

PREVENIREA INFRACTIUNILOR INFORMATICE CA FUNDAMENT PENTRU GARANTAREA SECURITĂȚII NAȚIONALE

PREVENTING CYBERCRIMES AS A FOUNDATION FOR ENSURING NATIONAL SECURITY

CZU: 351.86:004.056.5:355.1(478)

<https://doi.org/10.59295/spd2024s.37>

Marcel BENCHECI,

ORCID: 0000-0002-6619-5299

e-mail: marcelbencечи@mail.ru

Institutul de Cercetări Juridice, Politice, Sociologice,
Universitatea de Stat din Moldova

Nicolae PANFILII,

ORCID: 0009-0002-3640-6849

e-mail: n.panfilii22@gmail.com

Universitatea Liberă Internațională din Moldova

Diana HÎRBU,

ORCID: 0000-0002-7867-1731

e-mail: benchecidiana@gmail.com

Universitatea de Stat din Moldova

Summary. Preventing cybercrimes is essential for maintaining national security in an increasingly digitalized world. The use of cutting-edge technologies, such as artificial intelligence and intrusion detection systems, is crucial for protecting critical infrastructure. Additionally, updating laws in this field and enforcing strict regulations are essential for deterring and sanctioning cybercrimes. International cooperation on legislation can also improve the efficiency of prevention and combat measures. Raising awareness of risks and protective measures among citizens and employees can prevent many cyberattacks, and cybersecurity awareness and training programs should be prioritized to reduce vulnerabilities. By adopting these measures, cybercrime prevention can become a fundamental pillar of national security, protecting critical infrastructure and ensuring national stability and safety.

Keywords: security threats, cybercrime, Republic of Moldova, state, national security.

INTRODUCERE

Evoluția tehnologiei informației și diversificarea surselor de informare în masă, pe de o parte, creează condiții favorabile pentru buna funcționare a societății contemporane. Pe de altă parte, acestea facilitează extinderea utilizării de către entitățile subversive a mijloacelor de propagandă și agresiune mediatică, având ca scop destabilizarea situației social-politice și subminarea suveranității, independenței și integrității teritoriale ale Re-

publicii Moldova. Creșterea dependenței societății moderne de globalizarea sistemelor informaționale și a infrastructurilor de comunicații duce la sporirea vulnerabilității persoanelor, societății și statului în fața amenințărilor tot mai mari din domeniile tehnologic și mediatic.

Măsurile de prevenire, depistare și contracarare a amenințărilor complexe și persistente la adresa securității informaționale sunt posibile doar cu un cadru normativ adecvat, instrumente și metode bine definite și mecanisme de colaborare națională și internațională eficiente. Riscurile din spațiul cibernetic sunt direct proporționale cu nivelul de informatizare a societății, iar combaterea criminalității informatice trebuie să fie o preocupare majoră pentru toți actorii implicați. În ultimii ani, am observat o creștere a crimei organizate, care merge mână în mână cu evoluția criminalității informatice, aceasta fiind din ce în ce mai stimulată de aplicabilitatea și accesibilitatea tehnologiei în comiterea infracțiunilor.

Experiența internațională arată impactul pozitiv al infrastructurii informaționale și de comunicații asupra progresului societății moderne. Acest impact constă în extinderea accesului la informație și la resursele publice în diverse domenii de activitate umană, inclusiv guvernarea electronică, economia digitală, comerțul online, educația digitală, cultura digitală, și medicina digitală, printre altele. De asemenea, contribuie la creșterea numărului de locuri de muncă disponibile și ocuparea populației. Prosperitatea și dezvoltarea economică a Republicii Moldova depind de integrarea rapidă într-o economie regională și globală tot mai competitivă. Prin urmare, construirea unei societăți informaționale este crucială pentru progresul țării și trebuie să fie realizată într-un mod care să aducă beneficii tuturor cetățenilor.

Mediul online facilitează săvârșirea infracțiunilor prin furnizarea atât a unui nou obiect (informația stocată și procesată de sistemele informatice), cât și a unui nou instrument. Acest mediu oferă o gamă variată de tehnici și metode pentru comiterea infracțiunilor, ceea ce generează noi tipuri de infracțiuni. Fraudele informatice, atacurile cibernetice, escrocheriile cu carduri electronice și pornografia infantilă sunt exemple de infracțiuni care necesită investigații specializate și echipamente adecvate pentru aplicarea legii.

Criminalitatea informatică este un fenomen infracțional care alimentează, la rândul său, foarte multe riscuri și crize în spațiul cibernetic. Evoluția fenomenului criminogen în Republica Moldova în ultimii ani [1] este strâns legată de spațiul cibernetic, ceea ce se manifestă prin folosirea tot mai intensă a tehnologiilor informaționale la comiterea infracțiunilor. Internetul a devenit o componentă integrată și esențială a societății și economiei moderne. Cu cât o societate este mai dependentă de tehnologie, cu atât devine mai vulnerabilă la amenințări. Combaterea criminalității informatice este o prioritate pentru toți cei implicați, cu accent special pe nivel instituțional, unde responsabilitatea principală este elaborarea și implementarea politicilor coerente în acest domeniu.

Principalele acte normative care au stat la baza elaborării Strategiei de securitate informațională, documente valabile până în anul 2020 și relevante pentru dimensiunea

securității informaționale, urmează să transpună la nivel național modelul european de dezvoltare a societății informaționale. Acestea includ Strategia națională de dezvoltare a societății informaționale „Moldova Digitală 2020”, aprobată prin Hotărârea de Guvern nr. 857/2013, și Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016–2020, aprobat prin Hotărârea de Guvern nr. 811/2015. Conform Planului de acțiuni privind implementarea Programului național de securitate cibernetică pentru anii 2016–2020, au fost planificate 50 de acțiuni. Aceste acțiuni au fost structurate pe mai multe domenii de intervenție, incluzând procesarea, stocarea și accesarea sigură a datelor, securitatea rețelelor și a serviciilor de comunicații electronice, dezvoltarea capacităților de prevenire și de reacție rapidă la nivel național prin crearea rețelei CERT naționale, combaterea criminalității informatice, consolidarea capacităților de apărare cibernetică, educația și formarea continuă în domeniul securității cibernetice, precum și cooperarea internațională în domeniul securității cibernetice.

În același context, urmează a se menționa că scopul Strategiei securității informaționale a Republicii Moldova este de a corela juridic și de a integra sistemic domeniile prioritare cu responsabilități și competențe de asigurare a securității informaționale la nivel național, fiind bazat pe reziliența cibernetică, pluralismul multimedia și convergența instituțională în materie de securitate, destinate protejării suveranității, independenței și integrității teritoriale a Republicii Moldova [2]. În același timp, Strategia de securitate informațională examinează situația actuală în domeniul securității informaționale, evaluând progresele realizate și tendințele în dezvoltarea societății informaționale la nivel național, identificând problemele existente și potențialele, care generează riscuri și amenințări de securitate, inclusiv cele hibride. Adoptarea acestei Strategii a fost motivată de necesitatea protejării intereselor individuale, sociale și statale în spațiul informațional, având în vedere gravitatea și diversitatea amenințărilor la adresa securității informaționale în societatea modernă și importanța menținerii unui echilibru între aceste interese pentru asigurarea securității informaționale. De asemenea, dat fiind natura globală a sistemelor informaționale și a rețelelor de comunicații electronice, este esențială o coordonare strânsă între toate instituțiile responsabile, atât la nivel național, cât și la nivel global.

Un alt document de politică crucial pentru Republica Moldova este Strategia de Transformare Digitală pentru perioada 2023-2030. Acest document stabilește direcțiile de transformare digitală până în 2030 și reiterează angajamentul Ministerului Dezvoltării Economice și Digitalizării de a dezvolta o societate digitală modernă, focalizată pe nevoile cetățenilor și aliniată cu agenda de integrare europeană [4].

Percepțiile utilizatorilor de Internet și TIC despre propriile abilități și cunoștințe pentru a se proteja de victimizarea informatică le afectează comportamentul și activitățile online. Același lucru se aplică responsabilității pentru securitatea online personală [5]. Cu alte cuvinte, persoanele care sunt conștiente că securitatea informatică este o responsabilitate personală și care au competențele necesare adoptă probabil mai multe măsuri de securitate informatică și adoptă comportamente mai protectoare atunci când utili-

zează internetul și tehnologiile informației și comunicațiilor (TIC). Deși este adevărat că informațiile, strategiile de conștientizare și educația pot fi aplicate în orice grup de vârstă, eforturile și inițiativele în acest domeniu s-au axat în mare parte pe copii și tineri. Mass-media joacă un rol crucial în diseminarea informațiilor și în prevenirea violenței și criminalității în diverse contexte [5]. Prin urmare, mass-media poate juca un rol crucial în prevenirea criminalității informatice prin distribuirea informațiilor publice și prin desfășurarea de campanii de conștientizare în acest domeniu. Acest lucru poate fi realizat prin diverse mijloace de comunicare, inclusiv prin internet și rețele sociale, sau prin canale mai tradiționale, cum ar fi televiziunea. În orice caz, campaniile de informare și conștientizare ar trebui integrate într-o strategie mai largă de prevenire a criminalității informatice [6].

Dezvoltarea rapidă a mijloacelor de comunicare are un impact semnificativ atât asupra societății, cât și asupra individului. Într-o lume globalizată, caracterizată de interdependențe complexe, această evoluție aduce o serie de beneficii incontestabile, dar și provocări semnificative. Avansul tehnologic face ca mediul de securitate să devină din ce în ce mai dinamic, cu vulnerabilități și amenințări care depășesc limitele spațiului fizic și se manifestă frecvent în mediul virtual.

CONCLUZII

Prevenirea infracțiunilor informatice este crucială pentru menținerea securității naționale într-o societate tot mai digitalizată. Utilizarea tehnologiilor avansate, cum ar fi inteligența artificială și sistemele de detectare a intruziunilor, joacă un rol crucial în protejarea infrastructurilor critice. Este esențială actualizarea legislației și implementarea unor reglementări stricte pentru descurajarea și sancționarea infracțiunilor informatice. Colaborarea internațională în domeniul legislativ poate îmbunătăți eficiența măsurilor de prevenire și combatere a acestor infracțiuni. Conștientizarea riscurilor și promovarea măsurilor de protecție printre cetățeni și angajați sunt cruciale pentru prevenirea multor atacuri informatice. Programele de educație și formare în securitate cibernetică trebuie să fie prioritare pentru a reduce vulnerabilitățile. Prin adoptarea acestor strategii, prevenirea infracțiunilor informatice poate deveni un element fundamental al securității naționale, contribuind la protejarea infrastructurilor critice și asigurarea stabilității și securității naționale.

REFERINȚE

1. *Proiectul de Hotărâre a Guvernului cu privire la aprobarea Strategiei naționale pentru prevenirea și combaterea criminalității informatice pentru anii 2018 – 2021*. În: https://particip.gov.md/ro/download_attachment/7954 [Accesat: 16.03.2024].
2. Ordinul Procurorului General interimar nr. 19/3 din 28.02.2024 privind aprobarea Raportului de activitate al Procuraturii pentru anul 2023.

3. BURKE, RH. *An Introduction to Criminological Theory*. În: Oxon, 2009. Anglia: Taylor & Francis.
4. Strategiadetransformaredigitală. În: <https://mded.gov.md/transparenta/64373-2/> [Accesat: 08.03.2024].
5. APAV (2011). *Manual crianças e jovens vítimas de violência: compreender, intervir e prevenir*. ISBN 978-972-8852-50-4. Lisabona: APAV.
6. BREWER, R., DE VEL-PALUMBO, M., HUTCHINGS, A., HOLT, T., GOLD-SMITH, A., & MAIMON, D. *Cybercrime Prevention: Theory and Applications*. În: Springer Nature. 2019.

* Articolul este elaborat în cadrul subprogramului 01.05.01 „Securitatea națională a Republicii Moldova în contextul aderării la Uniunea Europeană: abordări juridice, politologice și sociologice”, realizat de Institutul de Cercetări Juridice, Politice și Sociologice al Universității de Stat din Moldova.