**UNIVERSITATEA DE STAT DIN MOLDOVA
FACULTATEA RELAȚII INTERNAȚIONALE, ȘTIINȚE POLITICE ȘI ADMINISTRATIVE
DEPARTAMENTUL RELAȚII INTERNAȚIONALE**

**LUCRUL INDIVIDUAL**la disciplina de curs: „Securitatea informațională”
Tema: „Provocări actuale în domeniul securității cibernetice – impact și contribuția Republicii Moldova în domeniu”

Elaborat de: Cobasiuc Anastasia, gr. SSN01
Coordonator științific: Busuncian T., dr., l. univ.

**Chișinău, 2023**

**Cuprins**

[INTRODUCERE 3](#_Toc150799321)

[Studiul amenințărilor și vulnerabilităților la adresa securității cibernetice 4](#_Toc150799322)

[Provocările în domeniul securității cibernetice în Republica Moldova 7](#_Toc150799323)

[Cadrul național în domeniul securității cibernetice 8](#_Toc150799324)

[Impactul Republicii Moldova în domeniul securității cibernetice 9](#_Toc150799325)

[CONCLUZII 10](#_Toc150799326)

[BIBLIOGRAFIE 11](#_Toc150799327)

# Introducere

***Actualitatea temei.*** A trecut deja mai bine de un an de la izbucnirea conflictului din Ucraina și s-a trecut prin diverse provocări din care s-au desprins nenumărate lecții învățate despre modul în care războiul cibernetic poate avea impact asupra mediilor economic, politic și social în care se desfășoară viața de zi cu zi. Autoritățile statului moldovenesc care au competențe în asigurarea securității naționale, inclusiv în spațiul cibernetic, s-au confruntat cu amenințări complexe concretizate și prin atacuri cibernetice. Acestea au variat ca volum, intensitate și diversitate, iar pe baza lor s-au făcut analize și s-au desprins elementele care au fost avute în vedere atunci când s-a consolidat și îmbunătățit reziliența în spațiul cibernetic al Republicii Moldova.

Înainte de anul 2014, războiul cibernetic, deși exista la nivel teoretic ca o componentă a războiului hibrid, nu a fost reliefat la adevărata sa dimensiune. Odată cu această agresiune, în imediata vecinătate a țării noastre, războiul cibernetic a ieșit la suprafață și a reprezentat momentul în care instituțiile statului și întreaga lume au început să înțeleagă la ce ne putem aștepta în continuare. Încă din anul 2014, autoritățile publice, sistemul energetic, sistemul bancar, furnizorii de servicii IT și sistemul de transport din Ucraina au fost ținta unor atacuri cibernetice care au afectat buna funcționare a statului. Pe măsură ce conflictul a escaladat, atacurile au devenit tot mai intense și efectele lor au fost tot mai vizibile, precum întreruperi în furnizarea energiei electrice, imposibilitatea de a utiliza sistemul bancar, lipsa accesului la servicii de internet și altele.

***Scopul și obiectivele lucrării***. Scopul lucrării constă în stabilirea și analizarea provocărilor actuale în domeniul securității cibernetice, cât și identificarea impactului acestora asupra securității Republicii Moldova și contribuția statului moldovenesc la contracararea acestor provocări. Pentru realizarea scopului, s-au consolidat eforturile spre soluționarea următoarelor obiective:

* dezvăluirea studiului asupra amenințărilor și vulnerabilităților la adresa securității cibernetice;
* examinarea provocărilor în domeniul securității cibernetice în Republica Moldova;
* studierea cadrului național în domeniul securității cibernetice;
* stabilirea impactului Republicii Moldova în domeniul securității cibernetice.

# Studiul amenințărilor și vulnerabilităților la adresa securității cibernetice

Securitatea cibernetică este legată, fără a fi în general considerată identică, cu conceptul de securitate a informațiilor. Acest ultim termen poate fi definit drept activitatea de protejare a informațiilor și a sistemelor informatice împotriva accesului neautorizat, utilizării, dezvăluirii, întreruperii, modificării sau distrugerii, pentru a asigura integritatea, confidențialitatea și disponibilitatea informațiilor.

Uneori, securitatea cibernetică este necorespunzător asociată cu alte concepte, cum ar fi confidențialitatea, schimbul de informații, colectarea de informații și supravegherea. Cu toate acestea, securitatea cibernetică este un instrument important în protejarea vieții private și prevenirea supravegherii neautorizate, iar schimbul de informații și colectarea de informații pot fi instrumente utile pentru asigurarea securității informatice.

Un atac reușit poate compromite confidențialitatea, integritatea și disponibilitatea unui sistem TIC și ale informațiilor pe care acesta le gestionează. Fenomene precum furtul sau spionajul cibernetic pot duce la obținerea unor informații financiare, personale sau profesionale, adesea fără cunoștința victimei. Atacurile de tip DoS (Denial-of-Service) pot încetini sau împiedica accesul utilizatorilor legitimi la un sistem informatic. Printr-un malware de tip botnet, un atacator poate comanda un sistem pentru a fi utilizat în atacuri cibernetice asupra altor sisteme. Atacurile asupra sistemelor de control industriale pot duce la distrugerea sau întreruperea echipamentelor pe care le controlează (generatoare, pompe, centrale), cu efecte grave la nivel regional sau statal.

Vulnerabilitatea este o slăbiciune a unui sistem hardware sau software ce permite utilizatorilor neautorizați să obțină acces asupra sa. Principalele vulnerabilități în cadrul sistemelor informatice sunt de natură fizică, hardware, software sau umană.

Sistemele informatice sunt vulnerabile în primul rând la atacurile clasice, atunci când un atacator reușește să pătrundă fizic în incinta sistemelor de calcul și să sustragă informații confidențiale. Pentru a preîntâmpina acest lucru trebuie să se asigure securitatea fizică a echipamentelor de calcul prin plasarea acestora în zone sigure, restricționate personalului neautorizat. Accesul la aceste zone trebuie făcut prin folosirea interfoanelor, cardurilor de acces sau dispozitivelor de scanare a datelor biometrice pentru autentificarea utilizatorilor cu permis de intrare. O altă vulnerabilitate a sistemelor informatice o reprezintă dezastrele naturale (cutremure, inundații, incendii) sau accidentele precum căderile de tensiune sau supratensiunile ce pot duce la distrugerea fizică a echipamentelor de calcul. De aceea trebuie avute în vedere și amplasarea echipamentelor pentru reducerea riscului față de amenințările mediului înconjurător.

Din punct de vedere software există mai multe tipuri de vulnerabilități:

* care măresc privilegiile utilizatorilor locali fără autorizație;
* care permit utilizatorilor externi să acceseze sistemul în mod neautorizat;
* care permit implicarea sistemului într-un atac asupra unui terț utilizator, de exemplu atacul DDoS (Distributed Denial of Service).

O clasificare poate fi făcută după gradul de pericol pe care îl reprezintă vulnerabilitățile pentru sistemul informatic supus atacului. Astfel, în funcție de pericolul prezentat, vulnerabilitățile prezintă 3 grade notate cu A, B și C.

Vulnerabilitățile de clasă C, cele care permit atacuri prin refuzul serviciilor, sunt vulnerabilități ale sistemului de operare, în special ale funcțiilor de rețea. Aceste vulnerabilități permit utilizatorilor externi să altereze serviciile de rețea ale unui sistem informatic, sau, în anumite cazuri, transformă sistemul victimă într-un sistem zombie ce va putea fi implicat ulterior într-un atac de tip DDoS. Aceste vulnerabilități, dacă sunt exploatate, duc la încetinirea sau la oprirea temporară a serviciilor de rețea oferite, cum este cazul unor servere HTTP, FTP sau de poștă electronică. Vulnerabilitățile de clasă C nu sunt considerate foarte grave deoarece implică doar alterarea serviciilor, nu și a datelor. Cu toate acestea, în anumite domenii în care se pune accent mare pe disponibilitatea datelor, aceste vulnerabilități reprezintă un risc ridicat.

Vulnerabilitățile ce permit utilizatorilor locali să-și extindă privilegiile fără autorizație, vulnerabilitățile de clasă B, ocupă o poziție medie pe scara consecințelor. Prin aceste vulnerabilități, un utilizator cu un cont limitat va putea obține privilegii de administrator în sistemul informatic respectiv. Tipurile de atac care permit mărirea privilegiilor unui utilizator într-un sistem informatic sunt atacurile buffer overflow. În urma unor erori de programare, unele aplicații alocă un spațiu insuficient de memorie pentru stocarea informațiilor. În momentul în care spațiul de memorie este total ocupat, informațiile ce depășesc spațiul alocat sunt stocate la o altă adresă din memorie. Prin manevrarea acestor adrese, un atacator poate executa diverse comenzi cu aceleași drepturi ca ale programului respectiv. Cum programul de regulă are drepturi de administrator în sistemul de operare, atacatorul care exploatează vulnerabilitatea buffer overflow poate executa comenzi în sistem cu drepturi de administrator. Vulnerabilitățile de clasă B sunt considerate vulnerabilități grave deoarece pot permite accesul unor utilizatori neautorizați la informații importante din sistem.

Vulnerabilitățile de tip A, cele mai grave pe scara consecințelor, permit utilizatorilor externi accesul la sistemul informatic. Prin atacuri cu troieni sau viermi informatici se pot deschide breșe în securitatea sistemului informatic prin care un utilizator extern se poate conecta în mod neautorizat la sistem. Sunt considerate vulnerabilități deosebit de grave deoarece permit accesul utilizatorilor la sistemul de operare și la baza de date a sistemului, aceștia putând fura sau chiar șterge datele importante.

Cauzele apariției vulnerabilităților într-un sistem informatic sunt multiple, câteva dintre acestea fiind:

* erorile existente la nivelul sistemelor de operare sau al aplicațiilor;
* configurarea necorespunzătoare a sistemului de operare sau a aplicațiilor;
* cunoștințele limitate ale administratorilor de sistem sau de rețea;
* lipsa suportului dezvoltatorilor de software în rezolvarea erorilor identificate în aplicațiile software.

Nu în ultimul rând, cele mai mari vulnerabilități sunt cele umane, date de personalul ce se ocupă de configurarea și administrarea sistemelor informatice. Prin lipsa experienței sau printr-o documentare inadecvată privind anumite configurări ale sistemului de operare sau ale aplicațiilor instalate, securitatea cibernetică poate fi total compromisă. Un tip aparte îl reprezintă vulnerabilitățile de tip zero-day, necunoscute dezvoltatorilor și furnizorilor de software și care pot fi exploatate de criminalii cibernetici.

Orice sistem informatic are vulnerabilități, astfel că putem spune că nu există un sistem 100% sigur. Aceste vulnerabilități sunt folosite de multe tipuri de atacuri ce vizează un sistem informatic în mod direct, cum ar fi atacurile de tip malware, sau indirect, în cazul implicării sistemului informatic într-un atac de tip DDoS.

# Provocările în domeniul securității cibernetice în Republica Moldova

Securitatea cibernetică este un domeniu foarte important și actual, care se referă la protecția datelor, sistemelor și rețelelor informatice de la atacuri sau amenințări din spațiul virtual. Republica Moldova, ca și alte state, se confruntă cu provocări în acest domeniu, dar și cu oportunități de a contribui la securitatea cibernetică la nivel regional și global.

Una dintre provocările majore este lipsa unui cadru legal și instituțional adecvat pentru a gestiona riscurile și incidentele cibernetice. Deși Republica Moldova a adoptat în 2018 Strategia Națională de Securitate Cibernetică și Planul de Acțiuni pentru implementarea acesteia, aceste documente nu au fost încă transpuse în legislație și nu au fost create mecanisme eficiente de cooperare între autoritățile responsabile. [De asemenea, Republica Moldova nu a ratificat încă Convenția de la Budapesta privind criminalitatea cibernetică, care este un instrument internațional esențial pentru combaterea acestui fenomen](https://old.academiadepolitie.ro/root/presa/evenimente/2018/Eveniment-7-mai-2018.pdf).

O altă provocare este nivelul scăzut de conștientizare și educație în domeniul securității cibernetice, atât la nivelul populației, cât și al sectorului public și privat. Mulți utilizatori de internet nu cunosc sau nu respectă regulile de bază de securitate cibernetică, cum ar fi folosirea unor parole puternice, actualizarea software-ului, evitarea link-urilor sau atașamentelor suspecte etc. [De asemenea, multe instituții și companii nu au politici și proceduri clare de securitate cibernetică, nu investesc suficient în infrastructura și personalul IT, nu raportează sau nu gestionează corespunzător incidentele cibernetice](https://www.gts.ro/ro/provocari-actuale-in-domeniul-securitatii-cibernetice).

În același timp, Republica Moldova are și potențialul de a contribui la securitatea cibernetică, prin valorificarea resurselor și oportunităților existente. De exemplu, Republica Moldova are un sector IT în plină dezvoltare, cu oameni talentați și inovatori, care pot oferi soluții și servicii de securitate cibernetică. De asemenea, Republica Moldova are un parteneriat strategic cu Uniunea Europeană, care oferă sprijin financiar și tehnic pentru consolidarea capacităților în domeniul securității cibernetice. [În plus, Republica Moldova poate beneficia de cooperarea cu alte state și organizații internaționale, cum ar fi NATO, OSCE, Consiliul Europei, ONU etc., pentru a schimba bune practici și a participa la inițiative comune de securitate cibernetică](https://www.arasec.ro/comunicate-de-presa/studiul-provocari-actuale-in-domeniul-securitatii-cibernetice-impact-si-contributia-romaniei-in-domeniu/).

# Cadrul național în domeniul securității cibernetice

Cadrul normativ privind securitatea cibernetică în Republica Moldova este format din mai multe acte legislative și normative, care reglementează aspectele legate de protecția rețelelor și sistemelor informatice, gestionarea incidentelor cibernetice, cooperarea între autorități și instituții publice, precum și cu partenerii externi, în domeniul securității cibernetice. Printre cele mai importante acte normative se numără:

* Legea nr. 48/2023 privind securitatea cibernetică, care transpune Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune. Această lege stabilește cadrul general de securitate cibernetică, competențele autorităților și instituțiilor publice, cerințele și măsurile pentru asigurarea securității rețelelor și sistemelor informatice esențiale, cadrul național de gestionare a crizelor cibernetice, precum și mecanismele de cooperare națională, regională și internațională în domeniul securității cibernetică.
* Legea nr. 1069/2000 cu privire la informatică, care reglementează activitatea de informatică în Republica Moldova, inclusiv aspectele de securitate a datelor și a sistemelor informatice, precum și responsabilitățile persoanelor fizice și juridice în acest domeniu.
* Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, care stabilește principiile și obiectivele informatizării în Republica Moldova, precum și regimul juridic al resurselor informaționale de stat, inclusiv măsurile de protecție și securitate a acestora.
* Legea nr. 71/2007 cu privire la registre, care reglementează organizarea și funcționarea registrelor de stat, inclusiv aspectele de securitate a datelor și a sistemelor informatice, precum și responsabilitățile persoanelor fizice și juridice în acest domeniu.
* Legea nr. 241/2007 comunicațiilor electronice, care reglementează activitatea de comunicații electronice în Republica Moldova, inclusiv aspectele de securitate a rețelelor și a serviciilor de comunicații electronice, precum și responsabilitățile persoanelor fizice și juridice în acest domeniu.

De asemenea, cadrul normativ privind securitatea cibernetică în Republica Moldova ține cont și de angajamentele internaționale ale Republicii Moldova, cum ar fi Acordul de Asociere cu Uniunea Europeană, Convenția de la Budapesta privind criminalitatea cibernetică, Strategia NATO de securitate cibernetică, etc.

# Impactul Republicii Moldova în domeniul securității cibernetice

Republica Moldova este o țară care contribuie la securitatea cibernetică prin adoptarea și implementarea unui cadru legal și instituțional adecvat, prin cooperarea cu partenerii internaționali și prin dezvoltarea capacităților și a culturii de securitate cibernetică în rândul populației și al sectorului public și privat.

Republica Moldova a adoptat în 2023 Legea privind securitatea cibernetică. Republica Moldova a ratificat în 2022 Convenția de la Budapesta privind criminalitatea cibernetică, care este un instrument internațional esențial pentru combaterea acestui fenomen. Convenția prevede măsuri de armonizare a legislației penale, de cooperare judiciară și de asistență tehnică în domeniul prevenirii și reprimării infracțiunilor informatice. Republica Moldova beneficiază de sprijinul financiar și tehnic al Uniunii Europene pentru consolidarea capacităților în domeniul securității cibernetică. De exemplu, UE a oferit asistență prin intermediul „Proiectului de Asistență Rapidă pentru Securitate Cibernetică pentru Republica Moldova”, care a sprijinit elaborarea Legii privind securitatea cibernetică și a altor acte normative în domeniu. De asemenea, UE a finanțat proiecte de dezvoltare a infrastructurii și a resurselor umane în domeniul securității cibernetică.

Republica Moldova cooperează cu alte state și organizații internaționale, cum ar fi NATO, OSCE, Consiliul Europei, ONU etc., pentru a schimba bune practici și a participa la inițiative comune de securitate cibernetică. De exemplu, Republica Moldova a participat la exercițiile de securitate cibernetică organizate de NATO, cum ar fi „Cyber Coalition” sau „Locked Shields”. De asemenea, Republica Moldova a aderat la Rețeaua Globală de Echipe de Răspuns la Incidente de Securitate Cibernetică (FIRST), care facilitează schimbul de informații și de experiență în domeniu.

Republica Moldova are un sector IT în plină dezvoltare, cu oameni talentați și inovatori, care pot oferi soluții și servicii de securitate cibernetică. De exemplu, Republica Moldova a fost recunoscută ca unul dintre cele mai bune locuri din lume pentru a externaliza servicii IT, inclusiv de securitate cibernetică. De asemenea, Republica Moldova a găzduit evenimente și concursuri de promovare a securității cibernetică, cum ar fi „Moldova Cyber Week” sau „Hackathonul Național de Securitate Cibernetică”. Acestea sunt doar câteva exemple de contribuții ale Republicii Moldova în domeniul securității cibernetică, care arată angajamentul și responsabilitatea țării pentru a asigura un spațiu cibernetic sigur și rezilient, atât la nivel național, cât și la nivel regional și global.

# Concluzii

Securitatea cibernetică este un domeniu foarte important și actual, care se referă la protecția datelor, sistemelor și rețelelor informatice de la atacuri sau amenințări din spațiul virtual. Republica Moldova, ca și alte state, se confruntă cu provocări în acest domeniu, dar și cu oportunități de a contribui la securitatea cibernetică la nivel regional și global.

Provocările actuale în domeniul securității cibernetice sunt legate de lipsa unui cadru legal și instituțional adecvat, nivelul scăzut de conștientizare și educație în domeniul securității cibernetice, precum și de creșterea numărului și complexității atacurilor cibernetice. Aceste provocări pot avea un impact negativ asupra securității naționale, economice și sociale a Republicii Moldova, precum și asupra drepturilor și libertăților cetățenilor săi.

Contribuția Republicii Moldova în domeniul securității cibernetice este reflectată în adoptarea și implementarea unui cadru legal și instituțional adecvat, cooperarea cu partenerii internaționali și dezvoltarea capacităților și a culturii de securitate cibernetică în rândul populației și al sectorului public și privat. Cooperarea la nivel internațional este esențială pentru combaterea amenințărilor cibernetice, iar Republica Moldova poate contribui prin implicarea activă în organizații și inițiative internaționale. Adoptarea și implementarea unei legislații adecvate în domeniul securității cibernetice și stabilirea unor structuri eficiente pentru gestionarea și răspunsul la incidente sunt esențiale. Implicarea sectorului privat în asigurarea securității cibernetice este la fel de importantă ca și intervenția guvernului, având în vedere că multe dintre infrastructurile critice sunt deținute și gestionate de către entități private. Republica Moldova poate contribui la securitatea cibernetică prin consolidarea capacităților naționale, participarea activă în comunitatea internațională, promovarea standardelor și practicilor bune, și dezvoltarea parteneriatelor cu alte state și organizații. Aceste contribuții pot avea un impact pozitiv asupra securității cibernetică a Republicii Moldova, precum și asupra cooperării și integrării regionale și globale a țării.

Prin urmare, securitatea cibernetică este un domeniu vital pentru Republica Moldova, care necesită o abordare integrată și coordonată, bazată pe angajamentul și responsabilitatea tuturor actorilor implicați. Republica Moldova are provocări, dar și oportunități în acest domeniu, care pot fi valorificate prin acțiuni concrete și cooperare eficientă.

# Bibliografie

1. Securitatea Cibernetică. Ministerul Dezvoltării Economice și Digitalizării. <https://mded.gov.md/domenii/tehnologia-informatiei-si-digitalizare/securitatea-cibernetica/>
2. Securitatea cibernetică: în ce fel combate UE amenințările cibernetice. <https://www.consilium.europa.eu/ro/policies/cybersecurity/>
3. Provocări în domeniul securității cibernetice în contextul transformării digitale. <https://ipre.md/2022/10/11/provocari-in-domeniul-securitatii-cibernetice-in-contextul-transformarii-digitale/>
4. Cadrul nomativ. Serviciul Tehnologia Informației și Securitatea Cibernetică. <https://stisc.gov.md/ro/cadrul-legislativ>
5. Moldova Cyber Week 2020. <https://eufordigital.eu/moldova-cyber-week-2020/>
6. Locked Shields 2023: Румыния объединилась с Республикой Молдова в крупнейших учениях по киберзащите. <https://serjmin.com/locked-shields-2023-krupnejshie-uchenija-po-kiberzashhite/>
7. Parteneriate. Serviciul Tehnologia Informației și Securitatea Cibernetică. <https://stisc.gov.md/ro/parteneriate>