

INSTRUMENTE DE VERIFICARE A INFORMAȚIEI FALSE DISTRIBUITE PE WEB

<https://doi.org/10.52673/18570461.21.2-61.02>
CZU:32.019.51:004

Doctorandă **Adela GOREA**

E-mail: adela.gorea@usarb.md

ORCID: <https://orcid.org/0000-0002-2912-4686>

Universitatea de Stat „Alec Russo” din Bălți

TOOLS FOR VERIFICATION OF THE FALSE INFORMATION DISTRIBUTED ON WEB

Summary. The article contains details on technologies for assessing the credibility of information on the Web. Special attention is paid to social networks and to the most important aspects of the distribution of incredible information on the Internet. The paper analyzes the basic features of several tools for verifying the credibility of the Web sources. Given that Web tools mostly check the content of sites, but not whether the Web address of the site is real, Web address verification technologies have been researched. Necessary suggestions were made in checking the site before you start reading the information on the Web.

Keywords: credibility, Web, social networks, fake sites, phishing.

Rezumat. Articolul conține detalii cu privire la tehnologiile de evaluare a credibilității informațiilor de pe Web. O atenție specială se acordă rețelelor de socializare și celor mai importante aspecte ale distribuției informației necredibile de pe Internet. Lucrarea analizează caracteristicile de bază ale mai multor instrumente pentru verificarea credibilității surselor Web. Având în vedere că instrumentele Web verifică preponderent conținutul site-urilor, dar nu și dacă adresa Web a site-ului este reală, s-au cercetat tehnologiile de verificare a adreselor Web. S-au făcut sugestii necesare pentru verificarea site-ului înainte de a începe citirea informațiilor de pe Web.

Cuvinte-cheie: credibilitate, web, rețele sociale, site-uri false, phishing.

INTRODUCERE

Odată cu dezvoltarea mediilor on-line și cu apariția Internetului, considerat un spațiu democratic, a devenit mult mai simplu pentru oricine să se exprime liber, oricând și oricum. Dincolo de instituțiile de presă, fiecare cu politicile editoriale proprii și cu diverși factori care decid dacă un eveniment poate sau nu poate fi transformat în știre, au apărut și multe site-uri care se prezintă în mediul on-line ca produse media, postând diverse conținuturi care pun însă la îndoială credibilitatea acestora. Iată de ce, atunci când suntem în punctul de a accepta sau de a respinge informații noi, ar trebui să ne întrebăm care este originea și reputația sursei.

În așa-numita „epoca reputației”, aprecierile critice ar trebui să fie direcționate nu către conținutul informațiilor, ci mai degrabă către rețeaua de socializare care a conturat acel conținut și care i-a oferit o anumită poziție meritat sau nemeritat în sistemul nostru de cunoaștere. Or, nu fiecare utilizator este capabil să facă o analiză și o definire a conținuturilor în credibile sau necredibile. Rețelele de social media sunt cele responsabile în primul rând de conținuturile distribuite și redistribuite zilnic de utilizatori, fără a fi verificate, creând deseori sentimente de panică și revoltă.

În acest articol sunt cercetate anumite aspecte în evaluarea credibilității informației de pe Web. Pornind de la scopul preconizat, lucrarea este structurată în câteva secțiuni. Inițial în articol sunt prezentate cele mai relevante aspecte ale rețelelor de socializare, care reprezintă cele mai frecvente instrumente de distribuire a informației pe Internet. Totodată, pornind de la exemplul rețelelor de socializare este definită noțiunea de credibilitate a informației și sunt tratate anumite aspecte ale acesteia. În continuare sunt prezentate câteva instrumente de verificare a credibilității surselor Web. Ținând cont de faptul că instrumentele în mare parte verifică conținutul de pe site-uri, dar nu și dacă adresa Web a site-ului este reală, s-au cercetat tehnologiile de verificare a adreselor Web. Cu atât mai importantă este verificarea adreselor Web cu cât prelucrarea informației de pe site, de cele mai dese ori nestructurată, necesită un efort sporit.

SPECIFICUL REȚELELOR MEDIA SOCIALE

Interesul pentru rețelele sociale crește continuu. De cele mai multe ori acestea constituie platforme pentru scrierea și distribuirea informațiilor textuale (gânduri, opinii, experiențe etc.), a conținuturilor

multimedia (imagini, filme, fișiere audio) create în timpul unor ocazii speciale în locații deosebite, iar scopul autorilor acestui content este de a-l comunica persoanelor aflate la distanță[1]. Cele mai populare rețele sociale sunt următoarele¹:

Blogurile – reprezintă platforme unde utilizatorii își pot expune gândurile, sentimentele, opiniile etc.

Facebook² este în prezent cea mai mare rețea socială din lume, cu peste 2,45 miliarde de utilizatori activi lunari, 1,62 miliarde de utilizatori activi zilnic, în 2020³. Este sugestiv faptul că 45 dintre utilizatori iau zilnic știri de pe Facebook, care generează 4 noi petabytes de date pe zi⁴.

Twitter⁵ este o platformă de rețea socială care permite utilizatorilor și grupurilor să posteze mesaje scurte (în limita de 140 de caractere). Acum există 1,3 miliarde de conturi Twitter, care trimit 500 de milioane de tweet-uri în fiecare zi⁶.

YouTube⁷ și **Vimeo**⁸ sunt utilizate pentru găzduirea și vizionarea de site-uri web. YouTube are în prezent 1,9 miliarde de utilizatori lunar și 500 de ore de videoclip sunt încărcate în fiecare minut⁹. În 2018 YouTube a fost cea mai descărcată aplicație de pe Apple app store¹⁰.

Flickr¹¹ este un site de găzduire a imaginilor și video. Din această rețea socială fotografiile pot fi partajate pe alte rețele sociale, cum ar fi Facebook și Twitter. Există peste 90 de milioane de utilizatori lunari care au distribuit peste 500 de milioane de imagini sub licența Creative Commons¹².

Instagram¹³ este o aplicație care permite utilizatorilor să partajeze fotografii și videoclipuri. Utilizatorii își pot procesa fotografiile și aplica filtre digitale și efecte speciale. În 2019, au existat 1 miliard de utilizatori activi și peste 40 de miliarde de fotografii au fost distribuite¹⁴. În 2018, Instagram este a doua aplicație după numărul de descărcări de pe Apple app store¹⁵.

¹<https://communications.tufts.edu/marketing-and-branding/social-media-overview/>

²<https://www.facebook.com/>

³<https://sproutsocial.com/insights/facebook-stats-for-marketers/>

⁴<https://www.brandwatch.com/blog/facebook-statistics/>

⁵<https://twitter.com/>

⁶<https://www.websitehostingrating.com/twitter-statistics/>

⁷<https://www.youtube.com/>

⁸<https://vimeo.com/>

⁹<https://www.brandwatch.com/blog/youtube-stats/>

¹⁰<https://blog.hootsuite.com/instagram-statistics/>

¹¹<https://www.flickr.com/>

¹²<https://expandedramblings.com/index.php/flickr-stats/>

¹³<https://www.instagram.com/>

¹⁴<https://www.brandwatch.com/blog/instagram-stats/>

¹⁵<https://blog.hootsuite.com/instagram-statistics/>

Snapchat¹⁶ este o aplicație mobilă care permite utilizatorilor să trimită fotografii și videoclipuri prietenilor sau să le adauge la „povestea” lor. Există 203 milioane de utilizatori activi zilnic, care postează în medie 3,5 miliarde de snap-uri zilnice¹⁷.

Grupurile **LinkedIn**¹⁸ este o rețea în care profesioniștii cu domenii similare de interes pot crea grupuri și împărtăși informații despre subiecte de interes. LinkedIn are peste 610 milioane de membri¹⁹, numărul total de grupuri LinkedIn este de peste 2 milioane, aici înregistrându-se 200 de discuții pe minut²⁰.

După cum am observat, cele mai populare rețele sociale subscriu perfect la scopul propus de a comunica cu persoanele aflate la distanță. Totodată, rețelele sociale constituie platforme excelente de pentru distribuirea știrilor din diverse surse, atât de pe rețele similare, cât și de pe site-uri și/sau portaluri de știri, alte surse on-line. Motivul pentru care există un mare interes și pentru astfel de activități în rețelele sociale constă în: (1) costuri reduse, acces ușor, diseminarea rapidă a informațiilor și (2) răspândirea știrilor de calitate scăzută (adesea intenționat pentru a induce în eroare cititorul) [2].

În [1] sunt formulate mai multe întrebări relevante cu referire la utilizarea rețelelor sociale, din care ne vom axa pe două: (1) putem avea încredere în toate știrile sau în toți utilizatorii care le răspândesc?; (2) putem îmbunătăți calitatea instrumentelor pentru valorificarea acestor informații?

În prezent, pe Twitter, nu există o metodă automată de a afla în timp real cum să monitorizăm credibilitatea utilizatorului și credibilitatea mesajelor [1]. În 2018 Mark Zuckerberg a recunoscut că există mai mult de 1 miliard de conturi false pe Facebook²¹. Conturile false constituie un real pericol în ce privește răspândirea de informații false și ca urmare, influențarea opiniei publice în legătură cu diverse fenomene, evenimente și probleme așa încât utilizatorii reali să fie dezinformați.

În lucrarea [1] sunt schițate două cele mai importante grupuri de abordări în detectarea știrilor false: ce țin de rețelele sociale și lingvistice.

Referitor la abordările privind rețelele sociale trebuie luată în seamă noțiunea de linked data²² [3; 4]

¹⁶<https://www.snapchat.com/>

¹⁷<https://zephoria.com/top-10-valuable-snapchat-statistics/>

¹⁸<https://www.linkedin.com/>

¹⁹<https://99firms.com/blog/linkedin-statistics/>

²⁰<https://expandedramblings.com/index.php/linkedin-business-page-and-group-statistics/5/>

²¹<https://www.ccn.com/facebook-billion-fake-account-zuckerberg-con-man/>

²²<https://www.w3.org/standards/semanticweb/data>

și de comportamentul utilizatorilor pe rețelele sociale [2; 5]. Cum utilizatorii urmează să se autentifice înainte de a utiliza o rețea socială, ei oferă o încredere sporită în datele care apar aici.

În cazul abordărilor lingvisticii computaționale informația este supusă unei statistici pe n -grame [6]. Propozițiile sunt transformate în forme mai avansate de reprezentare a informațiilor (cum ar fi arbori de decizie), se analizează probabilitățile de identificare a anomaliilor [3], se face un test semantic [2], se determină în acest context relațiile între elementele lingvistice, toate acestea contribuind la depistarea adevărului sau înșelăciunii [7]. În plus, pot fi utilizați clasificatorii SVM, clasificatorii de tip Bayesian Naïve [8] și rețelele neuronale [9].

Totuși, abordarea hibridă (combinarea învățării automate cu abordări de explorare a contextelor lingvistice din rețelele sociale) pare cea mai rezonabilă și promițătoare. În continuare vor fi prezentate câteva instrumente deja dezvoltate care au ca scop verificarea credibilității informației online.

INSTRUMENTE DE VERIFICARE A CREDIBILITĂȚII SURSELOR WEB

În ultimul deceniu, termenul de credibilitate online sau credibilitate web a fost folosit din ce în ce mai mult în diferite domenii. Cercetătorul Danielson s-a referit în studiile sale la patru caracteristici generale care îngreunează evaluarea credibilității web de către utilizatorii săi:

- lipsa relativă de filtrare și de mecanisme de gate-keeping;
- forma mijlocului de transmitere, incluzând tehnicile de interacțiune;
- ambiguitatea evidentă a sursei și lipsa atribuțiilor acesteia;
- caracterul nou al web-ului ca mijloc, lipsit de standarde de evaluare a web-ului [10].

Studii și analize cu referire la credibilitate au fost efectuate de cercetători din diverse domenii, cum ar fi știința informației, marketing, management, comunicații, inginerie web, jurnalism, și psihologie [11]. Drept rezultat, sunt elaborate un șir de instrumente de căutare și verificare a informațiilor în mediul online și puse la îndemâna utilizatorului pentru a fi folosite la evaluarea credibilității. Evidențiem în acest context câteva aplicații care luptă împotriva știrilor false și a dezinformării.

Karma reprezintă un sistem de evaluare a reputației utilizatorului pentru conținutul site-ului Point.md. Reputația utilizatorului s-a presupus că depinde de acțiunile lui pe site. Dezvoltatorii presupun

că reputația pozitivă poate fi obținută în mai multe moduri: prin citirea regulată a știrilor de pe acest site, comentarea și obținerea aprecierilor pentru comentariile date, identificarea erorilor în conținuturile postărilor pe site și expedierea știrilor importante sau a notelor despre evenimente la redacție. Principiul de acumulare a punctajului este următorul:

- Pentru a aprecia comentariul asupra unui articol se poate de acumulat de la 1 până la 5 puncte, în funcție de nivelul de influență al celui care te evaluează;
- Dacă sunt citite cel puțin 25 % din noutățile postate pe site se mai acumulează 1 punct;
- Participarea la vot +1 punct;
- Determinarea erorilor din conținuturi +10 puncte;
- Expedierea știrilor la redacție, care por apărea în fluxul de știri importante +100 de puncte.

Dacă utilizatorul încalcă regulile site-ului și comentariile sale sunt blocate de moderatori sau sunt depreciate de alți utilizatori, atunci nivelul *Karma* scade, adică a punctajului acumulat. De exemplu: pentru o depreciere a unui comentariu -1 punct, pentru blocarea comentariului de către moderator -10 puncte.

Logically²³ este o încercare de a îmbina instrumentele de inteligență artificială și umană pentru a combate dezinformarea, împuternicind mai mulți actori importanți (guvernele, platforma socială și consumatorii) să identifice și să minimizeze daunele. Tehnologia în spatele platformei alege informațiile cheie din text atunci când distribuie un articol. Poți selecta apoi informația care prezintă suspiciuni și dacă aplicația o poate verifica cu ajutorul algoritmului său, îți va indica imediat dacă conținutul este de încredere. În caz contrar, algoritmi din *Logically* vor începe să analizeze informația din postare.

Alte caracteristici utile ale aplicației includ alegerea unor articole bazate pe sistemul de analiză a sentimentelor (pozitive, negative și neutre) pentru fiecare articol care te pot ajuta să te poziționezi în cadrul unei dezbateri.

Alto Analytics²⁴ este o platformă de analiză a datelor care combate dezinformarea și tehnologia deepfake (tehnologia ce permite înlocuirea unei persoane dintr-o imagine sau a unui videoclip existent asemănător), pentru a proteja reputația unui brand și pentru a oferi informații comerciale și analize online/offline. Startup-ul își propune să ajute organizațiile publice, private și non-profit din întreaga lume să obțină informațiile de care au nevoie pentru a lua decizii în timp util pe baza unor informații corecte.

²³ <https://www.logically.ai/>

²⁴ https://www.alto-analytics.com/en_US/



Figura 1. Verificarea site-ului mediafax.ro cu ajutorul aplicației Rubrika.

Trueinchain²⁵ constituie platforma Web care folosește tehnologia din spatele criptomonedelor – blockchain – pentru a urmări și semnaliza știrile false. E nevoie doar să introduci linkul pentru informația falsă, să explici în comentarii sau printr-un fișier atașat de ce crezi că știrea respectivă este falsă, apoi tehnologia Trueinchain se va ocupa de restul. Trueinchain susține, de asemenea, o comunitate globală de “debunker” (eng. „to debunk” – a demasca). Aceștia urmăresc și demontează minciunile pentru a demonstra lipsa de fiabilitate a conținutului și surselor lor.

Fake News Guard²⁶ constituie o extensie pentru browserul Chrome care combină inteligența artificială cu feedback-ul de la utilizatori pentru a detecta informații false. Cu ajutorul extensiei pentru Chrome poți monitoriza pasiv paginile pe care le vizitezi, feed-ul de pe Facebook sau poți trimite în mod activ link-uri suspecte.

Factual.ro²⁷ este un site de fact-checking pe politicile și pe declarațiile publice din România. Platforma este întreținută voluntar de experți în politici publice, bună guvernare și comunicare. Echipa de proiect monitorizează decizii și declarații din spațiul public.

AdVerif.ai²⁸ este un startup de inteligență artificială care oferă soluții de verificare a conținutului pentru agenții de publicitate, editori și distribuitori de reclame.

Rubrika este aplicația ce-ți pune la dispoziție toate datele despre știrile pe care le accesezi. Datele despre sursele de știri sunt generate conform unui algoritm obiectiv ce îți indică scorul de încredere al domeniului web și alte date prezentate (figura 1).

Primul lucru care ar trebui să-l facă fiecare utilizator, cointerestat de credibilitatea datelor, este să verifice sursa unde a găsit informația. Dacă aceasta a apărut într-o sursă media, de asemenea urmează să fie verificată. Dacă vorbim de social media, de rețele de socializare, atunci se verifică persoana care a postat informația în spațiul virtual.

PERICOLUL SITE-URILOR FALSE

Constatăm faptul că este practic imposibil de a controla informația din Internet. Iată de ce Internetul rămâne locul unde un utilizator neatent riscă să înfrun-

te mai multe probleme, una dintre care o reprezintă site-urile false. Sunt mii de site-uri false astăzi, care urmăresc utilizarea datelor personale ale utilizatorilor de site-uri reale în scopuri criminale [12].

Această metodă ilegală de obținere a datelor confidențiale prin intermediul aplicațiilor din mediul on-line se numește **phishing**. De obicei, are forma unui mesaj prin care utilizatorul este îndemnat să completeze cu date confidențiale/personale un formular sau este informat că datele lui confidențiale/personale sunt necesare pentru rezolvarea unor erori tehnice prin accesarea unui link. La fel, poate fi folosit email-ul sau un serviciu de mesaje de pe site-urile de socializare on-line și care prin înșelăciune te provoacă să accesezi o adresă web sau să deschizi un fișier atașat [13].

Chiar dacă anumite site-uri false nu cer nimic, oricum ele au niște intenții ascunse, cum ar fi dezinformarea sau manipularea. În asemenea condiții este deosebit de important să fim atenți atunci când ajungem la astfel de site-uri de știri. Site-urile suspecte publică știri controversate, neadevărate, pline de invenții și le maschează după denumirile site-urilor cunoscute, publicând unele noutăți reale în care mai inserează informații false. De exemplu, de rând cu site-ul Ziarului de Gardă care este *zdg.md* a fost creat pe o platformă de blog un site *ziaruldegarda.blogspot.com*. Portalul Stopfals.md a încercat să elaboreze o listă de site-uri false²⁹ pentru știrile din Republica Moldova. Permanent apar o mulțime de site-uri false și permanent sunt elaborate liste cu astfel de site-uri pentru toate regiunile din lume³⁰. Însăși companiile renumite precum Google elaborează liste cu site-uri false³¹. Totuși, nu putem afirma că acestea sunt complete întrucât zilnic apar o mulțime de site-uri suspecte.

Pentru a nu cădea pradă unor astfel de surse de informație, cum sunt site-urile false, au fost formulate un șir de sugestii în vederea depistării acestora. Analizând mai multe surse, pot fi formulate următoarele sugestii necesare în verificarea site-ului înainte de a începe citirea informației de pe site^{32, 33}:

²⁹ <https://stopfals.md/ro/category/21>

³⁰ <https://db.aa419.org/fakebankslist.php>

³¹ <https://www.webarxsecurity.com/what-is-google-blacklist/>

³² <https://www.thesslstore.com/blog/5-ways-to-determine-if-a-website-is-fake-fraudulent-or-a-scam/>

³³ <https://www.asecurelife.com/how-to-spot-a-fake-website/>

²⁵ <https://trueinchain.org/en>

²⁶ <https://www.fakenewsguard.com/#/>

²⁷ <https://www.factual.ro/>

²⁸ <https://adverifai.com/>

Atenție la bara de adrese – adresa unui site web ar trebui să se înceapă cu *https* și nu cu *http*. Litera *s* este un indice cum că site-ul web este sigur și că folosește criptarea pentru protecția datelor de la hackerii.

Verificarea adresei și a domeniului – deseori escrocii creează site-uri web cu adrese care imită pe cele ale mărcilor sau companiilor mari, precum *Yah00.com* sau *Amaz0n.net*, bazându-se pe faptul că nu se va verifica atent adresa și numele domeniului.

Verificarea vechimii domeniului – de regulă site-urile false sunt create recent pentru anumite scopuri rapide. De aceea vechimea domeniului are o importanță deosebită. În vederea determinării ei există mai multe instrumente, de exemplu: *WhoIs*³⁴, *URL-Checker*³⁵ ș.a.

Verificarea gramaticală și ortografică a informației de pe site – un exces de greșeli de ortografie, de punctuație, de scriere cu majuscule etc. ar putea indica faptul că un site web a crescut rapid. Companiile cu site-uri web legitime pot avea cu siguranță greșeli de scriere accidentale, dar depun eforturi în prezentarea unui site web profesional.

Informații de contact sigure – dacă singura metodă de contact este un formular de e-mail on-line, ar trebui să fim mai prudenți. Ar fi bine ca pe site să existe informații precum telefon, e-mail și adresă fizică.

Practic acestea ar fi cele mai importante informații care ar trebui să fie verificate pentru a avea o credibilitate acceptabilă.

CONCLUZII

Rețelele sociale joacă un rol deosebit de important în distribuirea conținuturilor de diferit tip, care deseori nu sunt verificate și bulversează cititorul în parte și comunitatea în ansamblu. Procesarea și prevenirea distribuirii conținuturilor false în timp real este o sarcină complicată, în condițiile în care pe Web permanent este generat un volum enorm de conținut nou. Exemplul rețelelor sociale *Twitter*, *Facebook* sau *Google* dovedește că și cele mai puternice companii nu sunt capabile să soluționeze definitiv problema site-urilor Web false. Cercetarea arată că nu există tehnologii informatice perfecte pentru a verifica credibilitatea informației pe Web. Totodată, există încercări de a automatiza procesul dat, posibilitatea de a obține mai multe detalii cu referire la sursa de informații. În acest sens responsabilitatea privind veridicitatea sursei revine utilizatorului care trebuie să fie mult mai atent și să se intereseze mai insistent referitor la proveniența site-ului Web și a informației de pe el.

³⁴ <https://whois.domaintools.com/>

³⁵ <https://iplogger.ru/url-checker/>

BIBLIOGRAFIE

1. Iftene A. Exploiting Social Networks. Technological Trends. Habilitation Thesis submitted at „Alexandru Ioan Cuza” University, December 2019. 163 p.
2. Shu K., Sliva A., Wang S., Tang J., Liu H. Fake News Detection on Social Media: A Data Mining Perspective. In: *SIGKDD Explor. Newsl.*, vol. 19, no. 1, 2017, pp. 22-36.
3. Conroy N. J., Rubin V. L., Chen Y. Automatic Deception Detection: Methods for Finding Fake News. In: *ASIST 2015*, November 6-10, St. Louis, MO, USA, pp. 1-4.
4. Idehen K. U. Exploitation of a Semantic Web of Linked Data, for Publishers. 2017. [on-line] <https://medium.com/virtuoso-blog/exploitation-of-a-semantic-web-of-linked-data-for-publishers-295f16ee8525> (vizitat la 11.09.2020).
5. Shu K., Bernard H.R., Liu H. Studying Fake News via Network Analysis: Detection and Mitigation. In: *Emerging Research Challenges and Opportunities in Computational Social Network Analysis and Mining*, 2019, pp. 43-65, https://doi.org/10.1007/978-3-319-94105-9_3
6. Hadeer A., Issa T., Sherif S. Detection of Online Fake News Using N-Gram Analysis and Machine Learning Techniques. In: *International Conference on Intelligent, Secure, and Dependable Systems in Distributed and Cloud Environments ISDDC 2017*, pp. 127-138.
7. Rubin V., Lukoianova T. Truth and deception at the rhetorical structure level. In: *Journal of the American Society for Information Science and Technology*, vol. 66, no. 5, 2014.
8. Singh V., Dasgupta R., Sonagra D., Raman K., Ghosh I. Automated Fake News Detection Using Linguistic Analysis and Machine Learning. In: *Proceedings of Conference SBP-BRIMS 2017*, <https://doi.org/10.13140/RG.2.2.16825.67687>
9. Sneha S., Nigel F., Shrishra R.. A Deep Neural Network for Fake News Detection. In: *24th International Conference on Neural Information Processing (ICONIP 2017)*, Springer Int. Publishing AG 2017, part II, LNCS vol. 10635, pp. 1-10, https://doi.org/10.1007/978-3-319-70096-0_59
10. Rieh S. Y., Danielson D. R. Credibility: A multidisciplinary framework. In: *Annual Review of Information Science and Technology*, vol. 41, pp. 307-364, <https://doi.org/10.1002/aris.2007.1440410114>
11. Wineburg S., McGrew S., Breakstone J., Ortega T. Evaluating information: The cornerstone of civic online reasoning. In: *Stanford Digital Repository*. Stanford Hystory Education Club. 2018, 29 p.
12. Chem opasny sayty poddelki? [on-line] https://internetpolicy.kg/literacymodule/course_1/module1/glava1_5.html (vizitat la 23.10.2020).
13. Pranali O. P., Upadhyay D. Review on Phishing Sites Detection Techniques. In: *International Journal of Engineering Research & Technology*, Vol. 9 Issue 04, 2020, pp. 882-884, <http://dx.doi.org/10.17577/IJERTV9IS040759>

NOTĂ. Articolul este elaborat în cadrul proiectului 20.80009.5007.22 „Sisteme informatice inteligente pentru soluționarea problemelor slab structurate, procesarea cunoștințelor și volumelor mari de date” din cadrul Programului de Stat 2020–2023.