CZU: 378.091:004 DOI: 10.46727/c.steam-2023.p223-227

DIN EXPERIENȚA CERCETĂRII CONCEPTULUI DE „AMPRENTĂ DIGITALĂ” ȘI IMPACTUL ACESTUIA ASUPRA SECURITĂȚII INFORMAȚIILOR

Violeta BOGDANOVA, doctor, lector universitar
https://orcid.org/0000-0003-4140-6317
Universitatea Pedagogică de Stat „Ion Creangă” din Chișinău
Tetiana FILATOVA, lector superior universitar
https://orcid.org/0000-0001-9373-4756
Universitatea Națională „Politehnica Odessa”, Odessa, Ucraina

Rezumat. În articol se discută despre conceptul de amprentă digitală și necesitatea studierii amprentei digitale la nivel organizatoric, la nivel de stat. Este prezentat un chestionar elaborat pe tema „Amprenta digitală”. Este analizat gradul de conștientizare a elevilor în domeniul creării și gestionării amprentei lor digitale. Este fundamentată necesitatea dezvoltării competențelor și abilităților în ceea ce privește crearea și gestionarea unei amprente digitale pentru a asigura starea de securitate în mediul informațional.
Cuvinte cheie: amprenta digitală, securitatea informației, tehnologia informației, competențe informaționale.

Abstract. The article considers the concept of a digital footprint. The awareness of students in this area is analyzed. The didactic aspects of the formation of skills and abilities in terms of the formation and management of the digital footprint to ensure the state of security in the information environment are presented.
Keywords: digital footprint, information security, information technology, information skills.

Introducere

O mare oportunitate pentru analiza vulnerabilităților informaționale este amprenta digitală. O amprentă digitală este o serie nestructurată de date pe care un utilizator o lasă în rețeaua globală de informații: o achiziție cu un card de credit, o interogare de căutare, mișcare cu un smartphone, aprecieri pe rețelele sociale. Analiza amprentei digitale a unui utilizator ne permite să modelăm caracteristicile sale comportamentale și să folosim aceste date în diverse scopuri: oferirea de bunuri într-un magazin online, influență informațională și psihologică și multe altele.

Amprentele digitale pot fi active sau pasive. Utilizatorul însuși lasă o urmă digitală activă: pagini pe rețelele sociale, completarea formularelor pe site-uri web, activitare pe site-uri web. O amprentă digitală pasivă este colectată de site-uri web: adresa IP, informații despre sistemul de operare, browser și extensii, fus orar etc.

Companiile revizuiesc din ce în ce mai mult profilul digital al unui candidat pentru a reduce riscul unor viitoare riscuri reputaționale și financiare pentru organizație.

Atacatorii studiază amprenta digitală a unei persoane în activitățile lor ilegale. Agențiile guvernamentale sunt, de asemenea, interesate de extinderea datelor despre cetățeni [2].

Metode şi materiale aplicate

În cadrul lucrării de proiect în studiul disciplinei „Securitatea informației", împreună cu studenții, a fost elaborat un chestionar privind fenomenul „amprentă digitală":

1) *Vă rugăm să indicați sexul dvs.*
2) *Vă rugăm să indicați vârsta dvs.*
3) *Vă rugăm să indicați nivelul dvs. de educație.*
4) *Dacă sunteți student, indicați anul de studii.*
5) *Folosești rețele publice wi-fi (de exemplu, într-o cafenea)?*
6) *Parola dumneavoastră pentru rețelele sociale conține: a) doar numere; b) numai litere; c) cifre și litere; d) litere mari și mici, cifre, simboluri diverse.*
7) *Folosiți un VPN? („Virtual Private Network" înseamnă „rețea privată virtuală". Acesta este un serviciu care vă permite să rămâneți privat pe Internet și pe rețea. Un VPN stabilește o conexiune sigură, criptată între computerul dvs. și Internet, oferind un tunel privat pentru date și comunicații atunci când se utilizează rețele publice).*
8) *A fost piratat vreodată contul tău de rețea socială, de e-mail sau de mesagerie?*
9) *Utilizați conturi ale altor servicii pentru a vă autoriza (de exemplu, conectați-vă la Instagram prin Facebook)?*
10) *Schimbați des parolele pentru conturile de rețele sociale?*
11) *Ce informații postezi despre tine pe Internet? a) informații detaliate: nume complet, număr de telefon, vârstă, fotografii; b) numai datele necesare înregistrării; c) Nu postez nicio informație despre mine.*
12) *Sstudiați profilul unei persoane pe rețelele de socializare înainte de a merge pentru prima dată la o întâlnire reală?*
13) *Vi se cere să vă înregistrați pe un site terță parte. Ca informații personale, vi se cere să furnizați o adresă de e-mail sau să vă înregistrați folosind un cont de rețea socială. Ce metodă vei alege?*
    a) *Voi alege un e-mail: este convenabil și nu este nevoie să introduc date suplimentare*
    b) *Mă voi conecta printr-o rețea de socializare, astfel încât totul să fie legat de acesta*
    c) *Îmi voi crea un cont nou.*
14) *E-mail, rețele sociale, mesagerie instant, aplicație bancară, magazine online. Fiecare necesită un login și o parolă. Ce faci de obicei?: a) Am o singură parolă*

pentru toate conturile; b) memorizez toate parolele sau le notez într-un carnețel; c) Îmi trimit login-ul și parola prin messenger, astfel încât să le pot găsi rapid mai târziu.

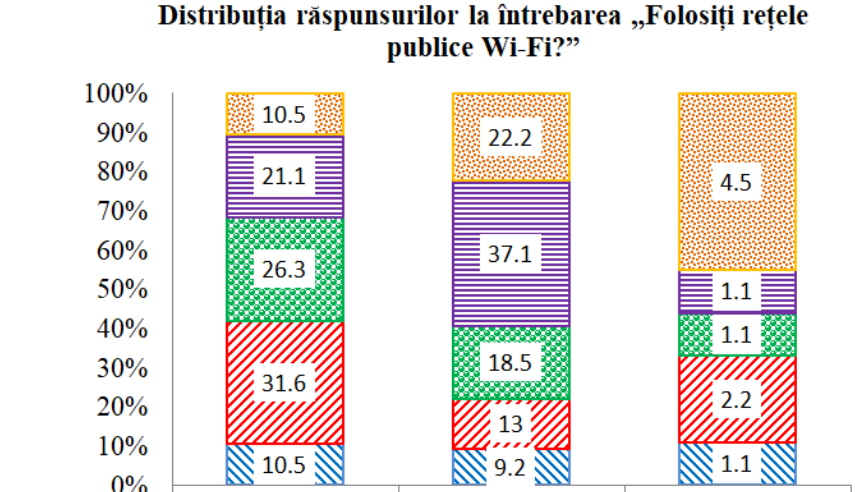
15) *Vă înregistrați pe o rețea socială nouă. Profilul tău va fi privat sau public?:*
   a) *bineînțeles deschis, nu am nimic de ascuns;*
   b) *o voi face privată: nu vreau ca străinii să știe cum trăiesc.*

16) *Vizitezi canalul tău de știri preferat în fiecare zi. Ce date crezi că „colectează" site-ul despre tine?*
   a) *nu colectează niciunul;*
   b) *adună ceva, dar nu pot spune ce anume;*
   c) *colectează numai date de locație (dacă este activată geolocalizarea);*
   d) *colectează datele pe care eu însumi le indic.*

Rezultate obținute

La sondaj au participat 101 studenți din trei niveluri de învățământ: învățământ neprofesional, învățământ secundar profesional și învățământ superior.

Majoritatea respondenților folosesc adesea rețele publice Wi-Fi, ceea ce crește riscul scurgerii de date. 20,8% dintre respondenți folosesc rar rețelele publice, 20,8% uneori, 19,8% întotdeauna. Și doar 9,9% dintre respondenți nu folosesc niciodată rețele publice Wi-Fi. Aceasta înseamnă că traficul lor este protejat și, prin urmare, greu de urmărit de către un atacator care se conectează la același punct de acces și folosește un software special care le permite să analizeze traficul (Figura 1).



	< 18	18-24	> 25
Mereu	10.5	22.2	4.5
De multe ori	21.1	37.1	1.1
Uneori	26.3	18.5	1.1
Rareori	31.6	13	2.2
Niciodată	10.5	9.2	1.1

Figura 1. Frecvența utilizării Wi-Fi în locuri publice, %

La întrebarea „Ți-a fost piratat vreodată contul de socializare, de e-mail sau de mesagerie instant?” majoritatea respondenților au răspuns afirmativ și ei. 7,9% dintre respondenți nu știu dacă rețeaua lor socială a fost piratată. Aproape jumătate dintre respondenți (48,5%) susțin că contul lor de socializare a fost piratat. Partea rămasă (43,6%) dintre studenți își monitorizează securitatea conturilor în spațiul cibernetic și îi împiedică să fie piratați (Figura 2).

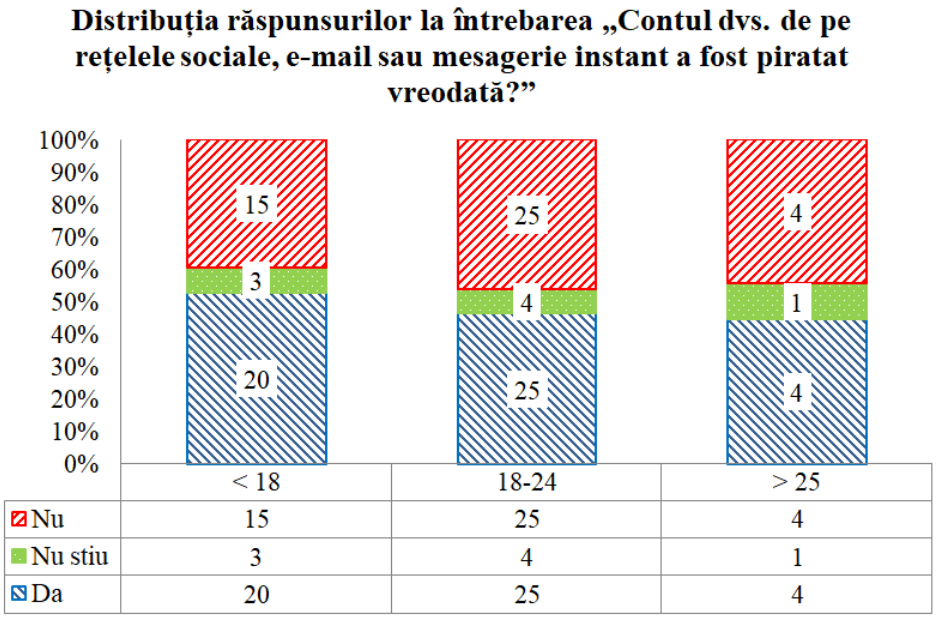


Figura 2. Frecvența piratarii rețelelor sociale, pers.

La întrebarea „Va fi cu acces deschis noul profil la crearea unui cont nou”, 57% dintre respondenți au răspuns afirmativ, 43% îl vor face privat. Și această tendință se observă la toate categoriile de vârstă ale respondenților (Figura 3).

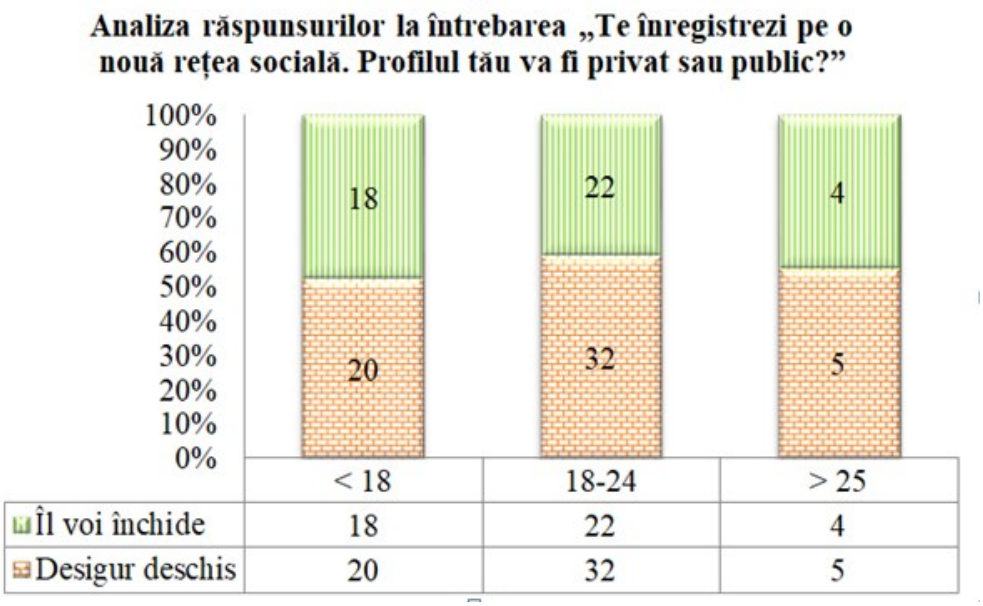


Figura 3. Tip de profil creat pe o nouă rețea socială, pers.

După cum se poate observa din sondajul studenților, mulți iau destul de ușor formarea amprentei lor digitale. Putem oferi mai multe recomandări pentru protejarea datelor cu caracter personal și gestionarea reputației online.

Concluzii

În prezent, amprenta digitală acționează de fapt ca o amprentă a vieții și a personalității, pe baza căreia este posibil să se creeze un portret al utilizatorului: să determine nivelul de dezvoltare intelectuală și starea mentală, să identifice interese și nevoi de bază, să-și dezvăluie statutul social și perspectiva. O amprentă digitală poate avea un impact negativ asupra finanțelor și reputației unei persoane. Este necesar să se studieze în cadrul disciplinelor ciclului informațional modalitățile de formare și control a amprentei digitale. Cunoașterea principiilor formării și managementului amprentei digitale permite reducerea riscurilor financiare și de reputație atât pentru persoane fizice, cât și pentru organizații.

Articol realizat în cadrul proiectului de cercetări științifice „Metodologia implementării TIC în procesul de studiere a științelor reale în sistemul de educație din Republica Moldova din perspectiva inter/transdisciplinarității (concept STEAM)”, inclus în „Program de stat” (2020-2023), Prioritatea IV: Provocări societale, cifrul 20.80009.0807.20, cu suportul financiar oferit de Agenția Națională pentru Dezvoltare și Cercetare

Bibliografie

1. Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/standard/44381.html
2. ГОРАШ, И.; БОГДАНОВА, В.; ДАРИЕНКО, М. Цифровая тень и цифровой след как угроза информационной безопасности. In: *The use of modern educational and informational technologies for the training of professional competences of the students in higher education institutions*. Balti, 2019, pp. 247-251. ISBN 978-9975-3369-3-2.
3. ШЕСТАКОВА, А.А. Цифровая личность: границы и барьеры коммуникативных практик в сетевом взаимодействии. In: *Материалы VIII международной социологической Грушинской конференции «Социолог 2.0: трансформация профессии»*. М, 2018. p. 422–425.
4. CHIRIAC, L.; BOGDANOVA, V. From the experience of studying the digital footprint from the position of information security. In: *CAIM 2023. Proceedings of the 30th Conference on Applied and Industrial Mathematics*, September 14-17, 2023. Iaşi: UAIC, 2023. p. 22-26. ISBN 978-9975-76-401-8.