite – una pe un server sau hard drive și alta în cloud. Această strategie ar trebui să ne protejeze împotriva erorilor software și hardware, hackerilor ransomware și a virușilor. Mai mult, această regulă ne poate proteja datele și în fața oricăror dezastre naturale.

Pentru a realiza o strategie fiabilă de recuperare în caz de dezastru subliniem (cu riscul de a ne repeta) câteva dintre aspecte prioritare ale celor mai bune practici în dezvoltarea acesteia:

costul - vom avea nevoie de un plan de backup a datelor pe care ni-l putem permite, pentru aceasta trebuie să analizăm cheltuielile potențiale ale unei încălcări sau pierderi, apoi, să cântărim acest lucru în raport cu costul proiectat al sistemului nostru de backup;

locul de stocare a copiilor de date - unele companii preferă backup-ul bazat pe cloud, altora le place să aibă o copie de rezervă fizică; cele mai prudente companii folosesc mai multe surse de rezervă, în acest fel, dacă o copie de rezervă eșuează, compania are o altă copie la dispoziție;

stabilirea riscurilor cu care ne putem confrunta referitor de date - fiecare companie trebuie să se gândească la riscurile provocate de malware și eventualele atacuri de phishing; cu toate acestea, este posibil ca acestea să nu fie singurele riscuri cu care compania se poate confrunta, spre exemplu o companie dintr-o zonă predispusă la inundații trebuie să ia în considerare daunele cauzate de apă; ar fi înțelept de asemenea să existe o soluție pentru backup și recuperare a datelor situată în afara locației companiei;

periodicitatea copierii de rezervă a datelor - unele companii generează date foarte frecvent, în astfel de cazuri, o copie de rezervă zilnică poate să nu fie suficientă, și este posibil să fie nevoie de un orar special pentru copiile de rezervă; pentru alte companii ale căror date sunt rar actualizate, o copie de rezervă o dată pe săptămână poate fi suficientă;

persoanele responsabile pentru planificarea backup-ului - instruirea angajaților este esențială pentru o strategie eficientă de backup. Este necesar ca în companie să exise personal cu cunoștințe solide în domeniu, pe care să ne putem baza la implementarea strategiei de backup și recuperare.

CONCLUZII

Continuitatea afacerii este „capacitatea strategică și tactică a organizației de a planifica și răspunde la incidente și perturbări ale afacerii pentru a continua operațiunile comerciale la un nivel predefinit acceptabil” [7], în timp ce recuperarea în caz de dezastru constă din „procesul, politicile și procedurile legate de pregătirea pentru recuperarea sau

continuarea infrastructurii tehnologice esențiale pentru o organizație după un dezastru natural sau indus de om".

După cum putem vedea din aceste definiții, accentul în recuperarea în caz de dezastru este pus pe tehnologie, în timp ce în continuitatea afacerii - este pus pe operațiuni de afaceri. Prin urmare, recuperarea în caz de dezastru face parte din continuitatea afacerii și am putea să o considerăm ca unul dintre principalii factori ai operațiunilor de afaceri sau ca parte tehnologică a continuității afacerii.

În fianl, cea mai importantă parte a evitarii intreruperii afacerii în cazul unui dezastru este planificarea timpurie. Prin stabilirea unor strategii fiabile de continuitate a afacerii și a recuperării în caz de dezastru, compania poate fi pregatită pentru o recuperare rapidă și eficientă, în cazul în care se declanșează un dezastru. Aceste strategii trebuie să includă obligator teste periodice pentru fi asigurați că planul se actualizează și pentru a putea evidenția eventualele vulnerabilități. Compania trebuie să fie pregatită să facă schimbări și să ofere instruire și resurse angajaților acolo unde este necesar, astfel încât în orice moment să fie sigură că planurile ei funcționează.

Indiferent de mărimea afacerii sau de experiența pe piata, toate organizatiile ar trebui să implementeze un plan de continuitate a afacerii și de recuperare în caz de dezastru și să le utilizeze împreună, pentru a asigura cea mai mare protecție împotriva întreruperii activității.

BIBLIOGRAFIE

1. IBM Security. *Cost of a Data Breach Report 2020*. Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/.
2. SM ISO/CEI 27031:2013. *Information technology. Security techniques. Guidelines for information and communication technology readiness for business continuity.*
3. SM EN ISO 22301:2020. *Security and resilience. Business continuity management systems. Requirements*.
4. *2020 Disaster Recovery Statistics That Will Shock Business Owners*. Available at: https://phoenixnap.com/blog/disaster-recovery-statisticss.
5. SM EN ISO/IEC 27001:2017. *Tehnologia informaţiei. Tehnici de securitate. Sisteme de management al securităţii informaţiei. Cerinţe*.
6. Mcdermott, M. *Forming a Backup Strategy: 4 Steps to Follow*. Available at: https://spanning.com/blog/backup-strategy-4-steps-to-follow/.
7. BS 25999-2:2007. *Business continuity management. Specification*.
8. SM EN ISO/IEC 27002:2017. *Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei.*

GENERAL INFORMATION ON THE IMPERATIVE, EVOLUTION AND CONCORDANCE OF THE MEANS AND METHODS OF PROTECTING ECONOMIC INFORMATION AND INFORMATION RESOURCES

GENERALITĂȚI PRIVIND IMPERATIVUL, EVOLUȚIA ȘI CONCORDANȚA MIJLOACELOR ȘI METODELOR DE PROTEJARE A RESURSELOR INFORMAȚIONALE ȘI INFORMATICE ECONOMICE

Leahu Tudor
Doctor în științe economice, conferențiar universitar
Universitatea Liberă Internațională din Moldova
e-mail: leahu.ts@mail.ru

Abstract
The imperative factors are elucidated, characterized the circumstances and environments of current and future economic information and informatics systems, which objectively contributed to the urgent need for invention, elaboration and using of various means and methods of protection of information resources. The functional value of the field in question in the market economy environment and in integrated informatics systems is emphasized. The content of the material is structured and rendered from the positions of the unitary process of economic management, which performs not only information, but also and the materials activities, in interconnection and direct interaction in real time. Its subdivisions are also specified and in this basis - determined the field of application of the above-mentioned means and methods in the existing conditions of processing the informational values of economic content.
In this context, the subdivisions of the previously nominated process, its constituents, are systematized and analyzed. The general scheme of the interconnection and interaction between the parameters of protection and efficiency of the functioning of economic integrated informatics systems is established and elaborated. Depending on the application environments, the categories of protection of information units, physically made in the form of data elements, on manual and informatics storage media are highlighted. At the same time, in terms of mutual influence with information resources, some aspects of the protection of other informatics resources are elucidated. Tangentially, the terminology is examined and the concordance of the means and methods of organizing and carrying the data protection processes is performed. The problems of this department of economic informatics and the possible ways to solve them are formulated.

Keywords: *categories, concordance, data protection means and methods, explanation terminology, imperative factors, integrated economic informatics systems, problems, systematization, ways to solve*

JEL Classification: *C55, D85, E47, L63, L86*

INTRODUCERE

Anticipat oricăror activități de cercetări sau de asigurare a evoluției lor în direcția anterior bine determinată, obiectiv se impune formularea, cunoașterea și aplicarea exactă a anumitor termeni specifici pentru domeniul concret al utilizării lor. Neglijarea acestei teze face imposibile inițierea, elaborarea, implementarea și funcționarea cotidiană a obiectului (procesului) gestionat.

În acest sens, și procesele de protejare a resurselor informatice au solicitat și permanent au înaintat cerințe tot mai stringente față de realizarea procedurilor, operațiunilor de prelucrare și păstrare a componenței, structurii și conținutului (valorilor) unităților de resurse anterior nominalizate. De constatat faptul că pentru a satisface și respecta aceste exigențe primordial apare necesitatea în formarea anumitei terminologii concordante cu compoziția, configurația și logica evoluției ariei de aplicare. De aceea, pornind de la complexitatea componenței resurselor, se cer elaborate și aplicate noțiuni referitoare la toată sfera de preocupări informatice, sector, sub-sector, compartiment,

resursă şi componentă constituantă a lor. În conformitate cu astfel de deziderat, pot fi evidenţiaţi termeni de ordin general, intermediar şi particular.

În contextul celor expuse până aici, raportat la protecţia sistemelor informaţionale şi informatice economice, se observă un număr relativ sporit de termeni, uneori cu conţinut contradictoriu, fără orientare spre mediul real ce a provocat formularea şi întrebuinţarea lor. Din motivul dat, atât pentru teoria, cât şi pentru practica elaborării şi funcţionării sistemelor în cauză, de importanţa deosebită dispune clarificarea esenţei şi conţinutului funcţional al unor termeni de bază referitor la acest domeniu.

CONŢINUTUL CERCETĂRII

În sursele bibliografice [1-4] şi activităţile practice de asigurare a protecţiei datelor cele mai frecvent utilizate sunt noţiunile „fiabilitate", „securitate", „protecţie", „confidenţialitate", „integritate", „risc (pericol)". Deşi fiecare din ele dispun de un anumit grad de sinonimitate, nu toate pot ft utilizate în măsură egală pentru un element ori altul al sistemului informaţional (informatic). Aşa, de exemplu, „securitatea" se interpretează drept minimalizare a vulnerabilităţii elementelor sistemului, iar „pericolul" - drept încălcare potenţiala a securităţii. Odată cu majorarea performanţei sistemelor de procesare a datelor, devine tot mai evidenta valoarea pericolelor neintenţionate şi intenţionate.

Cea mai vastă se considera noţiunea de „protecţie", care se referă la orice resursă a sistemului informatic. De aceea, privind resursele informaţionale, ea include în sine asigurarea confidenţialităţii datelor, protejarea informaţiei de modificări şi falsificări, de lichidare (ştergere) a ei şi excluderea „acaparării" resurselor sistemului cu stăpânirea lor monopolistă „Protecţia informaţională" se referă la tot sistemul de organizare, transformare şi utilizare a datelor şi la fiecare componentă (resursă, activitate) a lui în particular. De aceea în fiecare caz aparte ea se determină divers, în dependenţă de obiectele şi acţiunile, pentru care ea trebuie să fie asigurată.

De asemenea, „protecţia informaţională" include o totalitate de acţiuni, metode şi mijloace ce asigură soluţionarea a aşa probleme principale ca verificarea integrităţii informaţiilor; excluderea accesului neautorizat la resursele calculatoarelor, la programele şi datele informaţionale, excluderea utilizării neautorizate a programelor (protecţie de copiere a programelor).

Fiabilitatea caracterizează gradul de siguranţă a unui sistem ori componentă a lui în conformitate cu scopul conceput şi realizat; capacitatea funcţionării lui timp cât mai îndelungat. De aceea, noţiunea se referă mai mult la partea fizică (materială) a sistemului, măcar că la nivel general ea poate fi utilizată şi în sens de trăinicie, temeinicie, siguranţă şi chiar securitate a oricărui element al sistemului.

În acelaşi timp, „confidenţialitatea" are atribuţie mai cu seamă la sensul conţinutului resurselor informaţionale şi constă în asigurarea nedestăinuirii conţinutului, componenţei, numărului, structurilor şi valorilor unităţilor informaţionale.

De asemenea, şi „integritatea" ca termen se referă preponderent la partea informaţională a sistemului. Din acest motiv esenţa ei se reduce la asigurarea deplinătăţii şi exactităţii valorilor datelor prin excluderea modificării lor ocazionale sau intenţionate, anularea lor prin ştergere.

După cum a fost afirmat anterior, protecţia se raportează la orice resursă a sistemelor informatice şi de aceea termenul se consideră de cel mai general nivel, din ce cauză este justificată includerea parametrilor ce contribuie la realizarea ei. În aşa aspect, în dependenţă de categoria resurselor şi scopul protejării lor, termenul elucidat înglobează noţiunile de fiabilitate şi securitate. Deci, prin intermediul asigurării unui anumit grad de fiabilitate şi securitate, se atinge o anumită eficacitate a funcţionării sistemului. În această

bază, interconexiunea și concordanța dintre noțiunile parametrilor elucidați ai sistemelor nominalizate schematic poate fi prezentată prin interrnediul figurii 1.

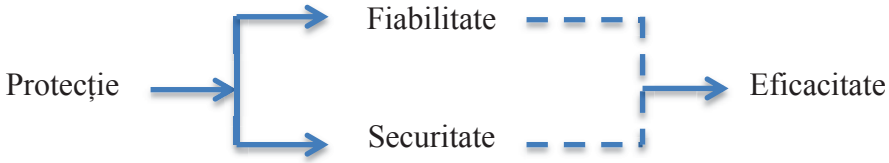


Figura 1. Schema interconexiunii și concordanței termenilor parametrilor protecției și eficacității funcționării sistemelor informatice economice (S.Ic.E.)

De menţionat că fiabilitatea se referă, mai cu seamă, la funcţionarea resurselor S.I$_c$.E., pe când securitatea are atribuţie preponderent la existenţa („păstrarea") lor. Prin urmare, prima asigură funcţionalitatea resurselor tehnice şi tehnologice, iar cea secundă - accesul şi confidenţialitatea celorlalte resurse. Însă, orice nu s-ar efectua în acest domeniu totul este orientat spre un singur scop - asigurarea calităţii resurselor informaţionale, ceea ce şi caracterizează integral eficienţa S.I$_c$.E. Sunt cunoscute aşa date că în S.U.A. (conform afirmării şi datelor companiei C.N.N.) valoarea pierderilor de la încălcările securităţii şi neasigurării fiabilităţii S.Ic.E. au atins cifre de zeci de miliarde de dolari [1, pp.311-312; 3, pp.33-35] .

Important este şi faptul că pentru economia de piaţă este caracteristică aplicarea cât mai frecventă a principiului selectiv de aplicare a resurselor informaţionale în activităţile de gestiune. El se reduce la acel concept că varietatea selectării se găseşte în dependenţă directă de complexitatea, componenţa şi plenitudinea conţinutului acestor resurse. De aceea cu cât mai variate şi mai voluminoase sunt informaţiile păstrate pe mediul fizic memorar al mijloacelor tehnice informatice, cu atât mai operativă şi mai aleatoare este selecţia lor în orice moment oportun.

În aşa context actualmente se constată noian de informaţii economice, ceea ce fără conştientizarea necesităţii formării şi afişării nu numai a celor rezultative, dar şi a celor iniţiale, de asemenea, complică şi acutizează problemele protecţiei şi eficienţei S.I$_c$.E.

SPECIFICUL FUNCȚIONĂRII DOMENIULUI EXISTENT DE APLICARE – IMPERIOZITATE DE PROTEJARE

Situația creată la moment și premisele evoluției posibile a managementului economic tot mai impunător confirmă faptul necesității transformării lui treptate, ca unitate organizatorică, într-un nucleu material – informațional de acțiune analoagă automată. În astfel de circumstanțe nu este exclusă influența decisivă nemijlocită și temporar imediată a activităților materiale și spirituale umane de starea proceselor informaționale.. Ca urmare a formării acestei conjuncturi, protecția unităților informaționale, operațiunilor și procedurilor de manipulare cu ele va dispune de valoare gestională extremă, deoarece "alterarea" lor prompt se va răsfrânge asupra activităților în cauză. Din motivul dat, abordarea sistemică și tratarea integrată vor deveni iminente pentru orice teren managerial economic, indiferent de dimensiunile razelor spațiale și temporale existențiale și evoluționiste ale lui.

În acest context preliminar apare necesitatea stringentă în analiza nivelului integrării sistemului actual de gestiune economică și implicit a sub-sistemului lui informațional. Ambele se caracterizează prin izolare spațială și evoluția discretă a proceselor materiale și informaționale, care virtual și în interpretare analogică formează un tot întreg. De aici - : multiplele discordanțe dintre activitățile acestor două categorii de procese, fărâmițarea sistemului managerial pe nivele (organisme) de gestiune (primare,

intermediare, superioare), perioade de funcționare (operative, curente, de pronostic) și a sistemului informațional pe subsisteme, complexe de probleme și probleme particulare.

Astfel de situație a condus la efecte cât mai expresive, mai cu seamă, la nivelele intermediare și superioare de gestiune, a rolului influențabil al subiectului asupra evenimentelor materiale și spirituale atât a societății umane în ansamblu, cât și a fiecărei subdiviziuni, individ al ei. S-au creat condiții de favorizare a înrăuririi precumpănitor negative tendențioase a sistemului managerial asupra obiectului (procesului) condus, precum și la predominarea metodelor și mijloacelor administrative aplicate practic în orice spațiu și moment de gestiune. De pe poziții unitare, toate aceste momente, cu prevalență, sunt provocate de necorespunderea nivelului de performanță a sub-sistemului managerial comparativ cu sub-sistemul condus de el. Formarea rupturii menționate s-a produs odată cu instituirea caracterului social al activităților materiale umane, ea fiind consecința penuriei accentuate de informații calitative.

Analiza desfășurării cursului acestor două constituente ale procesului unitar de gestiune economică scoate în transparență mersul obiectiv spre lichidarea izolării teritoriale și funcționării discrete a lor. În prezent și de la începutul socializării activităților subiectului așa înaintare se observă și este realizată prin inventarea, elaborarea și aplicarea diverselor mijloace tehnice, programate, metode tehnologice, etc., considerate drept resurse informatice. Trasând o paralelă între progresul dezvoltării resurselor elucidate, devine sesizabil faptul că cele enumerate anterior au avansat esențial, pe când, din punct de vedere a cuprinderii totale a fenomenului informațional ca unitate integrală, aplicarea lor în domeniile informativ și decizional economice este insuficientă. În sensul dat, se atestă o acoperire satisfăcătoare de către mijloacele și metodele informatice numai a unei etape transformative a informațiilor – a etapei de prelucrare (informațională, structurală, de calcul), celelalte două etape – inițială și de utilizare rămânând efectuate preponderent în mod manual de subiect. În rezultat, s-a format o discordanță substanțială dintre nivelele performanței metodelor și mijloacelor informatice și domeniul aplicării lor. Așa situație poate fi calificată drept nepregătire a resurselor informaționale pentru implicarea resurselor nominalizate în procesarea lor.

Circumstanțele create sunt provocate de extinderea spațială și vitezele inimaginabile de realizare a preocupărilor materiale umane. Despre aceasta mărturisește formularea evolutivă a concepției globalizării activităților în cauză, obiectiv fiind împinși de imperativul integrării material – informaționale. Altfel afirmând, globalizarea materială a provocat și nu poate fi realizată și funcționa fără globalizarea informațională.

De menționat că în prezent și permanent, în procesarea datelor pe bună dreptate și justificat se consideră decisive resursele informatice, enumerate mai sus. Însă, nu mai puțin valoroasă pentru această modalitate este și adecvarea structurării și organizării resurselor informaționale, interconexiunilor procesuale și funcționale ale lor. Prin realizarea consecutivă a acestor două categorii de interconexiuni se asigură continuitatea tuturor proceselor informaționale. În cazul, în care continuitatea este susținută de mijloace și metode tehnice, ea este automată. Prin urmare, nu numai factorii informatici, dar și însăși domeniul – resursele informaționale, prin interconexiunile sale structurale raționale, de organizare și prelucrare eficientă, contribuie direct la procesarea mașinală a lor. De aceea, de importanță decisivă în spriginirea funcționării automate a sistemului integrat de management economic dispun identificarea, respectarea, punerea în funcțiune și garantarea funcționării tehnice a interconectărilor de orice varietate în cadrul sistemului.

Din cele elucidate până aici, din punct de vedere științific și proiectant, rezumă justificarea imperativului elaborării concepției unitare de creare și asigurare a funcționarii fiabile și eficiente a unui sistem informatic, care ar integra într-un tot indivizibil resursele

și procesele (materiale + informaționale) apartenente lui. Așa sistem se solicită să fie nu numai unitar în plan compozițional și structural, dar și totalmente interconectat și procesual integrat.

Pornind de la considerentele menționate, concepția sistemului informatic integrat rezidă în cuprinderea cu procese informatice nu numai a activităților informaționale, dar și materiale în interconexiune și interacțiune nemijlocită. Unitatea acestui sistem se referă atât la organizarea, cât și structurarea și funcționarea tuturor elementelor constitutive ale lui de pe poziții unitare.

Astfel de abordare impune efectuarea elaborării, implementării și asigurarea evoluției lui cotidiene prin stabilirea și realizarea tuturor constituantelor, interconectărilor și interacțiunilor dintre ele, indiferent de razele teritoriale și temporale în baza principiului motivației, conform căruia materia cauzează informația, ultima fiind de predestinație informativă și decizională.

Pe lângă cele menționate mai sus, odată cu determinarea exactă și deplină a caracteristicilor menționate, respectarea întocmai și realizarea lor prin intermediul factorului informatic, se creează condiții de constituire a unui sistem de mansagement economic de acțiune analoagă, adică, automata și nu automatizată, ceea ce este propriu pentru asemenea sisteme în present. În așa situație sistemul va funcționa conform schemei din figura 2 [4, pp.251-253].

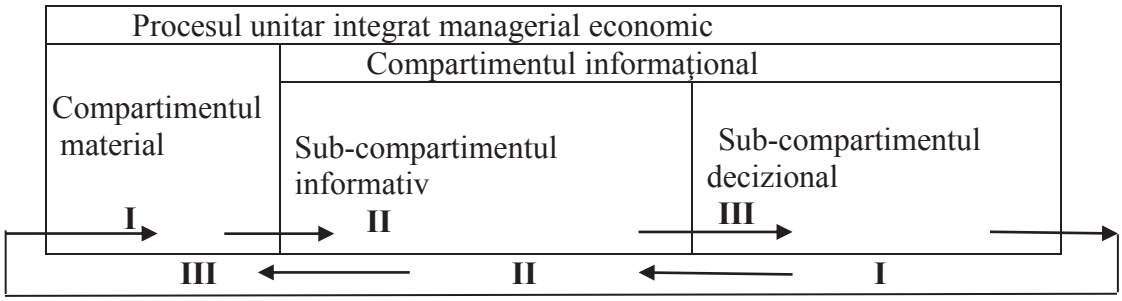


Figura 2. Schema conceptuală de funcționare a procesului unitar integrat de gestiune economică

Schema concepției succesiunii interconexiunii și interacțiunii compartimentelor și sub-compartimentelor procesului unitar integrat economic din figura 2 este bazată pe principiul motivației și pentru varianta inițierii evoluției lui. În cazul, în care procesul deja funcționează, astfel de ordine se inversează, adică deciziile formulate afectează procesele materiale, ultimele – procesele informative, iar ultimele – formularea repetată exactă, luarea autentică și realizarea eficientă a proceselor materiale, conform noilor valori decizionale, etc. până la încetarea funcționării acestui proces. După cum se vede, în ambele situații, în cadrul acestui ciclu material-informațional unitar, randamentul compartimentului **I și c**alitatea produselor sub-compartimentului **III** (varianta I → II → III) decisiv depind de nivelul autenticității produselor sub-compartimentului **II,** ceea ce și fondează imperativul asigurării unei protecții cât mai fiabile a lui.

De avut în ve4dere și acea circumstanță, conform căreia formarea (apariția) unei activități sau a unui complex de activități noi este motivată atât de rezultatele anumitor experimente (practici) impuse, cât și de consecințele evoluției proceselor. În acest sens, în prezent evoluția sistemelor informatice economice (S.I$_c$.E.) a condus la apariția și acumularea multiplelor și tot mai variatelor și voluminoaselor probleme ce necesită soluționare cotidiană, eforturi și resurse semnificative. Printre ele de prim ordin de valorificare și conceptual se consideră cele ce asigură gradul necesar de fiabilitate,

securitate şi eficacitate a acestor sisteme. Preponderent, practica funcţionării lor treptat a solicitat domeniului ciberneticii şi informaticii economice formarea anumitor ramuri de cunoştinţe teoretice şi deprinderi practice privind efectuarea activităţilor nominalizate (fiabilitate, securitate, eficacitate) [4, pp.205-208].

Aşa cum procesele economice materiale şi informaţionale se realizează spaţial şi temporal, există necesitatea coordonării lor în cadrul acestor raze. Din motivul dat, orice acţiuni şi activităţi ce se referă la ele solicită abordare sistemică de ordin ştiinţific. Pe lângă cele menţionate, e necesar de avut în vedere faptul că S.Ic.E. este o unitate destul de complexă, fiind compusă din diverse resurse, din care de bază sunt cele tehnice, informaţionale, matematice, programate, tehnologice, economice, socio-juridice, ş.a.

Aşa specific esenţial obiectiv a condus la luarea în considerare a interconexiunilor şi interacţiunilor dintre aceste componente în aşa mod ca sistemul în cauză să funcţioneze cât mai eficient, obţinând cele mai calitative produse informaţionale informative cu cele mai reduse consumuri.

Importanţa protecţiei datelor este, de asemenea, motivată şi de particularităţile mediului economiei de piaţă, care amplifică valoarea funcţională a asigurării acestor parametri calitativi ai S.Ic.E. E cunoscută situaţia că în acest mediu practic este nelimitată solicitarea informaţională a oricărui obiect ori activitate, ceea ce permanent sporeşte volumul şi complică componenţa resurselor informaţionale. Drept urmare se solicită atenţie deosebită protecţiei celor din urmă, care, la rândul sau, se realizează prin intermediul fiabilităţii şi securităţii tuturor celorlalte resurse (tehnice, programate, tehnologice, economice, socio-juridice), ultimele contribuind la eficacitatea generală a funcţionării S.Ic.E. în ansamblu.

EVOLUŢIA, FACTORII ŞI PROBLEMELE ASIGURĂRII PROTEJĂRII RESURSELOR INFORMAŢIONALE ŞI INFORMATICE ECONOMICE

Pe măsura evoluţiei practicii funcţionării S.I$_c$.E. tot mai insistent se solicită specializarea evidentă a serviciilor informatice sub formă de anumite subdiviziuni organizatorice în cadrul unităţilor economice, rareori fiind realizate sub formă de servicii de protecţie a datelor preponderent în sectoarele bancar, statal, afacerilor interne.

După cum se ştie, sistemele informaţionale economice se caracterizează prin volume considerabile, componenţă compusă şi repartizare spaţială extinsă a elementelor sale. Din acest motiv există necesitatea de a asigura o anumită concordanţă dintre diverse nivele şi compartimente ale lor în aşa mod ca obiectele şi procesele economice deservite de ele să dispună de evoluţie prosperă continuă.

În contextul dat conexiunea informaţională contribuie la integrarea activităţilor economice. sub formă de sistem unitar de efectuare a lor, ceea ce în realitate şi e necesar să se producă.

La începuturi, când producerea, distribuirea şi consumarea bunurilor materiale şi spirituale erau de caracter particular şi practic nu se realizau în anumite perioade de timp îndelungate şi pe scară spaţială extinsă, şi informaţiile respective privind aceste activităţi, de regulă, erau „dobândite”, memorizate, prelucrate şi utilizate de un individ sau de un grup redus de indivizi (gospodărie individuală) în mod oral şi în termene operative (pe parcursul activităţilor economice, într-o zi ori câteva zile), fără a implica în aceste procese anumite suporturi şi mijloace auxiliare speciale.

Pe măsura extinderii razei manifestării economice materiale umane tot mai pronunţat devine caracterul social al informaţiei în cauză, iar procesele informaţionale necesită organizarea şi efectuarea lor în mod conştient. De aceea, dacă la faza iniţială a activităţilor materiale economice umane fluxurile informaţionale spaţial se formau şi se

realizau acolo, unde şi cele materiale, apoi treptat, în mod evolutiv, ele tot mai esenţial şi-au majorat atât termenele, cât şi scara de acţiune.

În aşa circumstanţe funcţionarea eficientă a sistemului informaţional economic este bazată nu numai pe concordanţa spaţială şi temporală a proceselor informaţionale, dar în măsură egală şi pe asigurarea protecţiei valorilor unităţilor informaţionale funcţionale. Aceasta din urmă îşi găseşte explicarea în faptul, că odată cu integrarea activităţilor materiale economice în parametrii nominalizaţi, automat se produce şi integrarea fluxurilor informaţionale, ce le însoţesc. În consecinţa fenomenului produs e suficient ca o singură valoare a unităţii informaţionale să fie „alterată", sau pierdută şi sistemul informaţional în ansamblu poate să nu corespundă solicitărilor sistemului de gestiune concret, aşa cum unitatea informaţională respectivă dispune de mulţime de conexiuni cu o mulţime de alte aşa unităţi şi „pierderea" („alterarea") ei, firește, influenţează negativ sistemul informaţional integral. De aceea conceptul organizării resurselor informaţionale sub formă de fişiere separate nu accentuează în mod evident valoarea protecţiei datelor, aşa cum neasigurarea ei se referă la fiecare fişier în parte şi nu afectează tot sistemul informaţional în întregime sau o bună parte a lui.

Totodată, organizarea integrată a datelor înaintează probleme stringente privind securitatea lor din cauza că realizarea ei este condiţionată de conexiunile informaţionale dintre problemele soluţionate. În aşa condiţii „deteriorarea" unei unităţi de date poate să se răsfrângă asupra calităţii sistemului informaţional în ansamblu.

Aşadar, integrarea datelor în procesele de organizare şi transformare obiectiv acutizează necesitatea asigurării stricte a protejării tor. Pornind de la acest considerent, sporirea importanţei activităţilor de protecţie a datelor este condiţionată şi de următorii factori de bază:

1) evoluţia conceptului de organizare a datelor odată cu trecerea de la fişiere separate la baza informaţională unitară integrată, ce deserveşte tot obiectul economic şi fiecare subdiviziune, participant (activitate) şi resursă ale lui;
2) coordonarea şi reglarea proceselor informaţionale economice în spaţiu şi timp;
3) sporirea continuă a numărului şi volumelor unităţilor informaţionale funcţionale;
4) majorarea complexităţii structurale a acestor unităţi;
5) complexitatea varietăţii compoziţionale a unităţilor în cauză;
6) complicarea efectuării proceselor de organizare, transformare şi utilizare a valorilor unităţilor informaţionale în cadrul sistemului de gestiune a unităţii economice.

La rândul său, aceşti factori contributivi la protecţia datelor au condus la necesitatea:

1) evidenţierii, ordonării şi integrării funcţionale a unitaţilor structurale informaţionale, condiţionate de interconexiunea informaţională a problemelor soluţionate şi de utilizarea cât mai economă a spaţiului memorar al sistemului informatic;
2) scoaterii în vileag, sistematizării şi integrării structurale a unităţilor informaţionale cu scopul unificării structurii lor;
3) profilării, clasificării şi integrării procedurilor informaţionale, de prelucrare şi de utilizare a unităţilor structurale de date pentru a exclude dublarea şi iterativitatea lor nejustificată;

În prezent utilizatorii sistemelor informatice economice în mare măsură sunt conştienţi de actualitatea şi necesitatea stringentă a asigurării protecţiei informaţiilor de a fi accesate şi utilizate în mod neautorizat. Însă, deşi se dispune de număr considerabil de publicaţii, anumită experienţă în acest domeniu şi interes major faţă de tematica dată, rămân nesoluţionate următoarele probleme principale:

1) elaborarea unui mod unitar de abordări privind determinarea scopurilor de asigurare a protecţiei informaţionale a sistemului informatic (informaţional) economic;

2) interpretarea neunivocă a terminologiei;

3) elaborarea modului unitar de abordare a clasificării factorilor de influenţă asupra securităţii informaţionale cu evidenţierea şi sistematizarea riscurilor (pericolelor) intenţionate şi potenţiale;

4) compunerea şi respectarea riguroasă a modalităţii unitare de abordare a conceptului de protecţte a sistemului informaţional în ansamblu şi a componentelor lui în particular;

5) elaborarea modului unitar de abordare a evaluării (estimării) protecţiei resurselor sistemului informaţional;

6) întocmirea metodologiei unitare ştiinţifice şi variatelor metodici de realizare a ei în ceea ce privește determinarea dimensiunii pierderilor din cauza abuzurilor programatice;

7) elaborarea unui sistem unitar de criterii (indicatori) de determinare a dimensiunilor riscului şi eficienţei sistemului de securitate informaţională [4, pp.207-210].

ANALIZA MEDIILOR, MIJLOACELOR ŞI METODELOR DE PROTEJARE A RESURSELOR INFORMATICE

Protejarea datelor se efectuează divers în funcţie de mediul formării şi transformării lor. Se evidenţiază două medii de aşa natură – sistemul informaţional şi sistemul informatic. Primul include toate informaţiile ce sunt organizate, prelucrate şi utilizate conform cerinţelor şi în cadrul sistemului de gestiune concret în ansamblu, atât în baza metodelor manuale, cât şi a celor automate. De reamintit că sistemul informatic este nu altceva decât sistemul informaţional realizat prin intermediul mijloacelor tehnice. De atenţionat, de asemenea, că în economie până în prezent încă nu s-a reuşit ca sistemul informaţional să fie realizat pe deplin în mod automat.

În dependenţă de aceste două medii au fost inventate, elaborate şi aplicate diverse mijloace şi metode de protecţie a datelor caracteristice pentru fiecare din ele, ce pe parcurs au evoluat. Varietăţile lor sunt predeterminate de tipurile de suporturi, pe care se înregistrează în mod diferit informaţia. În aşa caz se observă două grupe de mijloace şi metode de securitate a datelor, una referindu-se la documente, iar alta - la suporturile informatice (tehnice). Primele se consideră manuale, iar cele secunde - preponderent automate. La rândul său, mijloacele şi metodele manuale sunt de caracter fizic, aşa cum ele depind de proprietăţile şi de „posibilităţile” fizice ale acestei categorii de suporturi (documente) de a proteja informaţia. Ele se elaborează şi se implementează în sistemele informaţionale bazate pe organizarea şi transformarea informaţiei în mod manual integral sau parţial.

Mijloacele şi metodele de protecţie a datelor caracteristice pentru suporturi tehnice (informatice) sunt atât de categorie fizică, cât şi programatică. În cadrul ambelor grupe de aşa mijloace şi metode (manuale şi informatice), de asemenea, pot fi realizate diverse procedee organizatorice de securitate a datelor. Metodele fizice sunt condiţionate nu numai de particularităţile fizice ale suporturilor, dar şi a dispozitivelor mijloacelor tehnice, a tehnologiilor informaţionale şi informatice. În acest sens se poate presupune că odată cu performanţa construcţiei elementelor constructive şi „duritatea” fizică a mijloacelor tehnice, ponderea şi valoarea mijloacelor programatice de securitate a datelor, posibil, vor scădea.

În general raportul dintre mijloacele şi metodele fizice şi cele organizatorice depinde de calitatea şi performanţa celor dintâi şi valoarea sociala a informaţiilor. Cu cât

primele sunt mai imperfecte cu atât componenţa metodelor organizatorice este mai variată, concomitent cu performanţa lor continuă.

Afară de cele menţionate, e necesar de atenţionat asupra faptului că, fiind inventată şi utilizată de subiect, informaţia economică se consideră produs artificial şi cu acest prilej aspectul subiectiv al mijloacelor şi metodelor de formare şi protejare a ei este decisiv. Din motivul dat asigurarea protecţiei acestei informaţii depinde nu numai de performanţa metodelor şi mijloacelor, dar şi de valoarea şi caracterul ei social. De aceea, cu cât valoarea funcţională şi socială a informaţiilor economice este în ascensiune, ce este firesc şi continuu pentru ea, cu atât mai complicate şi mai variate sunt tentativele de a o „altera" şi a o „lichida" ca produs de importanţă primordială în societatea umană. În contrariu acestor tentative se dezvoltă mijloacele şi metodele de protecţie a datelor.

După cum s-a stabilit anterior, metodele şi mijloacele de asigurare a protejării datelor în sistemul informaţional sunt de caracter manual şi limitate de proprietăţile unui singur tip de suporturi - documentul. Din acest motiv preponderent ele sunt de ordin fizic şi se realizează în mod organizatoric. Unele din ele se referă la protecţia sistemului informaţional în ansamblu (localurile, mijloacele auxiliare, mobilă specială şi alte echipamente de păstrare, organizare şi manipulare a documentelor), iar altele - la protecţia conţinutului funcţional al acestui sistem (diverse cartoteci, mape, dulapuri şi stelaje de păstrare a documentelor). De regulă, documentele completate sunt organizate în pachete după termenele de formare (perfectare) a lor (o zi, cinci zile, decadă, lună, trimestru, semestru, an, etc.) şi pe obiecte şi activităţi (de exemplu, documente pe intrările valorilor materiale, ieşirile lor, ori pe îndeplinirea anumitor volume de lucrări etc.). Protecţia conţinutului informational al documentaţiei elaborate este asigurată de semnăturile persoanelor responsabile de deplinătatea şi autenticitatea valorilor datelor înregistrate.

Accesul la informaţii este protejat prin intermediul diverselor documente reglementative (regulamente, acte normative, juridice, administrative, instrucţiuni de serviciu ş.a.) a activităţilor informaţionale, a obligaţiunilor funcţionale ale utilizatorilor, etc.

În aşa mod, afară de mijloacele si metodele fizice şi organizatorice, protejarea datelor este asigurată şi de metode şi mijloace juridice. Odată cu elaborarea, implementarea şi funcţionarea sistemelor informatice economice s-a schimbat şi componenţa mijloacelor şi metodelor de protecţie specifice lor. De exemplu, mijloacele tehnice de calcul trebuie să fie repartizate şi exploatate în aşa zone ale clădirilor, care ar asigura ferirea lor de diverse intenţii destructive. Locurile, unde se găsesc aceste mijloace, de asemenea, trebuie sa fie amenajate şi echipate conform cerinţelor ştiinţifice de asigurare a condiţiilor de menţinere fizica a tehnicii nominalizate în starea de funcţionare eficientă şi de excludere a posibilităţilor de a le distruge ori a le fura (uşi de fer. lacăte complicate, etc.).

De asemenea, e necesar de luat un şir de măsuri organizatorice privind excluderea accesului utilizatorilor neautorizaţi la fişiere şi programe sau a cauzelor generatoare de distrugere a lor. În acest scop se poate organiza eliberarea suporturilor (benzi, dischete, C.D.) cu fişiere numai în baza unor aprobări speciale ale persoanelor autorizate. Sălile calculatoarelor şi locurile de depozitare a fişierelor trebuie să fie protejate împotriva focului, prafului, excesului de temperatura şi umiditate, precum şi a altor cauze ce pot afecta datele păstrate.

În mediul sistemelor informatice economice pe larg este aplicată etichetarea fişierelor (internă, externă), care se consideră drept mijloc de protejare a datelor de utilizări eronate.

Protejarea fişierelor poate fi efectuată şi prin intermediul soft-ului, prin introducerea anumitor parametri (parole), care să ofere posibilitatea numai de citire sau citire şi înregistrare.

Pot fi utilizate anumite proceduri de restaurare a fişierelor de date sau de specificare a efectuării asupra lor a operaţiunilor de distrugere ori păstrare. De importanţă semnificativă dispun copiile fişierelor de date şi a resurselor programate pe suporturi păstrate în alte localuri, decât cele ale calculatoarelor.

În cazul prelucrării datelor în loturi se recomandă procedura de protecţie sub denumirea convenţională „bunic - tată – fiu" şi modificările ei. O procedura similara trebuie realizată şi în cazul, când fişierele sunt actualizate on - line. În cazul utilizării sistemelor de gestiune a bazelor de date, de administratorul bazei de date pot fi luate măsuri suplimentare prin utilizarea dicţionarelor de date şi a unor forme specifice de control confidenţial. Dacă datele sunt strict confidenţiale, se recomandă distrugerea (chiar şi prin ardere) a listelor iniţiale ori aplicarea protecţiei criptografice prin utilizarea codurilor secrete de transformare a datelor. Criptarea se recomandă pentru datele transmise prin linii de telecomunicaţii [2, 126- 135; 4, 207-210].

Protejarea datelor se asigură şi prin intermediul verificării deplinătăţii, clarităţii şi autenticităţii lor în cadrul fiecărei operaţiuni tehnologice de organizare, perfectare, păstrare şi prelucrare a lor. Controlul lor se efectuează de anumite mijloace, metode şi procedee.

La nivel de sistem informatic economic, în baza următoarelor criterii (principii) de clasificare, toate aceste metode şi mijloace pot fi sistematizate în următoarele grupe:

1) complexitatea încadrării (cuprinderii) – mijloace şi metode locale şi complexe;
2) predestinare funcţională – mijloace şi metode de anticipare (avertizare), depistare şi neutralizare a riscurilor, de restituire (recuperare) a sistemului interpretat drept unitate organizatorică de activitate;
3) natura categoriilor lor – mijloace şi metode juridice, organizatorico - administrative şi tehnico-programatice;
4) aria spaţială de acţiune - mijloace şi metode pentru zone necontrolate (externe), zone teritoriale controlate, pentru localurile funcţionării sistemului informatic, resursele lui;
5) etapele operaţionale de funcţionare a sistemului nominalizat - mijloace şi metode pentru controale la intrări, pe parcursul funcţionării (reglementării şi constrângerii redundanţei, reviziei, restituirii), la ieşiri din sistem;
6) obiectivele protecţiei - mijloace şi metode de protecţie de la acces neautorizat, de asigurare a valorii juridice, a conţinutului informaţional, de protecţie de la scurgere a informaţiei prin canalele sistemului, de protecţie de la abuzuri programatice, de la copieri neautorizate, difuzări a programelor şi informaţiilor confidenţiale computerizate;
7) caracterul opunerii - mijloace şi metode de protecţie activă şi pasivă.

Din cele enumerate, devine evident că componenţa metodelor şi mijloacelor de securitate a datelor este destul de variată şi depinde de scopurile aplicării lor, domeniile de realizare, modalităţile de efectuare ş.a. Despre conţinutul şi esenţa unora din ele se poate uşor de judecat în baza denumirilor lor. Altele, însă, necesită explicare, ultima fiind motivată şi de valoarea lor funcţională.

De pe aceste poziţii, metodele şi mijloacele de anticipare sunt predestinate pentru a crea aşa condiţii, în mediul cărora posibilitatea apariţiei şi realizării factorilor (riscurilor) de destabilizare să fie nulă sau minimă. Metodele şi mijloacele de depistare sunt orientate spre evidenţierea pericolelor apărute ori a posibilităţilor apariţiei lor şi colectarea informaţiilor suplimentare în acest sens. Metodele şi mijloacele de neutralizare contribuie

la neutralizarea pericolelor apărute, pe când cele de restituire (recuperare) - la restabilirea funcţionarii normale a sistemului informatic.

Metodele şi mijloacele tehnico-programatice de asigurare a securităţii datelor pot fi active şi pasive. Primele (cele active) sunt predestinate pentru delimitarea accesului la toate resursele sistemului informatic (tehnice, programatice, informaţionale ş.a.); transformarea datelor autentice în informaţii inutile (false) pentru infractor (acoperirea criptografică); restabilirea funcţionării normale a sistemului. Printre cele pasive de bază se consideră metodele şi mijloacele de monitoring a funcţionării sistemului informatic, de prelucrare şi analiză a datelor colectate pe parcursul monitoringului, de revizie şi audit a efectivului şi utilizării optime a resurselor sistemului, precum şi stabilirea (verificarea) integrităţii şi accesibilităţii acestor resurse.

Componenţa metodelor şi mijloacelor de securitate a datelor este condiţionată de varietăţile pericolelor ce pot avea loc în sistem. Posibilitatea realizării pericolelor depinde de locurile înguste (punctele vulnerabile) ale sistemului.

Drept pericol se consideră orice acţiune ce contribuie la dereglarea funcţionării sistemului. Se evidenţiază două tipuri de pericole de violare a securităţii datelor:

1) neintenţionate sau ocazionale;
2) acţiuni intenţionate.

Primul tip de pericole sunt de ordin extern şi intern. La cele externe se referă calamităţile naturale, factorii tehnogenici, politici, economici, sociali, extinderea tehnologiilor informaţionale şi comunicaţionale ş.a. În cadrul celor interne se includ pericolele provocate de stoparea funcţionării mijloacelor tehnice, erori în resursele programate, în activitatea personalului ş.a.

Cele mai răspândite acţiuni intenţionate de violare a securităţii resurselor sistemului informatic se consideră următoarele:

1) acces neautorizat la informaţii;
2) elaborarea resurselor programate specializate cu scopul accesului neautorizat;
3) elaborarea şi difuzarea viruşilor computeriali;
4) neglijenţă în elaborarea, susţinerea şi exploatarea resurselor programate;
5) furt de informaţii;
6) manipulare nejustificată a datelor;
7) încălcarea (nerespectarea) confidenţialităţii datelor;
8) negarea violării securităţii resurselor sistemului ş.a.

Cunoaşterea bazelor teoretice, dispunerea de anumită experienţă în activităţi de elaborare, implementare şi funcţionare a sistemelor de protejare a informaţională în economie va contribui în mod decisiv la majorarea calităţii resurselor informaţionale, ceea ce, la rândul său, va conduce la performarea sistemului de gestiune, iar ultimul - ia îmbunătăţirea rezultatelor activităţilor unităţilor materiale economice.

Actualmente de importanţă semnificativă dispune securitatea resurselor informaţionale ale reţelelor informatice – cele mai adecvate realizării automate a proceselor informative economice.

Aşa securitate este de valoare extremă pentru fiecare computer conectat la Internet, sau aflat într-o reţea de tip Intranet, Extranet şi chiar o reţea locală. Mai mult, chiar si pentru un P.C. stand-alone securitatea informaţiei poate fi o problemă serioasă, atunci, când acesta conţine informaţii personale, secrete, de anumit grad de confidenţialitate.

Prin intermediul acestei securităţi se protejează informaţiile de o paletă extinsă de pericole legate de asigurarea continuă a activităţilor, de minimizarea pagubelor şi de maximizarea recuperării investiţiilor şi a oportunităţilor de afaceri.

Indiferent, se află calculatorul în birou sau pe pupitru acasă, asigurarea securităţii informaţiilor poate dispune de aceeaşi acuitate. Evident, în cazul reţelei, asigurarea securităţii reprezintă o problemă mult mai stringentă şi, totodată, mult mai dificilă. Multe din atacurile recente de tip denial-of-service, care au pus în real pericol câteva site-uri de Web foarte populare, unele chiar guvernamentale, au reuşit să provoace situaţie de panică la autorităţile din mai multe ţări, chiar şi puternic dezvoltate. Unele voci au ajuns până la aceea că aşa pericole au devenit mult mai acute decât se credea până acum prin consecinţele sale, uneori inimaginabile.

Au existat suficiente dovezi, care susţineau poziţia acelora ce credeau că atacurile hackerilor au fost posibile din cauză că s-a reuşit obţinerea accesului doar la calculatoarele slab protejate. Cu alte cuvinte, spărgătorii de coduri au succes doar acolo, unde nu se asigură o securitate riguroasă tehnogenică.

Pericolul sabotajului prin calculator bazat pe viruşi, care pot face distrugeri extraordinare, este astăzi bine cunoscut şi de necontestat, nemaivorbind despre viruşi, care pot prelua controlul complet asupra unui calculator dintr-o reţea, precum periculosul cal troian "Back Orifice".

În pofida unor sisteme legislative destul de bine puse la punct, furtul de informaţii prin intermediul calculatorului s-a extins foarte mult, mai ales, în unele ţări, care deţin tehnologii avansate. El reprezintă un domeniu extrem de delicat, iar pentru protecţia si securitatea datelor se fac eforturi uriaşe.

Cele enumerate mai sus ar putea însemna doar o mică parte din numeroasele motive, pentru care este necesar să se acorde atenţie deosebită securităţii informaţiilor din calculatoare.

S-ar putea spune că majoritatea utilizatorilor din cele mai mari si mai importante instituţii din lume se află sub acoperirea unor firewall-uri de companie sau personale si că, în cazul lor, securitatea este complet asigurată. În realitate, însă, lucrurile nu stau chiar aşa. Şi dovezi în acest sens, desigur, există. Aproape zilnic apar pe Internet informaţii privind spargerea unor site-uri de Web importante, furturi de informaţii din diverse reţele, unele dintre cele mai bine puse la punct, iar dacă se mai ia în considerare că mulţi dintre cei păgubiţi refuză să-şi facă publice accidentele de această natură, chiar şi din simplul motiv de a nu risca pierderea credibilităţii sau a prestanţei, atunci, desigur, se poate confirma că statisticile nu oferă dimensiunea reală a fenomenului, iar acesta este cu mult mai îngrijorător.

În contextul afacerilor informaţiile şi procesele, pe care se sprijină sistemele si reţelele informatice, sunt subiecte deosebit de importante. Cele trei caracteristici de bază ale informaţiei (confidenţialitatea, integritatea si disponibilitatea) sunt esenţiale pentru menţinerea competitivităţii, profitabilităţii, legalităţii si imaginii comerciale ale unei organizaţii.

Din ce în ce mai mult, organizaţiile, sistemele si reţelele lor informatice se confruntă cu ameninţarea securităţii informaţiilor provocate de un larg spectru de surse, incluzând frauda, spionajul, sabotajul, vandalismul, incendiile şi inundaţiile. O sursă comună de pericol este prezentată de atacurile virusilor electronici, care pot provoca daune şi distrugeri considerabile. Aceste mijloace devin din ce în ce mai agresive şi mai sofisticate.

Unii oameni de afaceri şi profesionişti au ajuns la concluzia că un hacker suficient de competent poate pătrunde în aproape orice sistem de calcul, inclusiv în cele care au fost protejate prin metode bazate pe parole şi criptarea datelor. Alţii, mai sceptici, susţin că, chiar si atunci, când un sistem este bine protejat împotriva atacurilor din exterior, rămâne întotdeauna alternativa trădării din interior. Multe date secrete, cum ar fi listele de clienţi,

salariile angajaţilor, investiţii şi bugete, referate confidenţiale ş.a., pot fi copiate pur si simplu pe o dischetă sau USBFlash, iar aceasta poate fi scoasă de la locul de muncă, deseori chiar fără să se sesizeze ceva.

Calculatoarele de tip mainframe rezolvă problema furtului prin această sursă păstrând încuiate calculatorul şi suporturile mari de stocare a datelor. În cazul mainframe-urilor, singura cale de a putea folosi datele este cea oferită de terminalele aflate la distanţă, şi care sunt dotate cu un ecran, o tastatură, dar nu si cu unităţi de disc. Din cauza acestei siguranţe suplimentare oferite de sistemele de tip mainframe, unii experţi susţin că reţelele locale de calculatoare personale ar trebui configurate la fel, uitând că centralizarea excesivă a mainframe-urilor a fost unul din principalele motive, pentru care s-au dezvoltat calculatoarele personale.

Orice conectare obişnuită la Internet nu este întotdeauna lipsită de riscuri. Conexiunea propriu zisă, absolut inocentă la prima vedere, ar putea fi însoţită prin partaj fraudulos de un parazit sau un program spion, care dispune de rol foarte bine definit: de a fura o parte din informaţiile manipulate, unele din ele, desigur, de caracter strict confidenţial pentru proprietar. În acest sens, cu siguranţă există mare doză de neâncredere în aprecierile de natură pesimistă a unora, si de multe ori, cu sau fără voie, sunt exagerate.

În lumea specialiştilor I.T. se obişnuieşte să se spună că un P.C. este complet protejat de un produs firewall si de un program antivirus. Exista produse informatice ce pot asigura protecţie foarte bună pentru grupurile mici sau pentru P.C. - urile individuale. De exemplu, firewall-uri precum ZoneAlarm (www.zonelabs.com) sau BlackICE Defender (www.netice.com), sunt foarte la modă astăzi, iar produsele antivirus sunt foarte multe şi foarte eficace.

Tranziţia la societatea informaţională implică nevoia de informaţii credibile, iar progresul tehnologic are implicaţii de ordin exponenţial asupra evoluţiei lor. Din acest punct de vedere, necesitatea securizării informaţiilor păstrate şi procesate prin intermediul calculatoarelor decurge pur şi simplu din necesitatea de conectare si de comunicare, iar globalizarea şi Internetul au schimbat complet faţa lumii la confluenţa dintre milenii.

Calculatoarele personale prezintă vulnerabilităţi pentru că în general nu există protecţie hardware a memoriei interne şi externe: un program executabil poate avea acces oriunde în memoria internă sau pe hard-disk. În orice sistem informatic protecţia presupune asigurarea programelor şi datelor împotriva următoarelor acţiuni:

1) pierderi accidentale, cauzate de căderile de tensiune, defectarea unităţilor de hard disk;
2) accesare neautorizată a datelor şi programelor, prin acţiuni de parolare şi criptare;
3) fraudă pe calculator (sustragerea sau alterarea datelor, furturi de servicii);
4) virusarea software-ului.

Pentru o protecţie eficientă este necesar să fie cunoscute şi asigurate următoarele elemente:

1) identificarea accesului prin reguli şi relaţii între utilizatori şi resurse;
2) evidenţa accesului pentru urmărirea utilizării resurselor sistemului, precum şi pentru posibilitatea refacerii unor date în caz de distrugere;
3) integritatea şi confidenţialitatea datelor;
4) funcţionalitatea programelor.

Mijloacele prin care se poate asigura protecţia sunt:

1) măsuri organizatorice contra distrugerii datorate catastrofelor naturale, măsuri referitoare la selecţia profesională a personalului, organizarea unui sistem de control a accesului, organizarea păstrării si utilizării suporturilor de informaţii;

2) măsuri juridice, care cuprind documente normative ce controlează şi reglementează procesul prelucrării şi folosirii informaţiilor;

3) mijloace informatice constituite din programe de protecţie şi tehnici de criptare a informaţiilor.

Cele mai cunoscute şi utilizate modele de asigurare a protecţiei (autorizare a accesului) sunt:

1) Modelul Hoffman, constă dintr-un set de reguli referitoare la 4 tipuri de obiecte - utilizatori, programe, terminale şi fişiere, fiecare cu 4 caracteristici de securitate:

a) autoritatea (nesecret, confidenţial, secret, strict secret);
b) categoria (compartimente specifice de grupare a datelor (acces limitat, acces cu aprobare));
c) dreptul (grupa de utilizatori, care au acces la un anumit obiect);
d) regimul (mulţimea modurilor de acces la obiect: citire, actualizare, execuţie program).

2) Modelul Kent, are 5 dimensiuni: împuterniciri, utilizatori, operaţii, resurse, situaţii. El conţine un proces de organizare a accesului bine definit printr-un algoritm. Accesul la date este considerat drept serie de cereri ale utilizatorilor pentru operaţii la resurse într-un moment, în care sistemul se află în anumită stare [2, pp.176-183; 4, pp.220-224].

În final e necesar de accentuat că activitatea problemei protecţiei resurselor informatice este cauzată în primul rînd de masivitatea implementării şi utilizării celor de pe urmă practic în orice domeniu al activtăţii umane şi, mai cu seamă, a lucrărilor informaţionale economice, proprii pentru orice categrie de ocupaţii.

Aşa cum funcţionarea eficientă S.I$_c$.E. este asigurată prin interconexiunea şi interacţiunea corectă a constituantelor sale, astfel de preocupare devine iminamente imposibilă. Complicarea şi imperiositatea ei devin şi mai evidente în cazul aplicării mijloacelor şi metodelor informtice ce solicită îndeplinirea acţiunilor în mod automat. În aşa situaţie nu e exclus că în unele cazuri o singură eroare să conducă la alterarea şi prăbuşirea sistemului.

Din motivele enumerate mai sus şi menţionate de la începutul articolului prezent se impun conştientizarea convingătoare a rolului imperios al protejării componentelor informatice, cunoaşterea profundă a evoluţiei, distincţiei dintre fiabilitatea şi securitatea lor, categoriilor şi concordanţei mijloacelor şi metodelor acestor procese, ceea ce va contribui la performanţe notorii a lucrărilor legate de obţinerea produselor informaţionale în mediul informatic

CONCLUZII

1. Locul, rolul și valoarea funcțională în cadrul procesului unitar de gestiune economică dictează preocuparea primordială de protejare a informațiilor de conținut informativ.
2. Astfel de abordare este justificată de faptul că datele informative constituie consecința evoluției proceselor materiale și baza obținerii produselor decizionale. De aceea, de calitatea lor depinde formularea și luarea deciziilor, care direct influențează compartimentul material.
3. Totodată, protejarea izolată numai a unităților informaționale nu asigură nivelul performant deplin al calității lor, deoarece pe lângă protecție, asupra acestui parametru esențial influențează mijloacele, metodele și resursele implicate în procesarea valorilor acestor unități.

4. Din motivul dat protecția informațională integrală solicită elucidarea ei în interconexiune și interacțiune cu mijloacele și metodele de protejare a celorlalte resurse informatice.
5. Complexitatea compoziţională, volumele inimaginabile a resurselor informaționale și informatice, provocate de mersul obiectiv al proceselor globalizării activităților umane materiale și spirituale, au condus la complicarea şi acutizarea problemelor protejării şi eficientizării S.I$_c$.E.
6. Pe lângă acest fenomen, problemele în cauză sunt provocate şi de următorii factori de influenţă semnificativă:
   a) nivelul nesatisfăcător al parametrilor exploatativi ai mijloacelor tehnice informatice, de valoare decisivă dispunând suporturile informaţionale şi informatice, precum şi dispozitivele de afişare;
   b) tendinţa spre proprietatea privată a informaţiilor, aşa cum fiecare utilizator pretinde la resursele informaţionale proprii;
   c) valoarea juridică a informaţiilor economice, ceea ce solicită grad major de autenticitate a lor;
   d) ca şi orice alte informaţii, cele economice nu se consumă, din ce cauză pierderea poate conduce la imposibilitatea recuperării lor;
   e) primitivismul activităţilor de fiabilitate şi securitate a S.I$_c$.E., organizarea sistemică a cărora se găseşte la etapa iniţială.
7. Pe măsura evoluţiei practicii funcţionării S.I$_c$.E. în cadrul unităţilor economice,, tot mai insistent se impune specializarea evidentă a serviciilor informatice sub formă de anumite subdiviziuni organizatorice, rareori fiind realizate sub formă de servicii de protecție a resurselor informaționale și informatice, preponderent în sectoarele bancar, statal, afacerilor interne.
8. De pe pozițiile integrării într-un tot unitar și funcționării analoage, structurarea existentă a procesului managerial economic (fig.2) este provocată de următorii factori esențiali:
   a) dispersarea excesivă în spațiu și funcționarea expresiv discretă în timp, aceasta din urmă fiind cauzată în primul rând de gradul insuficient și primitivismul efectuării activităților materiale și informaționale umane;
   b) extinderea semnificativă a dimensiunilor teritoriale și scurtarea termenelor temporale ale preocupărilor materiale umane;
   c) respectiv, și ocupațiile informaționale, care sunt obiectiv impuse, deci, indetașabile de cele materiale, în evoluția sa s-au transformat din domeniu de preocupări a unui subiect (grup de subiecte) în domeniu de interes al societății în ansamblu.
9. Ieșirea din situația creată și perspectiva performanței permanente a domeniului elucidat pot avea loc prin crearea și aplicarea mijloacelor și metodelor bazate pe principiul integrării.

BIBLIOGRAFIE

1. Considerations on challenges and future directions in cybersecurity. Romanian Association Information Security, Romania, 2019, 333 p.
2. Ivan, I., Toma, C., Constantinescu, R. Information Security Handbook – Second Edition, Bucurежti Ed. ASE, 2009, 257-280 p..
3. Войтик А. И.,. Прожерин В.Г.Экономика информационной безопасности. Санкт-Петербург, Национальный Исследовательский Университет, 2012, 120 с.
4. Leahu T. Organizarea, structurarea și transformarea informațiilor sistemului managerial economic. Chișinău, CEP USM, 2009, 431 p.

CYBER HYGIENE CAPACITY BUILDING SKILLS THROUGH THE PRISM OF THE UNIVERSITY ECOSYSTEM

FORMAREA DEPRINDERILOR DE IGIENĂ CIBERNETICĂ PRIN PRISMA ECOSISTEMULUI UNIVERSITAR

Tutunaru Sergiu
Doctor în științe economice, conferențiar universitar
Academia de Studii Economice a Moldovei
e-mail: tutunaru@ase.md

Covalenco Ion
Inginer principal, Direcția Tehnologii Informaționale
Academia de Studii Economice a Moldovei
e-mail: covalenco@ase.md

Abstract
In this article, the authors address the importance of information security knowledge literacy for all categories of citizens, especially young people. The risks caused by non-compliance with cyber hygiene and the ways to overcome them are described. The main threats in the information space and the main methods to combat these threats are provided. The relevance of non-formal education and the possibility of implementing such non-formal education in the Republic of Moldova based on created in the Academy of Economic Studies of Moldova (AESM) educational ecosystem in the ICT fields and the materials provided free of charge by the American project CRDF is invoked. It is proposed to launch a pilot project at the AESM which aims to include as many universities and colleges as possible in the Republic of Moldova, with the task for promote non-formal education through an online course developed by CRDF.

Keywords: *education, ecosystem, cybersecurity, cyberhygiene.*

JEL Classification: *I25, I26, O39, Y80*

INTRODUCERE

Luna europeană a securității cibernetice, care a avut loc pe parcursul lunii octombrie a acestui an sub deviza „Securitatea cibernetică este fundamentul lumii digitale", s-a axat pe sensibilizarea publicului cu privire la amenințările cibernetice și promovarea importanței securității cibernetice în rândul cetățenilor și organizațiilor prin educație și schimbul de bune practici. Campania din acest an este rezultatul unei recomandări a Comisiei Europene de a se concentra asupra atacurilor online și își propune să contribuie la promovarea mesajului că igiena cibernetică ar trebui să facă parte din viața de zi cu zi a fiecărui cetățean.

Vicepreședintele Comisiei Europene Andrus Ansip, responsabil pentru piața unică digitală, a declarat: „Securitatea cibernetică este fundamentul lumii digitale; este responsabilitatea noastră comună, a tuturor, în fiecare zi." [1]

Problemele legate de dezvoltarea capacităților digitale pentru toate segmentele populației au fost reflectate pe larg și în cadrul a două reuniuni ministeriale ale Parteneriatului estic privind economia digitală (11 iunie 2015, Luxemburg și 5 octombrie 2017, Estonia), unde au fost identificate caracteristicile și direcțiile dezvoltării eficiente a economiei digitale.

REZULTATELE CERCETĂRII

Criminalitatea informatică este un domeniu aflat într-o permanentă inovare şi cunoaşte o rată foarte rapidă de dezvoltare şi diversificare. Astfel, expansiunea tipurilor de dispozitive care fac posibilă accesarea mobilă a internetului a dus la creşterea exponenţială a numărului de utilizatori şi, implicit, a riscurilor de victimizare.

În contextul în care, pe fundalul creșterii numărului de utilizatori, se poate constata o scădere a gradului de cunoaștere a riscurilor și amenințărilor care apar în mediul online, precum și a metodelor de eliminare a acestora, apreciem că este foarte importantă dezvoltarea parteneriatului cu toate organizațiile care pot contribui la creşterea gradului de conștientizare a fenomenului în rândul cetățenilor și, implicit la o mai bună siguranță".

În prezent se depun eforturi pentru prevenirea și combaterea criminalității cibernetice, care se manifestă prin infectarea cu malware, hacking, social engineering, phishing, diverse fraude online sau vulnerabilități ale hotspot-urilor Wi-Fi abordări tehnice sau legale, precum și de creștere a gradului de conștientizare în rândurile utilizatorilor de tehnologie.

Educația în domeniul securității cibernetice trebuie începută de la vârste fragede, întrucât copiii de astăzi au acces la echipamente conectate la internet și pot expune în mediul online, în mod periculos, date importante. Această educație trebuie susținută că efort atât de școală cât și de familie, iar cei responsabili trebuie să fie implicați în acest proces de educație, conștienți fiind de riscurile pe care le implica greșelile și nerespectarea unor reguli de comportament în mediul online, precum și de nevoia continuă de a cunoaște informații privind amenințările la care se expun. [2]

Probleme comune de igienă cibernetică. Întreprinderile au adesea mai multe elemente care au nevoie de igienă cibernetică. Toate componentele hardware (calculatoare, telefoane, dispozitive conectate), programele software și aplicațiile online utilizate ar trebui incluse într-un program de întreținere obișnuit și continuu. Fiecare dintre aceste sisteme prezintă vulnerabilități specifice care pot duce la diferite probleme. Unele dintre aceste probleme includ:

– Pierderea datelor: hard disk-urile și spațiul de stocare online cloud care nu sunt copiate sau întreținute sunt vulnerabile la hacking, corupție și alte probleme care ar putea duce la pierderea informațiilor.

– Date înlocuite: o igienă cibernetică deficitară ar putea însemna pierderea datelor în alte moduri. Este posibil ca informațiile să nu fie corupte sau dispărute definitiv, dar cu atâtea locuri de stocare a datelor, plasarea greșită a fișierelor devine din ce în ce mai obișnuită în întreprinderea modernă.

– Încălcarea securității: există amenințări constante și imediate pentru toate datele întreprinderii. Phishingul, hackerii, programele malware, spam-ul, virușii și o varietate de alte amenințări există în peisajul modern al amenințărilor, care este în permanență într-o stare de flux.

– Software învechit: aplicațiile software ar trebui să fie actualizate periodic, asigurându-se că cele mai recente patch-uri de securitate și cele mai multe versiuni actuale sunt utilizate în întreaga întreprindere - pentru toate aplicațiile. Software-ul învechit este mai vulnerabil la atacuri și malware.

– Software de securitate mai vechi: software-ul antivirus și alte software-uri de securitate trebuie să fie actualizate continuu pentru a ține pasul cu amenințările în continuă schimbare. Software-ul de securitate învechit - chiar și software care a trecut câteva luni fără o actualizare - nu poate proteja întreprinderea împotriva ultimelor amenințări

Activitatea online, folosind conferințe video, chat-uri de grup, platforme de schimb de date a permis să se atingă un nou nivel de eficiență și confort. Dar tranziția către munca și studiile la distanță a dus la o creștere semnificativă a atacurilor cibernetice și a scurgerilor de informații. Furtul de identitate și siguranța informațiilor cu caracter confidențial au devenit în prezent o problemă globală,

Pentru a diminua consecințele acestor fenomene este necesar să se respecte principiile de bază ale igienei cibernetice. Igiena cibernetică se referă la acțiunile și metodele pe care utilizatorii de computere și alte dispozitive trebuie să le urmeze pentru protejarea datelor personale și corporative, care ar putea fi preluate sau deteriorate. [3]

În cele ce urmează vom examina principalele pericole care ne urmăresc atunci când folosim rețelele de Internet. [4]

Vulnerabilitatea conexiunilor Wi-Fi. Wi-Fi-ul este un mijloc comod pentru verificarea rapidă a poștei electronice, schimbul de documente și conectarea la rețelele de socializare. Dar utilizarea rețelelor Wi-Fi în locuri publice: parcuri, restaurante, hoteluri, aeroporturi etc. amenință siguranța protecției datelor personale și confidențialitatea informației.

Una din măsurile de protecție ar fi eliminarea rețelelor publice Wi-Fi din lista rețelelor de încredere (acasă, la birou etc.). Astfel se va exclude posibilitatea conectării automate la rețelele publice fără consimțământul utilizatorului. O altă măsură ar fi asigurarea securității maxime a contului personal pentru a contracara încercările hackerilor de a obține acces la dispozitivul utilizatorului și a pirata sau a distruge informațiile.

Poșta electronică și riscurile pe care le comportă. Regula de bază în folosirea poștei electronice în scopuri de serviciu este de a utiliza doar poșta corporativă. Trebuie evitată trimiterea și primirea de informații și fișiere confidențiale prin serviciile de poștă publică (Yandex, Google etc.).

Nu se recomandă accesarea linkurilor indicate în scrisori și deschiderea fișierelor atașate fără a avea certitudinea că ele nu comportă riscuri de acces neautorizat. De obicei, astfel de scrisori conțin cereri de acțiune imediată (urmați linkul, deschideți urgent un atașament, instalați o aplicație etc.), acțiuni care pot afecta securitatea informației.

Un alt pericol îl prezintă mesajele de tip phishing, având adresa expeditorului similară cu adresa unor resurse oficiale, dar care diferă în unul sau două caractere (decan@asem.md, info@gogle.com etc.).

Phishingul este un tip de fraudă pe Internet, al cărui scop este de a obține acces la datele confidențiale ale utilizatorilor - autentificări și parole. Mesajele de tip phishing conțin fișiere care arată ca documente obișnuite (invitatie.doc, de exemplu), dar sunt de fapt programe care, de îndată ce sunt deschise, rulează în numele utilizatorului. Ca urmare, ele încep să își îndeplinească funcțiile, obținând, de obicei, acces la calculator sau telefon. Din acest moment, atacatorul va avea aceleași drepturi de acces ca și utilizatorul.

Mesageria electronică și pericolul scurgerii informației. Pentru a evita scurgerea de informații confidențiale trebuie evitat, pe cât e posibil, transferul prin aplicații de mesagerie (WhatsApp, Facebook, Messenger, WeChat, Telegram, Viber, Snapchat ș.a.). Dacă trebuie să transmitem urgent informații cu caracter confidențial sau care conțin secrete comerciale, și alte posibilități de transmitere nu există, informația respectivă trebuie ștearsă imediat după ce a fost transmisă. Același lucru trebuie să-l facă și destinatarul.

Atacuri Ransomware. (https://politia.md/ro/content/cunosti-ce-este-ransomware-cum-sa-previi-atacurile)

Ransomware este un tip specific de malware (programe dăunătoare) care cere fraudulos o răscumpărare financiară de la victime, amenințând cu publicarea, ștergerea sau blocarea informației.

Cel mai frecvent, atacurile Ransomware implică criptarea datelor personale sau ale companiei, astfel încât să nu poată fi utilizate sau accesate, și apoi obligă victima să plătească o răscumpărare pentru a debloca datele. Dacă vă aflați în situația în care vi se cere să plătiți răscumpărarea, nu vă lăsați pradă șantajului; aceste acțiuni se consideră drept fraude și se pedepsesc aproape în toate țările.

Pentru a nu fi jertfa unor asemenea atacuri trebuie respectate anumite reguli, cum ar fi neglijarea link-urilor sau atașamentelor suspecte din mesajele email, crearea regulată a cópiilor de rezervă pentru datele importante pe suporturi auxiliare, actualizarea permanentă a sistemului de antivirus etc.

Utilizarea parolelor ”slabe”. Se recomandă de a stabili parole diferite pentru conturi diferite, astfel încât cunoașterea parolei pentru o aplicație să nu permită accesul răufăcătorului la alte aplicații.

Parolele trebuie să fie complexe, suficient de lungi (12-15 caractere mixte) și să nu conțină date personale ușor de ghicit (Ana-1997) sau parole legate de compania la care lucrați (asem-2020).

Experiența ASEM. În scopul de a reduce decalajul dintre formarea academică și nevoile pieței resurselor umane în domeniul TIC a fost format un parteneriat între incubatorul inovator IT4BA cu 8 companii rezidente și Departamentul de informatică aplicată în afaceri, de curând creat,

Una dintre direcțiile ecosistemului creat este pregătirea informală la nivel național a tinerilor și a altor reprezentanți pentru particularitățile economiei digitale, inclusiv problemele de securitate cibernetică, prin seminare, training-uri, mese rotunde și cursuri de specialitate. [5]

În toamna anului 2020, Academia Economică a Moldovei a semnat un memorandum cu organizația CRDF Global, biroul din Kiev, pentru promovarea și desfășurarea unui curs online gratuit pentru învățarea studenților noțiunile de bază ale igienei cibernetice. În acest scop, materiale promoționale au fost postate pe site-ul oficial al ASEM, precum și în diferite rețele sociale. Au fost organizate ateliere de lucru cu studenți de la diferite specialități pentru a explica importanța respectării regulilor de igienă cibernetică în scopul asigurării securității personale și a rețelei.

Partenerul acestui proiect este organizația americană independentă non-profit CRDF Global, înființată în 1995, care promovează cooperarea științifică și tehnică internațională prin granturi, resurse tehnice, instruire și servicii. CRDF se angajează să promoveze aplicarea științei și tehnologiei la creșterea economică prin parteneriate internaționale și învățare care promovează invenția, inovația, antreprenorialul și comercializarea tehnologiei și accelerează cercetarea universitară și educația în știință și tehnologie. [6]

Implementarea acestui proiect va fi realizată de Incubatorul de Inovație IT4BA al ASEM are ca scop promovarea cursurilor online gratuite cu tema „Reguli de securitate de bază în sistemul digital mediu înconjurător". Instruirea online este disponibilă în prezent în engleză și ucraineană, iar versiunile în rusă și română vor fi disponibile în curând.

În termen de două săptămâni de la lansarea proiectului peste 80 de studenți s-au înscris pe site-ul CRDF Global (https://cybereducation.org/), o parte dintre care, după finalizarea cursurilor, au trecut cu succes testul final. În viitor, geografia educației va fi extinsă, atrăgând în proiect studenți și din alte universități din Moldova (Universitatea de Stat, Universitatea Pedagogică, Universitatea din Comrat și altele). Programul online conține următoarele 11 module:

Introducere și evaluare inițială; Principalele greșeli ale utilizatorilor; Utilizarea în siguranță a telefoanelor mobile; Utilizarea în siguranță a computerelor; Utilizarea în

siguranță a e-mailului; Siguranța în rețelele sociale; Utilizarea în siguranță a internetului; Tipuri de software rău intenționat; Știri false; Regula de bază a protecției datelor; Ce să faci dacă ai avut probleme.
Cursul se încheie cu un test online de 41 de întrebări cu răspuns multiplu. Participanții care răspund cu succes la cel puțin 31 de întrebări din 41 vor primi diplome internaționale de la CRDF Global, ceea ce va fi, fără îndoială, un bun suport pentru cariera lor. Pentru a trece testul, fiecare participant are dreptul la 3 încercări. Finalizarea proiectului este programată pentru aprilie 2021.

CONCLUZII

Concluzionând, putem spune că răspândirea virusului COVID-19 a schimbat radical viața oamenilor de pe glob. În aceste circumstanțe, instituțiile de stat și companiile private încearcă să se adapteze la condițiile noi, una din soluții fiind activitatea la distanță. Dar organizarea activităților online atrage după sine și o creștere bruscă a criminalității cibernetice. Se urmărește extinderea pe mai departe a proiectului prin atragerea unui număr cât mai mare de universități și colegii din țară.

BIBLIOGRAFIE

1. https://www.caleaeuropeana.ro/luna-europeana-a-securitatii-cibernetice-avira-si-cert-ro-vor-distribui-gratis-licente-antivirus-liceenilor-din-romania/
2. https://start-up.ro/bune-practici-de-igiena-cibernetica-cum-te-aperi-de-amenintarile-din-online/
3. https://DIGITALGUARDIAN.COM/BLOG/WHAT-CYBER-HYGIENE-DEFINITION- CYBER -HYGIENE-BENEFITS-BEST-PRACTICES-AND-MORE
4. https://vc.ru/u/545411-konsaltingovaya-gruppa-obereg/138612-kak-obezopasit-sebya-v-cifrovom-mire
5. Tutunaru, Sergiu; Covalenco, Ion. National Activities IT4BA incubator in the framework of the EU Digital Economy Strategy (DES). Conferința științifică Internațională ”Competitivitatea si inovarea în economia cunoașterii”, 28-29 septembrie 2018, Chișinău 2018, p. 49-52, ISBN 978-9975-75-934-
6. https://ru.qaz.wiki/wiki/CRDF_Global

ONLINE INSURANCE, CYBER RISKS AND THEIR PREVENTION

ASIGURĂRILE ONLINE, RISCURILE CIBERNETICE ȘI PREVENIREA ACESTORA

Dogotari Ilie
Doctorand, Universitatea Liberă Internațională din Moldova
e-mail: dogotari@gmail.com

Spînu Ana
Doctor în științe economice, conferențiar universitar
Universitatea Liberă Internațională din Moldova
e-mail: aspinu@ulim.md

Abstract
The actuality of the subject is explained by the fact that electronic insurance is not a future related field. Customers want electronic insurance because it has great benefits for modern people. The digital age creates many new opportunities for the economy and society. But at the same time, it brings new challenges. To have successful online insurance, insurance companies need to have a cyber risk prevention policy, so the security of networks and information systems is essential for the proper functioning of the insurance market. The aim of the research is to identify how the cyber risks influencing online insurance can be predicted. The main research methods applied to the elaboration of the article are induction, deduction, analysis, synthesis, documentation and observation. As a result of the research, we mention that to minimize the effects of cyber risks on the field of insurance, it is necessary to adopt a wide range of measures to protect the digital market and to protect infrastructure and citizens.

Keywords: *Insurance, cyber risks, online insurance, regulations, cyber security*

JEL Classification: *G220 Insurance; Insurance Companies; Actuarial Studies*

INTRODUCERE

Asigurările electronice nu mai țin de domeniul viitorului. Clienții vor asigurări electronice, pentru că ele prezintă avantaje enorme pentru omul contemporan. Azi nu mai avem timp să ne deplasăm pentru a primi un produs sau serviciu, fie el și unul financiar. Indiferent de complexitatea serviciilor, majoritatea oamenilor prefera ca acestea să fie accesibile direct din computerul său, smartphone sau tabletă.

Asemenea altor sectoare financiare, în ultimii ani se constată o creștere spectaculoasă a sectorului (industria) asigurărilor. Pe lângă mijloacele tradiționale de încheiere a polițelor de asigurare, marile companii prezente pe piață încep să acorde o importanță tot mai mare canalelor de distribuție online a produselor. Astfel, orientarea către un nou mod de promovare/vânzare a produselor va determina pe de o parte creșteri ale cifrei de afaceri a companiilor de asigurări, în timp ce pe de altă parte, ia amploarea, frecvența și impactul incidentelor de securitate care sunt în creștere și reprezintă o amenințare gravă pentru funcționarea rețelelor și a sistemelor informatice. Sistemele respective pot să devină, de asemenea, o țintă pentru acțiunile dăunătoare deliberate menite să afecteze sau să întrerupă funcționarea sistemelor. Astfel de incidente pot să împiedice desfășurarea activităților economice, să genereze pierderi financiare substanțiale, să submineze încrederea utilizatorilor și să provoace pagube majore companiei.

REZULTATELE CERCETĂRII

Era digitală creează numeroase noi oportunități pentru economie și societate. Dar, în același timp, introduce noi provocări. Un studiu privind atitudinile față de securitatea cibernetică efectuat de Eurobarometru în 2018 arată că cetățenii UE sunt preocupați de securitatea cibernetică și de confidențialitate [18]. Astfel, 88% dintre utilizatorii zilnici de internet și-au exprimat mari îngrijorări cu privire la atacurilor cibernetice, iar 77% dintre utilizatorii zilnici de internet și-au exprimat mari îngrijorări cu privire la faptul că informațiile lor personale nu sunt păstrate în siguranță de site-uri web.

Pentru ca asigurările online să aibă succes este necesar ca companiile de asigurare să aibă o politică de prevenire a riscurilor cibernetice, prin urmare, securitatea rețelelor și a sistemelor informatice este esențială pentru buna funcționare a pieței de asigurări.

Asigurarea electronică reprezintă totalitatea documentelor electronice ce constituie actul juridic prin care asiguratul se obligă să plătească o primă asiguratorului care preia asupra sa riscul asigurat, obligându-se la producerea acestuia, să plătească asiguratului sau unei terțe persoane o despăgubire sau suma asigurată.

Dezvoltarea tehnologiei informaționale din ultimii ani, a dus la schimbarea radicală a mediului de afaceri. Deschiderea info-structurii IP (Internet Provider) a înlesnit apariția noilor modele de afaceri și a creat oportunități fenomenale.

Tot mai multe întreprinderi își trec afacerile pe online, în special comerțul, deoarece acesta implică mai puține costuri, astfel fiind mai profitabile. Însă, odată cu începerea activităților pe online, apar o mulțime de probleme, precum:

- veridicitatea informațiilor;
- imposibilitatea interzicerii intrării persoanelor nedorite în rețea;
- securitatea datelor clienților.

Se presupune că o afacere online creează medii nesigure de lucru. În acest sens, trebuie evaluate riscurile și beneficiile pe care o societate le are în urma implementării IT și, în funcție de acestea trebuie organizată activitatea pe care o desfășoară.

În discursul său despre statul Uniunii de pe 13 septembrie 2017[15], președintele Comisiei Europene, Jean-Claude Juncker a menționat că *atacurile cibernetice nu cunosc frontiere și nimeni nu este imun.*

Noțiunea de risc cibernetic cuprinde o multitudine de riscuri care amenință bunurile firmelor, guvernelor sau persoanelor fizice, pierderile în general incluzând active financiare sau nefinanciare, identități, divulgarea de informații sensibile și întreruperea activităților/afacerii.

Conform statisticii guvernului Regatului Unit, criminalitatea informatică generează pierderi anuale de peste 38 miliarde USD [5]. Chiar și așa, în Europa 68% dintre organizații nici nu au estimat impactul financiar al unui atac cibernetic. Doar 25% dintre companii dețin un plan de răspuns în cazul atacurilor cibernetice. La nivel mondial, se estimează pierderi cauzate de riscuri cibernetice la aproape 0,5% din PIB-ul mondial și aproape de două ori mai mult decât media anuală a pierderilor datorate dezastrelor naturale.

Se estimează că riscurile aferente activității în mediul online, apar de fiecare dată când se deschide o poartă în rețea, de fiecare dată când se permite accesul unei persoane din exterior la rețeaua companiei. Afacerile online reprezintă o activitate nouă și majoritatea companiilor nu realizează riscurile aferente acestui nou format. Printre acestea se enumeră:

- responsabilitatea companiei pentru datele colectate, utilizate și stocate, de la clienți, parteneri și angajați;

- pierderea datelor personale sau ale clienților - o amenințare constanta pentru orice companie - exista riscul unui atac de tip hacking sau a unor incidente interne, ca urmare a neglijenței sau unui act intenționat;
- pierderea de venituri ca urmare a întreruperii activități;
- riscuri reputaționale;
- riscuri de atac în scopul răscumpărărilor;
- riscul de sancțiuni din partea supraveghetorilor

Riscul cibernetic trebuie gestionat din mai multe perspective. Modelul clasic de gestionare a riscului cibernetic cuprinde următoarele etape:

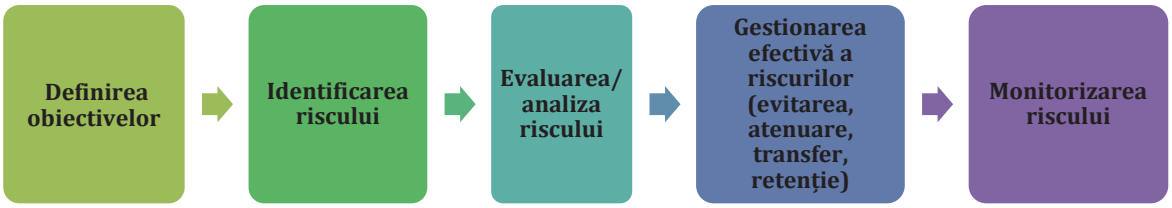


Figura 1. Etapele de gestionare a riscului cibernetic

Sursa: [elaborat de autor]

Pentru ca asigurările online să se dezvolte, trebuie excluse sau, cel puțin, minimizate riscurile cibernetice. Toți emitenții de asigurări online trebuie să garanteze consumatorului/clientului un mediu sigur.

Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare. În acest sens, asiguratorii trebuie să adopte politici interne și să pună în aplicare măsuri care să respecte, în special, principiul protecției implicite a datelor, în corespundere cu legislația privind protecția datelor cu caracter personal.

Uniunea Europeană a adoptat o gamă largă de măsuri pentru a proteja piața unică digitală europeană și pentru a proteja infrastructura, guvernele, întreprinderile și cetățenii. Printre aceste măsuri se enumeră și un șir de reglementări.

Unul dintre aceste acte este *Regulamentul general privind protecția datelor (GDPR)* [16] - introdus în mai 2018, care oferă noi reguli pentru a oferi cetățenilor un control mai mare asupra datelor lor personale și un avantaj competitiv pentru companiile conforme.

Un alt document este *Directiva privind confidențialitatea electronică* [17], care asigură protejarea confidențialității comunicărilor noastre online. Această directivă asigură confidențialitatea comunicărilor și definește regulile privind urmărirea și monitorizarea online. La momentul actual directiva urmează a fi actualizează pentru a acoperi noile mijloace de comunicații online, astfel de e-mailuri web și servicii de mesagerie (Regulamentul ePrivacy).

Drept exemplu mai poate fi adus și *Regulamentul eIDAS* [18], document ce reglementează sistemul de identificare și autentificare electronică la nivelul UE. Sistemul de identificare electronică, autentificare și servicii de încredere (eIDAS) a intrat în vigoare în octombrie 2018, introducând modalități sigure pentru persoanele fizice și companiile de a efectua tranzacții online.

Acest sistem include:

- ✓ Un sistem de semnături digitale transfrontaliere;
- ✓ Profilare digitală conformă cu GDPR;
- ✓ Respectarea principiului „o singură dată”, în care cetățenii și companiile trebuie să furnizeze autorității informații standard o singură dată.

Deci, în scopul dezvoltării unui mediu sigur este necesar ca autoritățile de supraveghere și control să creeze reguli clare și stricte în ceea ce privește siguranța informațională.

Dreptul la viață privată este expres prevăzut în Constituția Republicii Moldova, prin consacrarea sa în Articolul 28, care prevede că "statul respectă și ocrotește viața intimă, familială și privată" care include în sine și dreptul la protecția datelor cu caracter personal. La 15 februarie 2007 a fost aprobată prima lege privind protecția datelor cu caracter personal [19], acel act legislativ definea domeniul de aplicare, noțiunile principale și cerințele de bază în procesul de prelucrare a datelor cu caracter personal, stabilind regimul de confidențialitate și instituirea Centrului Național pentru Protecția Datelor cu Caracter Personal ca autoritate de supraveghere și control. Ulterior, pe data de 8 iulie 2011 a fost adoptată Legea Nr. 133[7] privind protecția datelor cu caracter personal în versiune nouă, fapt ce a permis eliminarea, în mare parte, a discrepanțelor între legislația europeană și cea națională. Deși de la adoptarea noii legi privind protecția datelor cu caracter personal a trecut o perioadă, constatăm, totuși, un șir de restanțe în ceea ce privește implementarea ei.

Concepţia securităţii informaționale a Republicii Moldova, aprobată prin Legea nr. 299/2017, reprezintă documentul de bază pentru elaborarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024. Aceasta strategie urmează să transpună la nivel național modelul european de dezvoltare a societății informaționale și a poate fi considerată un punct de pornire pentru consolidarea protejării intereselor persoanelor, ale societăţii și ale statului în domeniul informaţional.

Pe lângă Centrul Național de Protecție a Datelor cu Caracter Personal, este necesar ca și Comisia Națională a Pieței Financiară să elaboreze politici și regulamente care să vizeze securitatea informațională a clienților pe piața asigurărilor. În România, de exemplu, există deja Ghidul Consumatorului privind Comercializarea prin Mijloace electronice a produselor și serviciilor de Asigurare. În acestea sunt explicate clienților noțiunile de bază. Totodată, sunt explicate drepturile și obligațiunile asiguraților. De asemenea, sunt enumerate un șir de cerințe ce trebuie să le întrunească o pagină destinată comerțului online, astfel încât, clientul să aibă măcar câteva criterii la care ar putea să facă referire atunci când decide să procure o asigurare electronică [4]. Toate aceste lucruri, conferă entităților emitente de servicii electronice, în primul rând mai multă credibilitate și în al doilea rând, acestea sunt obligate să întrunească norme minime de siguranță.

Piața de asigurări din România, a fost nevoită să treacă printr-o serie de schimbări legislative. Printre acestea, se numără ajustarea cadrului legal cu Regulamentul privind Protecția Datelor Personale (GDPR), și Directiva privind Distribuția în Asigurări (IDD) – care a transformat întreaga distribuție de asigurări, a pus accent pe protecția consumatorilor și impune o serie de cerințe exigente în ceea ce privește pregătirea profesională.

Companiile de pe piața de asigurări din România, au înţeles foarte bine răspunderea adusă de noul regulament privind protecţia datelor şi au reacţionat prompt pentru implementarea cerinţelor legislative, unii începând introducerea prevederii chiar din 2017. Companiile din industria asigurărilor au reuşit să integreze cu succes prevederile GDPR în fluxul intern de lucru, sporind astfel încrederea clienţilor şi câştigând valoare adăugată prin prelucrarea securizată a datelor cu caracter personal.

Pe lângă acestea, în România au fost elaborate un șir de acte normative care au menirea să protejeze asiguraţii și să constrângă brokerii și asigurătorii să se conformeze cerințelor vis-a-vis siguranța informațională, precum:

1. *Norma nr.15/2015 privind comercializarea prin mijloace electronice a contractelor de asigurare [2]* care stabilește condițiile în baza cărora Autoritatea de Supraveghere Financiară (ASF) reglementează activitatea de comercializare prin mijloace

electronice a contractelor de asigurare. Norma a impus un minim necesar de condiții pentru furnizori de soluții și/sau aplicații software dedicate pentru activitatea de comercializare on-line sau prin mijloace electronice a contractelor de asigurare - care include prezentare informației despre serviciilor oferite către utilizator, politica de prelucrare a datelor cu caracter personal și securitate cu obligativitatea utilizării protocolului de securitate Transport Layer Security (TLS utilizând chei de minimum 2048 biti), sau protocoale similare ori cu aceleași capacități tehnice și certificate emise de un furnizor acreditat.

Această normă a fost valabilă până la 20 decembrie 2018, fiind abrogat și înlocuită prin *Norma 19/2018 privind distribuția de asigurări* care reglementează: încadrarea intermediarilor de asigurări, reasigurări și asigurări auxiliare în anumite categorii, raporturile juridice dintre distribuitori și canalele de distribuție ale acestora, procesul de înregistrare a intermediarilor, procesul de supraveghere și monitorizare permanentă de către ASF - Autoritatea de Supraveghere Financiară a activității de distribuție desfășurate de către distribuitori, inclusiv a respectării regulilor de conduită, activitatea de comercializare a contractelor de asigurare prin intermediul site-urilor distribuitorilor și/sau prin alte mijloace de comunicare, etc.

2. Ordinul CSA nr. 23/2009 pentru punerea în aplicare a Normelor privind informațiile pe care asigurătorii și intermediarii în asigurări trebuie să le furnizeze clienților [3]. Această normă a fost valabilă până la 20 decembrie 2018, fiind abrogată prin Normă 19/2018 privind distribuția de asigurări menționată anterior.

Spre deosebire de alte industrii, companiile din domeniul asigurărilor prelucrează o gamă largă de date cu caracter personal pentru scopuri diverse, precum servicii de asigurare de viaţă, asigurare de sănătate, soluţionarea dosarelor de daună şi altele. Astfel, protecția datelor este esențială pentru menținerea încrederii asiguraților.

Prin exemplele menționate ne convingem de faptul că cadrul normativ în domeniul protecției asiguraților și activității intermediarilor de asigurări și asigurătorilor este în continuă modificare și perfectare.

Deși, în Legislația Republicii Moldova sunt norme care reglementează securitatea informațională, protejarea datelor cu caracter personal, printre care regăsim și Legea privind protecţia datelor cu caracter personal scopul căreia este asigurarea protecţiei drepturilor şi libertăţilor fundamentale ale persoanei fizice în ceea ce priveşte prelucrarea datelor cu caracter personal, în special a dreptului la inviolabilitatea vieţii intime, familiale şi private [7], acestea totuși, din dorința de a cuprinde toate domeniile existente sunt mult prea generale, iar pe alocuri neclare pentru domenii anume. Din acest motiv, este necesar ca autoritățile de supraveghere să conlucreze, astfel încât companiile de asigurare și brokerii să aibă norme clare, regulamente de care se pot conduce în procesul de lucru. Ideal ar fi ca autoritățile să organizeze seminarii de instruire, care să finalizeze cu examene.

Totodată, pe lângă cerințele legale vis-a-vis de siguranța datelor, este important ca fiecare companie, dar mai ales, emitenții de servicii electronice de asigurare, să implementeze standardelor internaționale de management al securității informaționale, ISO 27001, acesta demonstrează angajamentul pentru protecţia datelor procesate, continuitatea activităţilor (business continuity) şi respectarea legislaţiei naţionale şi internaţionale în domeniu [1].

Alinierea la Cadrul UE de certificare de securitate cibernetică ar aduce avantaje întregului sistem al asigurărilor. Sistemul european de certificare de securitate cibernetică este un set cuprinzător de norme, cerințe tehnice, standarde și proceduri convenite la nivel european pentru evaluarea proprietăților de securitate cibernetică ale unui anumit produs, serviciu sau proces.

Certificarea de securitate cibernetică joacă un rol important în sporirea încrederii utilizatorilor în produsele, serviciile și procesele care sunt esențiale pentru funcționarea corespunzătoare a pieței unice digitale și în consolidarea securității acestora. Având în vedere gama largă de produse, servicii și procese TIC și multiplele întrebuințări date acestora, cadrul european de certificare de securitate cibernetică permite crearea unor sisteme UE de certificare personalizate și bazate pe riscuri.

Pentru a exprima riscul de securitate cibernetică, un certificat se poate referi la trei niveluri de asigurare (de bază, substanțial, ridicat), care sunt proporționale cu nivelul de risc asociat utilizării preconizate a produsului, procesului sau serviciului în cauză din perspectiva probabilității survenirii unui incident și a impactului acestuia. De exemplu, un nivel ridicat de asigurare înseamnă că produsul care a fost certificat a trecut cele mai exigente teste de securitate.

Certificatul acordat va fi recunoscut în toate statele alineate la cadrul UE, ceea ce va facilita, pe de o parte, schimburile comerciale transfrontaliere între întreprinderi și, pe de altă parte, înțelegerea de către utilizatori a elementelor de securitate ale produsului sau serviciului respectiv. Acest lucru permite o concurență benefică între furnizori pe întreaga piață a UE, ceea ce se reflectă într-o mai bună calitate a produselor și într-un raport calitate-preț mai bun.

Consumatorii au dreptul de a primi informații corecte, încă înainte de a încheia un contract de asigurare, adică în faza precontractuală, referitor la toate condițiile contractului de asigurare.

Este important ca persoana să înțeleagă de ce anumite categorii de date sunt colectate, o pagină de internet care comercializează produse de asigurare online, trebuie să dea explicații clar clienților săi, de ce unele date sunt colectate și de ce anume într-o anumită măsură. Până la procurarea produsului de asigurare, clientul trebuie să facă cunoștință cu termenii și condițiile companiei, cu politica de confidențialitate, cu regulile ce țin de reziliere, returnarea de primă și calculul primei de asigurare.

Conținutul paginii de internet trebuie să fie unul accesibil, clar, fără echivoc, nu trebuie să fie solicitată informație suplimentare, ce ar putea fi utilizate în scopuri decât emiterea contractelor de asigurare. Este foarte important ca utilizatorul paginii să-și dea consimțământul pentru prelucrarea datelor cu caracter personal, și nu doar! Clientul trebuie să aibă opțiunea de a alege scopurile pentru care pot fi utilizate acele date.

Dar până a ajunge la acest nivel, este necesară educarea populației. Mare parte a populației din Republica Moldova suferă de lipsă de cunoștințe în domeniul juridic și financiar. Cum ar putea persoana să fie pregătită să procure ceva online, nemaivorbind de asigurări electronice, dacă aceștia nu înțeleg, sau ce e mai grav, nu au acces la internet, la un card. Este de datoria statului să informeze populația despre modul în care populația își poate gestiona riscurile. Aceste lucruri trebuie educate din școli, la cea mai fragedă vârstă. După care am putea să ne racordăm la cele mai variate studii din Europa, și să preluăm practicile acestora. Moldovenii în continuare preferă să facă cumpărături offline. Mai ales când vorbim despre produsele financiare, precum asigurările.

Drept argument a celor menționate apelăm la raportul BNM referitor la indicatorii activității în cadrul sistemelor de plăți cu cardurile de plată din Republica Moldova pentru anul 2019 [12] conform căruia se constată că din volumul total al operațiunilor cu carduri de 70 594 184,5 mii lei doar 4 471 477,25 mii lei sunt plăți fără numerar fără prezența fizică a cardului cea ce constituie o cotă de 6,33%. Astfel, se observă o lipsa de încredere din partea populației față de tot ce ține de comerțul electronic.

CONCLUZII

În concluzie constatăm că în vederea dezvoltării asigurărilor online trebuie excluse sau, cel puțin, minimizate riscurile cibernetice. În acest scop este necesar de a actualiza legislația Republicii Moldova care este alcătuită din norme mult prea generale, iar pe alocuri neclare pentru domenii anume. Din acest motiv, este necesar ca autoritățile de supraveghere să conlucreze, astfel încât companiile de asigurare și brokerii să aibă norme clare, regulamente de care se pot conduce în procesul de lucru.

BIBLIOGRAFIE

1. ISO/IEC 27001. Information security management. Disponibil: http://www.iso.org/isoiec-27001-information-security.html
2. Norma nr.15/2015 privind comercializarea prin mijloace electronice a contractelor de asigurare. În: Monitorul Oficial al României, Partea I nr. 641 din 24 august 2015. Disponibil: https://lege5.ro/Gratuit/g42tenbvg4/norma-nr-15-2015-privind-comercializarea-prin-mijloace-electronice-a-contractelor-de-asigurare
3. Ordinul nr. 23/2009 pentru punerea în aplicare a Normelor privind informațiile pe care asigurătorii și intermediarii în asigurări trebuie să le furnizeze clienților, precum și alte elemente pe care trebuie să le cuprindă contractul de asigurare. În: Monitorul Oficial al României, Partea I nr. 908 din 23 decembrie 2009. Disponibil: http://lege5.ro/Gratuit/geztaobygy/ordinul-nr-23-2009-pentru-punerea-in-aplicare-a-normelor-privind-informatiile-pe-care-asiguratorii-si-intermediarii-in-asigurari-trebuie-sa-le-furnizeze-clientilor-precum-si-alte-elemente-pe-care-treb
4. ASF. Ghidul Consumatorului privind Comercializarea prin Mijloace electronice a produselor și serviciilor de Asigurare. Disponibil: http://asfromania.ro/files/consumatori/Ghid_comert%20electronic.pdf
5. Cyber Essentials: Requirements for IT infrastructure. Disponibil: http://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-IT-infrastructure-2-1.pdf
6. Geneva Association. Understanding and Addressing Global Insurance Protection Gaps. Disponibil: https://www.genevaassociation.org/sites/default/files/research-topics-document-type/pdf_public/understanding_and_addressing_global_insurance_protection_gaps.pdf
7. LEGE Nr. 133din 08-07-2011 privind protecţia datelor cu caracter personal. În: Monitorul Oficial al RM, Nr. 170-175 art.492. Disponibil: https://www.legis.md/cautare/getResults?doc_id=110544&lang=ro
8. Directiva privind securitatea rețelelor și a sistemelor informatice. https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
9. Legea UE privind securitatea cibernetică . Disponibil: https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en
10. Noile norme în domeniul telecomunicațiilor intră în vigoare. http://ec.europa.eu/commission/presscorner/detail/ro/IP_09_1966
11. Legea Nr. 299 din 21-12-2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova. Disponibil: http://www.legis.md/cautare/getResults?doc_id=105660&lang=ro
12. Raport: Indicatorii activităţii în cadrul sistemelor de plăţi cu cardurile de plată din Republica Moldova. Disponibil: http://www.bnm.md/bdi/pages/reports/dsp/DSP1.xhtml?id=0&lang=ro
13. Eurobarometru. Europa pentru cetățeni. http://www.europarl.europa.eu/romania/ro/ue_pentru_celateni/eurobarometru.html
14. Norma 19/2018 privind distribuția de asigurări. Disponibil: https://asfromania.ro/files/Asigurari/norme/2019/Norma%2019_2018%20%20%20_MoF.pdf
15. Discursul Președintelui JEAN-CLAUDE JUNCKER PRIVIND Starea Uniunii 2017. Disponibil: http://ec.europa.eu/commission/presscorner/detail/ro/SPEECH_17_3165

16. Regulamentul (UE) 2016/679 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și libera circulație a acestor date. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN
17. Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0058&from=RO
18. Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă. Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32014R0910&from=RO
19. LEGE Nr. 17 cu privire la protecţia datelor cu caracter personal din 15.02.2007. Disponibil: http://lex.justice.md/index.php?action=view&view=doc&lan-g=1&id=324657

CALCULATION OF DAMAGE FROM EMERGENCY SITUATIONS

РАСЧЁТ УЩЕРБА ОТ ЧРЕЗВЫЧАЙНЫХ СИТУАЦИЙ

Пянковский Сергей
Аспирант, Международный Независимый Университет Молдовы
e-mail: an_stern@hotmail.com

Abstract
The technique of determining the damage from various emergencies is considered. The analysis of the classifier of emergency situations is presented. Examples of damage calculation for specific situations are given.

Keywords: *Analysis, Emergency Situation, Damage from emergencies*

JEL Classification: *H56, D81, C23, C41, M15*

ВВЕДЕНИЕ

В современном технологически развивающимся мире и постоянно меняющимися природными процессами, прослеживается рост аварий и катастроф, которые уносят человеческие жизни, приводят к необратимым изменениям экологического равновесия, и как следствие к кардинальным изменениям в экономике и в политике на пострадавших территориях. Для успешного противостояния этим изменениям наступает понимание пересмотра процессов принятия решений, создание единой системы, объединяющей практические и математические модели. Для систем поддержки принятия решений необходимо определить и классифицировать все возможные прямые и косвенные риски, связанные с возникновением чрезвычайных ситуаций. Знание и понимание всех этих процессов поможет найти методику, существенно сокращающую пагубное влияние последствий чрезвычайных ситуаций их влияния на экономическое и политическое развитие Республики Молдова.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Сам по себе каждый метод оценки ущерба имеет свои нормативные параметры, показатели и определения. Наступает понимание в объединении всех методов оценки ущерба, в единую систему которая позволит Генеральному Инспекторату по Чрезвычайным Ситуациям в Республике Молдова выбрать наиболее приемлемый метод, отвечающий реалиям времени. Оценивание ущерба от чрезвычайных ситуаций природного и техногенного характера – сложная и многосторонняя задача.

На данный момент, Генеральный Инспекторат по Чрезвычайным Ситуациям Республики Молдова отражает в статистическом учёте прямой ущерб основных фондов и ущерб населению, от чрезвычайных ситуаций природного и техногенного характера. На рисунке №1. представлена диаграмма прямого ущерба от чрезвычайной ситуации за последние 10 лет произошедших на территории Республики Молдова.

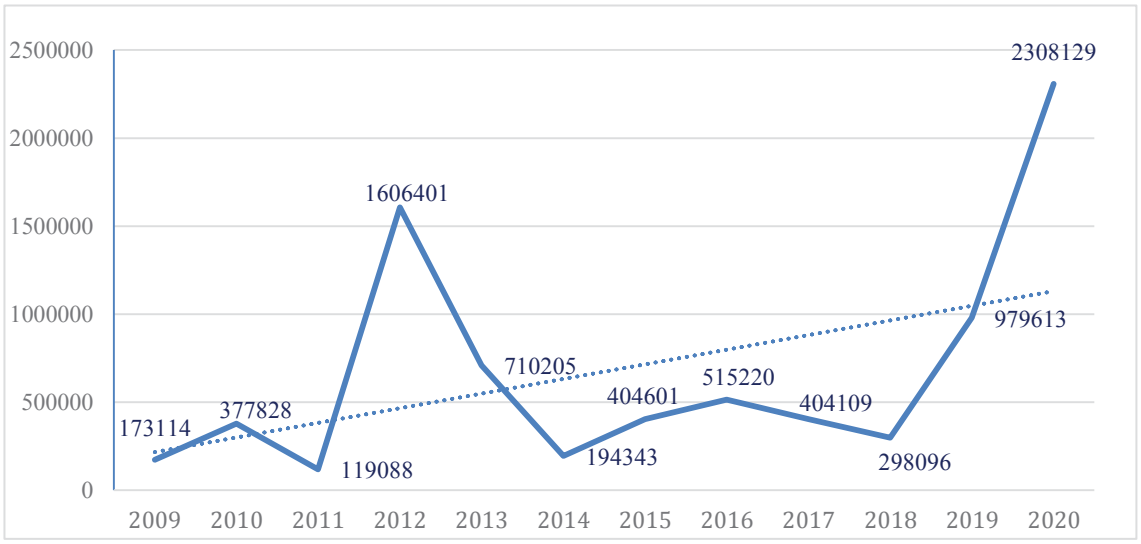


Рисунок 1. Диаграмма прямого ущерба от чрезвычайных ситуаций в течении последних 10 лет в Республике Молдова

Источник: составлено автором на основе статистических данных Генерального Инспектората по Чрезвычайным Ситуациям Республики Молдова

Наклон средней составляющей, показанный на графике пунктирной линией, демонстрирует рост прямого материального ущерба от чрезвычайных ситуаций. Так же на графике заметны пиковые всплески, например в 2012 году, где сумма прямого ущерба была в более 2 раза больше по сравнению с средним показателем по годам и составила 1606,401 тыс. лей. 2019 год тоже отметился всплеском прямого материального ущерба, составил 979,613 тыс. лей, что в свою очередь превысил средний показатель по годам на величину более 600 тыс. лей. За первое полугодие 2020 года величина ущерба превысила отметку более двух миллионов и продолжает стремительно расти. Этот рост вызван небывалой засухой в 2020 году, в результате которой высохли водоемы, пострадал урожай зерновых и технических культур.

Полный ущерб от чрезвычайных ситуаций рассчитывается как сумма всех составляющих прямого и косвенного ущерба.

$$У_{полный} = \sum_{n}^{1} У_{прямой} + \sum_{m}^{1} У_{косвенный}$$

Значения переменных n и m изменяется в зависимости от типа чрезвычайных ситуаций, а также от жизненных ценностей общества или группы лиц, производящих данный расчёт.

Сама по себе задача оценки ущерба от чрезвычайных ситуаций природного и техногенного характера, не имеет простого решения, в виду большого количества факторов влияющий на точный расчёт с большими степенями свободы.

Анализируя переменные входящие в состав прямого материального ущерба явно выделяются две основные, фундаментальные группы, такие как, ущерб, нанесённый в производственной сфере и ущерб, нанесённый в непроизводственной сфере.

$$У_{прямой} = \sum_{n}^{1} У_{производственный} + \sum_{m}^{1} У_{непроизводственный}$$

Где

$$У_{призводственный} = \sum_{a}^{1} У_{осф} + \sum_{b}^{1} У_{обф} + \sum_{e}^{1} У_{прочий}$$

$$У_{непроизводственный} = \sum_{c}^{1} У_{нас} + \sum_{d}^{1} У_{си}$$

Следовательно, формулу прямого материального ущерба, состоящую из следующих факторов можно представить, как, - сумму ущерба всех (ОСФ) основных фондов + сумма ущерба всех (ОБФ) оборотных средств + сумма ущерба (НАС) населению + сумма ущерба (СИ) социальной инфраструктуре + сумма ущерба прочим производственным объектам находящихся на территории предприятия.

$$У_{прямой} = \sum_{a}^{1} У_{осф} + \sum_{b}^{1} У_{обф} + \sum_{c}^{1} У_{нас} + \sum_{d}^{1} У_{си} + \sum_{e}^{1} У_{прочий}$$

Значения переменных **a, b, c, d** и **e** изменяется в зависимости от типа чрезвычайных ситуаций, а также от жизненных ценностей общества или группы лиц, производящих данный расчёт.

При детальном рассмотрении косвенного материального ущерба выделяются три основные группы: - ущерб, связанный с остановкой производства (ОП), влияющего на уменьшение объема добавленной стоимости + ущерб третьим лицам (ЛИЦ) + ущерб, связанный с предупреждением и ликвидацией чрезвычайных ситуаций (ПЛ).

$$У_{косвеннный} = \sum_{a}^{1} У_{оп} + \sum_{b}^{1} У_{лиц} + \sum_{c}^{1} У_{пл}$$

Простой линейный подход на основе физических свойств системы приводит к огромным погрешностям и как следствие недооценке величины получаемых результатов. Наиболее точные результаты получаются при объединении экспериментальных и математических методов оценки ущербов. В основе анализа и прогнозирования экономического ущерба от чрезвычайных ситуаций прослеживается два направления это теоретическо-познавательная и управленческая которая на прямую связана с возможностью приятия правильных точечных решений, на основе полученных результатов.

Предлагается использовать полученные результаты для обоснования инвестиционных проектов, направленных на защиту граждан и территории от природных и техногенных катастроф, а также определение необходимой суммы для финансирования служб экстренного реагирования. Данный подход позволяет определить полный ущерб от чрезвычайных ситуаций. На рисунке №2 представлена карта расчёта полного ущерба от воздействия чрезвычайной ситуации. Карта разработана автором. Одним из очень сложных процессом является определение ущерба, в случае потери жизни, этот показатель не внесён в предложенную карту.

Практика показывает, что при расчёте косвенного материального ущерба, необходимо учитывать будущие периоды, в которых будут происходить финансовые затраты. Как правило эти процессы, происходят на протяжении долгого периода после ликвидации чрезвычайной ситуации, могут привести к двойному учёту.

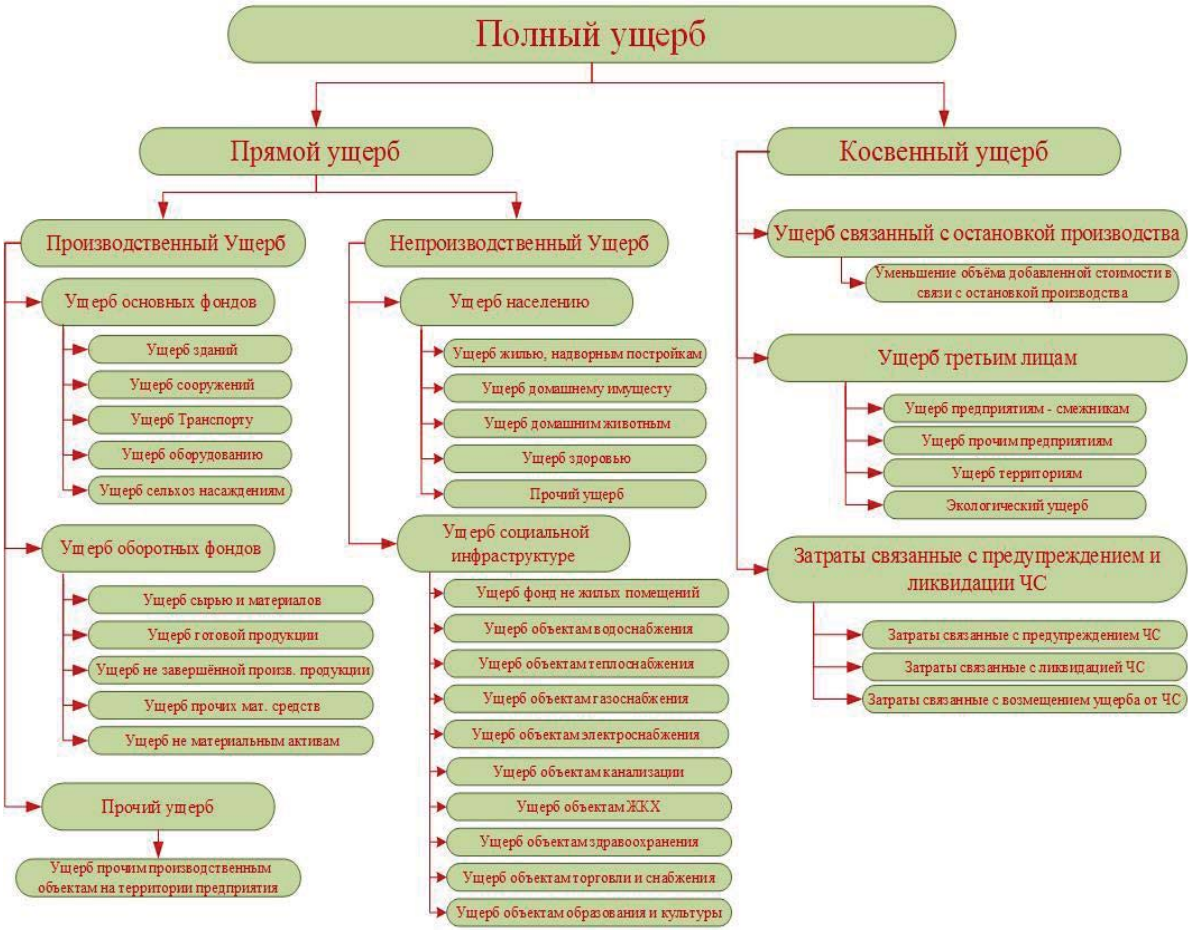


Рисунок 2. Карта формирования расчётов полного ущерба в результате возникновения чрезвычайной ситуации

Источник: разработана автором

Для разных форм собственности и от типа чрезвычайной ситуации, а также от методов наблюдения и анализа реализации этой карты расчётов, могут иметь существенные различия. [3]

Можно выделить три основных метода анализа и прогнозирования ущерба от чрезвычайной ситуации, оперативный метода применяемый в командном пункте оперативного управления на чрезвычайную ситуацию, тактический метод предусматривает постоянное наблюдение, мониторинг за основными индикаторами характеризующие чрезвычайную ситуацию за объектами возможных чрезвычайных ситуаций, стратегический метод по сути дела правильно поставленный статистический учёт наблюдения за объектами и территориями на которых могут произойти чрезвычайные ситуации сопровождаемые негативными последствиями.

Все предложенные затраты, представленные в карте, можно разделить на три группы: затраты до возникновения, во время возникновения и после возникновения чрезвычайной ситуации. [1] Предложенная карты является неотъемлемой частью метода цикличного управления рисками с экономической составляющей каждого этапа. [2, p.240] Позволяет определить необходимые затраты как на этапе планирования и подготовки, определить ущерб на этапе реагирования и необходимое количество финансовых средств на этапе восстановления.

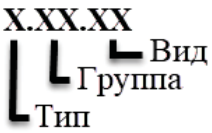
Представленная к рассмотрению карта не претендует на то, что она является полной для всех возможных чрезвычайных ситуаций, возникающих в результате

жизнедеятельности человека, она базируется только на чрезвычайные ситуации природного и техногенного характера, которые могут произойти на территории страны.

Полный список чрезвычайных ситуаций, который могут произойти на территории Республики Молдова отражён в Постановлении Правительства Nr. 1076 от 16.11.2010, в разработке которого автор принимал непосредственное участие.

Как показывает классификатор на территории страны могут происходить все типы чрезвычайных ситуаций за исключением цунами и вулканов. Отсутствие этих типов чрезвычайных ситуаций обусловлено географическим расположением страны.

Структурно классификатор построен трёх уровневым по десятичной системе.



Первая цифра, это **ТИП** чрезвычайной ситуации, в состав входит три основных типа чрезвычайных ситуаций:

1 – чрезвычайные ситуации техногенного характера;

2 – чрезвычайные ситуации природного характера;

3 – чрезвычайные ситуации биолого-социального характера:

Второй уровень определяет **ГРУППУ** чрезвычайной ситуации. К третьему уровню относится **ВИД** чрезвычайной ситуации.

К примеру, **транспортные аварии на мостах и железнодорожных переездах** – определён номер – 1.1.7 – это расшифровывается как чрезвычайная ситуация техногенного характера, группа Транспортных аварий (катастроф), вида аварии на мостах и железнодорожных переездах.

Собрав воедино все представленные виды ущерба, получается реальная экономическая картина приемлемая к одному из видов чрезвычайных ситуаций природного и техногенного характера.

На данный момент нет единых методик расчёта косвенного ущерба, это направление подлежит детальному изучению с созданием единого подхода получения реальных экономических результатов. На данный момент прослеживается прямая зависимость от ценностей, поддерживаемых в определённом обществе, которые влияют на получение реальных экономических результатов, приводя их к различным количественным данным.

Проанализировав полученные экономические данные предложенной карты можно с уверенностью 100% утверждать, что затраты, связанные с предупреждением чрезвычайных ситуаций, будут составлять не более 20% от суммы всего ущерба. Этот доход должен ложиться в основу составления годового бюджета, направленного на защиту граждан и территории от природных и техногенных катастроф, а также определение необходимой суммы для финансирования служб экстренного реагирования.

Применяя к данному методу закон Парето, верно, следующее утверждение: - Выделение денежных средств из бюджета, на предупреждение от чрезвычайных ситуаций, в размере 20% от полного ущерба за прошлый период, позволить уменьшит сумму полного ущерба на 80% в текущий момент времени.

Или обратное утверждение, для того чтобы уменьшить на 80% сумму полного материального ущерба, необходимо выделить всего лишь 20% от суммы нанесённого ущерба от чрезвычайной ситуации за прошлый финансовый период.

В целях эффективного использования средств государственного бюджета, а также достижения положительных социально-экономических эффектов, необходимо закладывать в бюджет на следующий период средства, направленные на развитие и поддержание сил реагирования на чрезвычайные ситуации и их последствий, сумму не менее 20% от суммы материального ущерба за прошлый период. В эту сумму не должен быть включен фонд заработной платы и обязательные государственные налоги.

В то же время необходимо разработать и отобрать инвестиционные проекты, направленные на уменьшение последствий от чрезвычайных ситуаций. Такое утверждение базируется на данных, представленных в классификаторе. Это связано с тем, что есть типы чрезвычайных ситуаций, для которых не существует методик и практик, где силы экстренного реагирования могут на прямую воздействовать для уменьшения пагубного влияния происходящих процессов. К примеру, землетрясения, засуха или сильные циклоны сопровождающееся сильным ветром и выпадением большого количества осадков и т.д. В эти случаях силы экстренного реагирования направляют на ликвидацию последствий. Если взять, к примеру засуху, то единственное с чем сталкиваются силы реагирования при проявлении такого природного явления это борьба с пожарами.

Но, чтобы не допустить потери урожая, например, в период засухи необходимо на государственном уровне внедрить проекты по ирригации сельскохозяйственных земель. Эти инвестиции не входят в компетенцию сил экстренного реагирования, они относятся к другим отраслевым министерствам. Основной целью предложенных инвестиций это помощь в формировании и укреплении существующих центров социально экономического развития их территориально производственных и туристических зон.

ВЫВОДЫ

Предложенный метод расчёта позволит достоверно, наиболее точно определить сумму полного ущерба для чрезвычайных ситуаций техногенного и природного характера. Системный подход в определение полного ущерба поможет находить правильные решения при реагировании на возникшие чрезвычайные ситуации так и на существенное сокращение пагубного влияния на экономическое и политическое составляющие региона.

БИБЛИОГРАФИЯ

1. Авдотьин В.П.; Дзыбов М.М. Оценка ущерба от чрезвычайных ситуаций природного и техногенного характера. Монография; МЧС России. М.: ФГБУ ВНИИ ГОЧС (ФЦ), 2012. 468 с.
2. Пянковский С.П., Информационная поддержка системы принятия решений в чрезвычайных ситуациях, Родзинка-2019, Черкаси : ЧНУ ім. Б. Хмельницького, 2019, стр. 240
3. Самсонов К.П., д.э.н., ГУ ИМЭИ, Методология оценки экономического ущерба от чрезвычайных ситуаций природного и техногенного характера. 2012, МЧС России, 2012, 7 с.
4. Peancovschii S. *Mobile situational center for prevention and reduction of emergency situations (Centrul mobil de comandă pentru lichidarea situațiilor excepționale)*, Economics, Social and Engineering Sciences Year 2, Nr.3-4/2019, Chișinău 2019, p.254.

THE MECHANISM FOR MANAGING THE ECONOMIC SECURITY OF INDUSTRIAL ENTERPRISES IN THE CONTEXT OF THE SPREAD OF INDUSTRY 4.0

МЕХАНИЗМ УПРАВЛЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В УСЛОВИЯХ РАСПРОСТРАНЕНИЯ ИНДУСТРИИ 4.0

Куценко Дмитрий
Аспирант, Черкасский Национальный Университет им. Богдана Хмельницкого
e-mail: lawagens@gmail.com

Зачёсова Наталия
Доктор экономических наук, профессор
Черкасский Национальный Университет им.Богдана Хмельницкого
e-mail: natazachosova@gmail.com

Abstract
The relevance of the study is explained by the need to find ways to adapt the existing mechanisms for managing economic security to the realities of the development of the external and internal environment for the functioning of business entities. This primarily concerns industrial enterprises, which are especially influenced by the trends of Industry 4.0. Rebuilding production processes requires the modernization of all management processes, including the process of economic security management. Purpose. The aim of the study was to determine the necessary directions for the adaptation of mechanisms for managing the economic security of industrial enterprises to ensure effective counteraction to the risks of Industry 4.0. Research methods. The research methods were theoretical analysis and content analysis of materials devoted to the problems of strategic management and economic security management, as well as the generalization method, which was used to develop the author's proposals and conclusions based on the results of the research conducted. Results. The problems of functioning of industrial enterprises in the conditions of the spread of Industry 4.0 and possible risks for the state of their economic security in a strategic perspective are identified. Proposals were made regarding the transformation of the structure and functioning of the mechanism for managing economic security in new conditions for enterprises.

Keywords: *economic security, industrial enterprise, Industry 4.0, management, risk.*

JEL Classification: *D0, M1, M21*

1. ПРОБЛЕМЫ ФУНКЦИОНИРОВАНИЯ ПРОМЫШЛЕННЫХ ПРЕДПРИЯТИЙ В УСЛОВИЯХ РАСПРОСТРАНЕНИЯ ИНДУСТРИИ 4.0 И ВОЗМОЖНЫЕ РИСКИ ДЛЯ СОСТОЯНИЯ ИХ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ В СТРАТЕГИЧЕСКОЙ ПЕРСПЕКТИВЕ

Проблемы обеспечения экономической безопасности на микроуровне все чаще поднимаются в публикациях современных исследователей [Babina N. & Zanora V., 2018, Herasymenko O. & Shevchenko A., 2018, Koval O., 2020]. Авторами этой публикации так же совершались попытки усовершенствования теоретических основ стратегического и тактического управления экономической безопасностью бизнес-структур [Zachosova N., 2018, Kutsenko D., 2019]. Материалы проведенных ранее исследований показали, что существует ряд проблем функционирования промышленных предприятий в условиях распространения Индустрии 4.0, которые в целом можно систематизировать в такой список: отсутствие ресурсов для обновления активов и внедрения инноваций, низкий уровень информационной

грамотности персонала для работы в условиях цифровой экономики, чрезмерная продолжительность производственных циклов, высокий уровень брака, несоответствие продукции мировым стандартам качества и современным требованиям клиентов, низкий уровень технологичности и экологичности отдельных производственных процессов, отсутствие у персонала мотивации к развитию и поддержке уровня безопасности.

Закономерно, что новые условия функционирования, изменения внешней и внутренней среды существования предприятий формируют новый набор рисков для состояния их экономической безопасности: кадровые риски, информационные риски, технико-технологические риски, правовые риски и репутационные риски. Влияние последних будет особенно ощутимо в стратегической перспективе.

2. ТРАНСФОРМАЦИИ СТРУКТУРЫ И ФУНКЦИОНИРОВАНИЯ МЕХАНИЗМА УПРАВЛЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ В НОВЫХ ДЛЯ ПРЕДПРИЯТИЙ УСЛОВИЯХ

Под механизмом управления экономической безопасностью предприятия понимаем совокупность элементов, причинно-следственных и функциональных связей между ними, которые используются с целью организации системы защиты корпоративных ресурсов и интересов компании от пагубного влияния на их состояние и результат их использования внешних и внутренних угроз и опасностей и их последствий, а также на обеспечение беспрерывности производственных и других бизнес-процессов в условиях существования различных рисков. Современные механизмы управления экономической безопасностью промышленных предприятий имеют такие особенности, как ориентация на физическую защиту активов и персонала, контроль безопасности труда во время производственного процесса, защита коммерческих секретов и информации с ограниченным доступом, ресурсное содействие в конкурентной борьбе.

В условиях Индустрии 4.0 конкурентные преимущества промышленных предприятий определяются его инновационностью, способностью к минимизации используемых ресурсов, политикой работы со стейкхолдерами, финансовой и экономической независимостью в сочетании со способностью привлекать инвестиции для быстрой модернизации производственных процессов. Также конкурентным преимуществом становится персонал, пусть даже не обладающий должным опытом работы, но готовый быстро и интенсивно обучаться, гибко реагировать на изменения. Учитывая все перечисленное, механизм управления экономической безопасностью в условиях Индустрии 4.0 должен сочетать в себе возможность способствовать достижению стратегических целей предприятия и стремительно запускать защитные протоколы и процедуры на тактическом уровне в ответ на новые вызовы.

Наши предложения по трансформации структуры и функционирования механизма управления экономической безопасностью промышленных предприятий в новых экономических условиях таковы: необходимо от физической защиты активов перейти в плоскость организации киберзащиты цифровых ресурсов, переключится от фрагментарности защитных действий к беспрерывности и комплексности защитных мероприятий и от компенсации убытков и резервирования финансовых ресурсов на эти цели – к подготовке персонала к вовлечению в процессы обеспечения экономической безопасности.

ВЫВОДЫ

В условиях перехода к цифровой экономике и интернету вещей невозможно обеспечить для предприятия состояние экономической безопасности, пользуясь традиционными подходами. Физическая защита ресурсов и финансовая компенсация последствий проявления рисков, которые до сих пор были положены в основу функционирования механизма управления экономической безопасностью промышленных предприятий – более не дают необходимого эффекта. Поэтому пора разрабатывать и внедрять механизмы комплексной цифровой и киберзащиты, а также обеспечить всеобщее участие (персонала, клиентов, других категорий стейкхолдеров) в процессах управления экономической безопасности компании с целью предупреждения влияния угроз, а не минимизации их последствий.

БИБЛИОГРАФИЯ

1. Zachosova N., Babina N., Zanora V. Research and methodological framework for managing the economic security of financial intermediaries in Ukraine. Banks and Bank Systems, 2018, 13, 4, 119-130.
2. Zachosova N., Herasymenko O., Shevchenko A. Risks and possibilities of the effect of financial inclusion on managing the financial security at the macro level. Investment Management & Financial Innovations, 2018, № 15 (4), 304-319.
3. Koval O.V. Strategic management of economic security system of business entities: theoretical aspects. Bulletin of the Cherkasy National University. Economic Sciences, 2020, 1, 40-47.
4. Kutsenko D. Orienters of strategic management of financial and economic security of enterprises: interests, challenges, risks. Bulletin of the Cherkasy Bohdan Khmelnytsky National University. Economic Sciences, 2019, № 2, 50-58.

AREAS OF STRATEGIC MANAGEMENT OF BUSINESS ENTITIES` ECONOMIC SECURITY: RISKS AND OPPORTUNITIES

НАПРАВЛЕНИЯ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ: РИСКИ И ВОЗМОЖНОСТИ

Коваль Алексей
Аспирант, Черкасский Национальный Университет им.Богдана Хмельницкого
e-mail: oleksii.koval.aba@gmail.com

Зачёсова Наталия
Доктор экономических наук, профессор
Черкасский Национальный Университет им.Богдана Хмельницкого
e-mail: natazachosova@gmail.com

Abstract
The relevance of the research is explained by the need to develop effective strategies for maintaining the level of economic security of enterprises and other business structures in the long term. In the context of the influence of numerous risks on the financial and economic state of economic entities, the long-term planning of the results of their activities and the foresight of financial indicators become a problematic management aspect. In view of this, it becomes necessary to develop theoretical and methodological approaches to strategic economic security management of business. Purpose. The aim of the study is to search for directions of strategic economic security management of business entities, to identify strategic risks for the efficient and profitable functioning of enterprises and to characterize the opportunities for business entities whose top management decides on the implementation of strategic economic security management. Research methods. The research methods were theoretical analysis and content analysis of materials devoted to the problems of strategic management and economic security management, as well as the generalization method, which was used to develop the author's proposals and conclusions based on the results of the research conducted. Results. As a result of the study, it was possible to substantiate the need for strategic economic security management of business and describe its directions; to identify strategic risks to the economic security of enterprises; and to make assumptions about the benefits that strategic management of economic security will bring to the business.

Keywords: *economic security, management, risk, strategy, threat.*

JEL Classification: *D0, M1, M21*

1. НЕОБХОДИМОСТЬ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ БИЗНЕСА И ЕГО НАПРАВЛЕНИЯ

Эффективное стратегическое управление бизнесом имеет своей целью максимально точное (с учетом возможных изменений внешней и внутренней среды функционирования субъектов хозяйствования) определение долгосрочных векторов его развития и путей достижения установленных перспективных ориентиров, а также прогноз необходимых для этого ресурсов. Имеет место разница в позициях и взглядах теоретиков и практиков, которые занимаются проблемами стратегического планирования. Первые стараются разработать методы повышения достоверности долгосрочных прогнозов показателей предприятий для того, чтобы обеспечить управленческий персонал релевантной информацией для принятия верных стратегических решений. Менеджеры субъектов бизнеса, в свою очередь, ориентированы на разработку стратегий деятельности предприятий, конкретные

действия в рамках которых могут гибко реагировать на изменения экономической ситуации. В то же время, и теоретики, и практики сходятся во мнении о необходимости своевременного определения рисков для финансового состояния, конкурентной способности и в целом для экономической безопасности бизнеса, поскольку именно их существование, трансформация с течением времени, активизация и диверсификация влияют на точность прогнозов, вызывают необходимость пересмотра стратегических ориентиров, приводят к негативным экономическим и финансовым последствиям, например, к перерасходу ресурсов, недополучению ожидаемых доходов, падению уровня конкурентных преимуществ, снижению деловой репутации, конфликтов со стейкхолдерами и т.д.

Авторами этого исследования [Zachosova N., 2018, 2020; Koval O., 2020], а также другими исследователями проблем обеспечения экономической безопасности на микроуровне [Kutsenko D., 2019, 2020] уже совершались попытки доказать необходимость стратегического управления именно экономической безопасностью субъекта хозяйствования как одного из важных, а главное – самостоятельных направлений современного менеджмента, обладающего собственной методологической базой и особенностями реализации на практическом уровне. Стратегическое управление экономической безопасностью – это спектр действий, направленных на долгосрочное планирование работы предприятия в таком ритме и в таких направлениях, которые гарантируют безопасность его активов при эффективном их использовании с целью достижения собственных целей предприятия и максимального удовлетворения интересов его стейкхолдеров. Необходимость стратегического управления экономической безопасностью объясняется следующим:

- долгосрочное планирование защитных мероприятий и необходимых для них ресурсов позволит избежать лишних расходов и, в случае проявления угрозы, быть готовым компенсировать убытки от ее влияния;

- координация стратегических целей функционирования предприятия с целями обеспечения его экономической безопасности позволит предупредить конфликт интересов основных категорий стейкходлеров;

- организация действий по обеспечению экономической безопасности в стратегической перспективе позволит лучше понять существующие проблемы в структуре построения ее системы и в механизме управления ею, и таким образом, позволит своевременно модернизировать и адаптировать архитектонику системы экономической безопасности предприятия;

- необходимость вовлечения персонала бизнес-структуры в процессы обеспечения экономической безопасностью на всех уровнях управления требует пересмотра кадровой политики и подготовку сотрудников компаний, их обучения, мотивации к новой форме поведения в условиях нарастающих рисков, и т.д.; выполнение этой задачи требует времени, поэтому успех решения кадровой проблемы состоит в возможности пересмотра генеральной стратегии и внесения нового стратегического ориентира в цели компании – формирование кадрового резерва, способного к поддержанию уровня экономической безопасности в процессах выполнения своих обязанностей;

- требования к информационной открытости компаний склоняют к стратегическому подходу в принятии решений относительно того, в каком направлении будет развиваться транспаретность бизнеса и как именно это может повлиять на его экономическую безопасность, в том числе, и в долгосрочной перспективе, так как определенные риски могут не стразу проявиться и имеют

отложенный момент негативного результата (например, слухи, понижающие уровень деловой репутации предприятия могут через определенное время привести к потере клиентов и постоянных партнеров).

Таким образом, направления стратегического управления экономической безопасностью можно очертить, как:

- стратегическое планирования путей управления угрозами экономическому состоянию компании и их последствиями (в том числе финансовое планирование компенсации причиненных ими убытков или недополученных доходов);
- стратегическое управление рисками и управление стратегическими рисками с целью повышения вероятности положительного результата для хозяйствующего субъекта от их существования и с целью минимизации проявления их негативных последствий (в том числе разработка плана по использованию инструментария идентификации, систематизации, классификации, каталогизации рисков, их оценивания и выбора стратегии управления рисками (уклонения, передачи, избегания, принятия, диверсификации);
- разработка стратегии формирования кадрового резерва, способного к работе в условиях появления все новых рисков, опасностей, угроз, и готового нести ответственность за свои действия, идущие в разрез с принятой политикой безопасности компании;
- разработка стратегии поиска и привлечения ресурсов с минимальным риском потери компанией финансовой и экономической независимости;
- оценивание инвестиционных планов и программ на предмет соотношения потенциальных доходов и возможных убытков в ситуации реализации инвестиционных рисков и проявления их последствий, и влияние такой ситуации на уровень экономической безопасности в будущем;
- разработка стратегии безопасной информационной политики компании, которая будет сочетать в себе готовность быть максимально открытыми для клиентов и стейкхолдеров, и при этом сохранять высокий уровень защиты от несанкционированного доступа к базам данных, коммерческим тайнам и корпоративным секретам бизнес-процессов хозяйствующего субъекта.

2. СТРАТЕГИЧЕСКИЕ РИСКИ ДЛЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

Можно предложить такой ориентировочный перечень стратегических рисков для экономической безопасности, который является универсальным для субъектов хозяйствования различных видов экономической деятельности: появление на рынке товаров-субститутов (или услуг-аналогов), которые стоят дешевле и удовлетворяют более широкий спектр потребностей клиентов; появление на рынке новых конкурентов (например, европейских компаний) с высоким уровнем деловой репутации и известным в мире брендом; изменение цен на ключевые ресурсы, сырье, материалы, комплектующие детали; необходимость временного прекращения финансово-хозяйственной деятельности или ее быстрой адаптации к новым условиям (например, в условиях пандемии и установления карантина); изменение валютных курсов (особенно ощутимым этот риск является для импортеров и экспортеров товаров и услуг); появление инноваций и ноу-хау, внедрение которых будет требовать коренной трансформации хозяйственных процессов; изменение государственной политики в отрасли, в которой работает субъект хозяйствования; диджитализация экономических отношений в различных сферах.

Идентифицировать стратегические риски и искать эффективные методы и пути противодействия их негативному влиянию управленческому персоналу стоит

на этапе разработки или избрания стратегии для деятельности предприятия в целом и обеспечения его экономической безопасности в частности, а также в процессе реализации стратегий через механизмы динамического изменения ее отдельных положений в соответствии новым вызовам среды функционирования предприятия.

3. ПРЕИМУЩЕСТВА ДЛЯ БИЗНЕСА ОТ СТРАТЕГИЧЕСКОГО УПРАВЛЕНИЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТЬЮ

Грамотное стратегическое управление экономической безопасностью гарантирует бизнесу различные и многочисленные преимущества перед конкурентами. Наличие стратегии обеспечения экономической безопасности позволяет организовать и реализовать процесс предсказания потенциальных рисков, которые будут характерны для предприятия в будущем, учитывая его курс к достижению конкретных стратегических ориентиров на основе идентификации имеющихся для его деятельности рисков; будет способствовать правильной их каталогизации и прогнозированию их вероятного как положительного, так и отрицательного влияния на экономическое состояние предприятия и поможет в разработке тактических методов управления рисками средствами системы обеспечения финансово-экономической безопасности для минимизации их нежелательных последствий для целостности и эффективности использования корпоративных ресурсов компании. Кроме того, неоспоримыми преимуществами станет наличие различных сценариев (оптимистического, реалистического и пессимистического) поведения бизнеса в соответствии с экономическими условиями, которые сложатся в обозримом будущем, наличие каталогов управленческих решений (планов, как действовать в случае проявления той или иной угрозы, какими инструментами и при помощи каких ресурсов уменьшать ее влияние на состояние компании и ее активов); формирование культуры управления рисками среди персонала компании, что позволит уменьшить количество кадровых рисков и улучшит понимание ценностей компании.

ВЫВОДЫ

Необходимость стратегического управления экономической безопасностью бизнеса объясняется важностью рационального долгосрочного планирования защитных мероприятий для охранения целостности активов и корпоративных ресурсов компании, потребностью в координации стратегических целей функционирования предприятия с целями обеспечения его экономической безопасности с тем, чтобы агрессивная модель управления субъектом хозяйствования в погоне за дополнительной прибылью не привела к возникновению таких угроз, результатом которых может стать полное прекращение его работы, банкротство, ликвидация; значимостью организации действий по обеспечению экономической безопасности в стратегической перспективе для достижения генеральных целей функционирования и развития компании; необходимостью вовлечения персонала бизнес-структуры в процессы обеспечения экономической безопасностью на всех уровнях управления, поскольку комплексное обеспечение экономической безопасности компании возможно лишь в том случае, если действия каждого сотрудника будут осуществляться с полным осознанием тех рисков, которые их сопровождают, и тех угроз, которые они могут собой нести; возрастанием требований к информационной открытости деятельности компаний, которые призывают топ-менеджмент предприятий к такому уровню транспарентности, который может стать угрожающим для уровня

конкурентоспособности компании, ее финансового состояния, рыночной стоимости, деловой репутации.

Основными стратегическими рисками для экономической безопасности являются: появление на рынке товаров-субститутов, появление на рынке новых конкурентов или усиление рыночных позиций компаний, которые и ранее были основными конкурентами, изменение цен на ключевые ресурсы, сырье, материалы, комплектующие детали, необходимость временного прекращения финансово-хозяйственной деятельности или ее быстрой адаптации к новым условиям, рискам, угрозам, изменение валютных курсов, появление инноваций и ноу-хау, внедрение которых будет требовать коренной трансформации хозяйственных процессов, изменение государственной политики в сфере, в которой работает компания, диджитализация экономических отношений в различных сферах.

Преимущества для бизнеса от стратегического управления экономической безопасностью состоят в предвидении и своевременном предупреждении угроз, рисков и их последствий, установлении баланса между уровнем удовлетворения интересов различных категорий стейкхолдеров; избежании противоречий между целями обеспечения экономической безопасности компании и ее генеральными целями в долгосрочной перспективе; формировании механизма комплексного управления экономической безопасностью на основе подготовленного и вовлеченного в бизнес-процессы персонала, который хорошо ориентируется в вопросах безопасности.

БИБЛИОГРАФИЯ

1. Zachosova N., Babina N., Zanora V. Research and methodological framework for managing the economic security of financial intermediaries in Ukraine. Banks and Bank Systems, 2018, 13, 4, 119-130.
2. Zachosova N., Kutsenko D., Koval O., Kovalenko A. Financial and economic security management in the digital economy: aspects of strategic, personnel, project and risk management. India, Ukraine, Brazil & Greater Mekong Subregion. International Conference – 2020, IUBGMS, 2020. Global Challenges and Threats to National Economies Nowadays, 39-41.
3. Kutsenko D. Orienters of strategic management of financial and economic security of enterprises: interests, challenges, risks. Bulletin of the Cherkasy Bohdan Khmelnytsky National University. Economic Sciences, 2019, 2, 50-58.
4. Koval O.V. Strategic management of economic security system of business entities: theoretical aspects. Bulletin of the Cherkasy National University. Economic Sciences, 2020, 1, 40-47.

PROBLEMS OF PERSONNEL SECURITY MANAGEMENT IN THE SYSTEM OF ENSURING THE FINANCIAL AND ECONOMIC SECURITY OF BUSINESS STRUCTURES

ПРОБЛЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ В СИСТЕМЕ ОБЕСПЕЧЕНИЯ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ БИЗНЕС-СТРУКТУР

Коваленко Андрей
Аспирант, Черкасский Национальный Университет им.Богдана Хмельницкого

Зачёсова Наталия
Доктор экономических наук, профессор
Черкасский Национальный Университет им. Богдана Хмельницкого
e-mail: natazachosova@gmail.com

Abstract
Personnel security is one of the components of the financial and economic security of a business. The staff carries security threats, and at the same time acts as a resource that requires protection from all kinds of risks. Personnel policy is able to resolve issues of personnel security management. Purpose. The purpose of the study is to develop proposals for solving problems of personnel security management in the system of ensuring the financial and economic security of business structures. Research methods. The research methods were theoretical analysis and content analysis of materials devoted to the problems of strategic management and economic security management, as well as the generalization method, which was used to develop the author's proposals and conclusions based on the results of the research conducted. Results. The problems of managing the personnel security of the enterprise at different stages of work with personnel are identified. The influence of employees on the state of financial and economic security has been substantiated. The role of the personnel policy of the enterprise in relation to countering the personnel risks of an economic entity is determined.

Keywords: *business structure, economic security, management, personnel, personnel policy, risk.*

JEL Classification: *D0, M1, M21*

1. ПРОБЛЕМЫ УПРАВЛЕНИЯ КАДРОВОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ НА РАЗНЫХ ЭТАПАХ РАБОТЫ С ПЕРСОНАЛОМ

Проблемы обеспечения кадровой безопасности являются частью исследований проблематики управления финансово-экономической безопасностью бизнес-структур, которая прослеживается в публикациях современных ученых [Babina N. & Zanora V., 2018, Kutsenko D., 2019, Koval O., 2020]. Авторами этого исследования так же рассматривались различные аспекты как управления экономической безопасностью в целом [Zachosova N., 2018], так и в рамках функционирования подсистемы кадровой безопасности хозяйствующих структур [Kovalenko A., 2020]. Неоспоримым является тот факт, что отсутствие механизмов управления кадровой безопасностью непременно приводит возникновению конфликтных ситуаций в коллективе, к перерасходу ресурсов, случаям воровства, непродуктивной трате рабочего времени, и в целом к действиям или бездействиям персонала, которые способны причинить компании убытки, как материальные, так и репутационные, что приведет к снижению уровня ее финансово-экономической безопасности.

Менеджеры предприятий, которые ставят перед собой цель упорядочить действия по защите персонала от рисков и по защите самой бизнес-структуры от рисков со стороны сотрудников, в единую систему или механизм, приходят к пониманию, что проблемы управления кадровой безопасностью предприятия возникают на разных этапах работы с персоналом. Так, в момент собеседования с потенциальным работником сотрудник отдела кадров может не рассмотреть признаки его склонности к девиантному поведению, а сам кандидат может оказаться завербованным конкурентами «разведчиком». На этапе адаптации сотрудника к условиям работы им могут быть намеренно или по незнанию нарушены правила техники безопасности. На этом этапе также часто неэффективно используется рабочее время, неправильно исполняются должностные обязанности, возникают конфликты с другими сотрудниками и в первую очередь с наставниками. Во время рабочего процесса количество рисков является максимальным – это и инсайдерство, и вредительство, и срыв бизнес-процессов, и порча активов компании. На этапе увольнения персонала можно ожидать, что бывший сотрудник будет требовать компенсацию, инициировать конфликты, а после увольнения станет плохо отзываться о компании, угрожая ее репутации, а также разглашать информацию, которая была предназначена для внутреннего пользования.

2. ВЛИЯНИЕ РАБОТНИКОВ НА СОСТОЯНИЕ ФИНАНСОВО-ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ И РОЛЬ КАДРОВОЙ ПОЛИТИКИ ПРЕДПРИЯТИЯ ОТНОСИТЕЛЬНО ПРОТИВОДЕЙСТВИЯ КАДРОВЫМ РИСКАМ ХОЗЯЙСТВУЮЩЕГО СУБЪЕКТА

Влияние работников на состояние финансово-экономической безопасности сложно переоценить. Именно их действия определяют, насколько эффективно будут использоваться ресурсы предприятия, каков будет результат от бизнес-процессов, какие риски и угрозы будут своевременно идентифицированы и предупреждены. Кадровая политика, путем конкретизации проработанных сценариев поведения сотрудника в той или иной ситуации позволяет сформировать правильную, ориентированную на безопасность модель обращения работника с активами компании, ее клиентами, партнерами и другими стейкхолдерами, понимать миссию компании и необходимость высокого уровня финансово-экономической безопасности для ее достижения, собственную роль и значимость в этом процессе. Крайне важно заложить в кадровую политику инструменты стимулирования персонала к ответственному поведению и бережному отношению к материальным ресурсам компании. Полезно будет четко и конкретно продемонстрировать, как именно интересы компании и собственные интересы сотрудника связанны, и как достижение первых положительно скажется на его служебном положении или финансовом благосостоянии. Структурно, кадровая политика должна содержать разделы, посвященные определению кадровых рисков на каждом этапе работы с персоналом, причем как тех, которые от него исходят, так и тех, которые на него влияют, раздел инструкций для менеджеров по работе с персоналом, раздел сценариев поведения персонала в той или иной ситуации, раздел мотивации персонала, раздел стратегии развития кадрового потенциала и раздел обеспечения кадровой безопасности.

ВЫВОДЫ

Эффективное управление кадровой безопасностью позволяет существенно снизить кадровые риски и убытки бизнес-структуры от их влияния на состояние ее финансово-экономической безопасности. Удобнее всего для компании начать управление кадровой безопасностью с разработки ориентированной на управление кадровыми рисками кадровой политики. Этот документ должен быть полностью транспарентен, знаком и понятен каждому сотруднику. Вариант управления безопасностью, когда каждый работник осознает свою значимость, свою сферу ответственности, ценности компании и необходимость защищать ее интересы, так как они неразрывно связанны с его собственными, является не только наиболее эффективным, но и требует наименьшее количество ресурсов, поскольку кадровые риски снижаются путем их предупреждения со стороны самого источника риска, а не посредствам финансирования мер противостояния им и компенсации убытков от их проявлений.

БИБЛИОГРАФИЯ

1. Zachosova N., Babina N., Zanora V. Research and methodological framework for managing the economic security of financial intermediaries in Ukraine. Banks and Bank Systems, 2018, 13, 4, 119-130.
2. Kovalenko A. Personnel security as an element of human resources (personnel) policy in the economic and financial security system of the business entity. European journal of economics and management, 2020, Volume 6, Issue 1, 100-106.
3. Koval O.V. Strategic management of economic security system of business entities: theoretical aspects. Bulletin of the Cherkasy National University. Economic Sciences, 2020, 1, 40-47.
4. Kutsenko D. Orienters of strategic management of financial and economic security of enterprises: interests, challenges, risks. Bulletin of the Cherkasy Bohdan Khmelnytsky National University. Economic Sciences, 2019, 2, 50-58.

THE CONFERENCE INTERNATIONAL SCIENTIFIC COMMITTEE:

Tomșa Aurelia, *PhD, Associate Professor, head of the Economic Theory and Policy department, Academy of Economic Studies of Moldova*

Ignatiuc Diana, *PhD, Associate Professor, department Economic Theory and Policy, Academy of Economic Studies of Moldova*

Barbăneagră Oxana, *PhD, Associate Professor, department Economic Theory and Policy, Academy of Economic Studies of Moldova*

Bucos Tatiana, *PhD, Associate Professor, department Economic Theory and Policy, Academy of Economic Studies of Moldova*

Ohrimenco Serghei, *Phd hab., Professor, Laboratory of Information Security, Academy of Economic Studies of Moldova*

Pirașca Grigore, *PhD, Associate Professor, Dean of the Faculty of Theoretical and Applied Economics, Bucharest Academy of Economic Studies*

Zachosova Natalia, *PhD, Professor, Bohdan Khmelnytsky National University of Cherkasy*

Golubev Vladimir, *PhD, Director of the Computer Crime Research Center*

Kulikova Elizaveta, *Lecturer, Odessa National Economic University*

Bochulia Tetiana, *PhD, Professor, Kharkiv State University of Food Technology and Trade*

Velev Dimiter, *PhD, Prof., University of National and World Economy*

Varadzhakova Desislava, *PhD, Bulgarian Academy of Sciences*

Angelova Polya, *PhD, Vice-Rector for Science and Staff Development of the D.A. Tsenov Academy of Economics, Svishtov*

Leszek Fryderyk Korzeniowski, *prof. nadzw. dr hab., president European Associationfor Security*

Maria Urbaniec, *DSc, Professor, Department of Entrepreneurship and Innovation of the Cracow University of Economics*

Gojayeva Elmira Mahammad, *PhD, Associate Professor, Azerbaijan Tourism and Management University*

Bazhenova Elena, *Associate Professor, Institute for Sociology and Regional Studies, Southern Federal University*

Pugacheva Olga, *PhD, Associate Professor, Gomel State University, Francisk Skorina*

Čekerevac Zoran, *DSc, Professor, "UNION-Nikola Tesla" University in Belgrade, Faculty of Business and Law, Belgrade-Mladenovac*

Online International Scientific-Practical Conference ”Economic Security in the Context of Sustenable Development”, December 11, 2020

Conference organizer:

Department of Economic Theory and Policy, Academy of Economic Studies of Moldova, www.ase.md

Conference co-organizers:

Chamber of Commerce and Industry of the Republic of Moldova, www.chamber.md

Bucharest Academy of Economic Studies, www.ase.ro

Tsenov Academy of Economics, www.uni-svishtov.bg

Computer Crime Research Center, www.crime-research.org