CANCELARIA DE STAT A REPUBLICII MOLDOVA

Nr. 21-05-8788 Chișinău 31. 10. 2018

Biroul Permanent
al Parlamentului

În temeiul art.73 din Constituția Republicii Moldova, se prezintă spre examinare proiectul de hotărîre a Parlamentului pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului pentru implementarea acesteia, aprobat prin Hotărîrea Guvernului nr.992 din 10 octombrie 2018.

Responsabil de prezentarea în Parlament a proiectului de hotărîre a Parlamentului este Serviciul de Informații și Securitate.

Anexe:

1. Hotărîrea Guvernului cu privire la aprobarea proiectului de hotărîre a Parlamentului (în limba română – 1 filă și în limba rusă – 1 filă);
2. Proiectul de hotărîre a Parlamentului (în limba română – 61 file și în limba rusă – 76 file);
3. Nota informativă la proiectul de hotărîre a Parlamentului (în limba română – 8 file și în limba rusă – 9 file);
4. Avizele și recomandările, în original, recepționate în cadrul avizării și consultărilor publice (29 file);
5. Raportul de expertiză, în original (4 file);
6. Sinteza obiecțiilor și propunerilor (recomandărilor) la proiectul de hotărîre a Parlamentului, în original (28 file).

Secretar general adjunct al Guvernului **Roman CAZAN**

SECRETARIATUL PARLAMENTULUI
REPUBLICII MOLDOVA
D.D.P. Nr. 373
„01" 11 2018
Ora

Ex.: N. Sandu
Tel.: 022 250 579

Casa Guvernului,
MD-2033, Chișinău,
Republica Moldova
Telefon:
+ 373 22 250 101
Fax:
+ 373 22 242696

GUVERNUL REPUBLICII MOLDOVA

H O T Ă R Î R E nr.992

din 10 octombrie 2018
Chișinău

Privind aprobarea proiectului de hotărîre a Parlamentului pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia

---

În scopul executării articolului 3 din Legea nr. 299/2017 privind aprobarea Concepției securității informaționale a Republicii Moldova (Monitorul Oficial al Republicii Moldova, 2018, nr. 48-57, art. 122), Guvernul HOTĂRĂŞTE:

1. Se aprobă şi se prezintă Parlamentului spre examinare proiectul de hotărîre a Parlamentului pentru aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia (se anexează).

2. Finanțarea acțiunilor prevăzute în Planul de acțiuni privind implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 se va efectua din contul și în limitele mijloacelor aprobate în bugetele instituțiilor responsabile de implementare. Costurile estimative ale acţiunilor vor fi ajustate pe perioada implementării Planului de acţiuni ţinînd cont de volumele alocaţiilor disponibile în bugetul de stat.

Prim-ministru **PAVEL FILIP**

Contrasemnează:

Ministrul finanţelor Octavian Armaşu

Ministrul justiţiei Victoria Iftodi

Y:\006\ANUL 2018\HOTARIRI\17026\17026-redactat-ro.docx

Proiect

PARLAMENTUL REPUBLICII MOLDOVA

HOTĂRÎRE
privind aprobarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024 şi a Planului de acţiuni pentru implementarea acesteia

Parlamentul adoptă prezenta hotărîre.

Art. 1. – Se aprobă:

1) Strategia securităţii informaţionale a Republicii Moldova pentru anii 2019-2024, conform anexei nr.1;

2) Planul de acţiuni pentru implementarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024, conform anexei nr. 2.

Art. 2. – Ministerele, instituţiile şi alte autorităţi administrative centrale vor prezenta anual Serviciului de Informaţii şi Securitate al Republicii Moldova, începînd cu anul 2020, pînă la data de 1 martie, informaţia despre executarea Planului de acţiuni pentru implementarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024, conform competenţelor stabilite.

Art. 3. – Serviciul de Informaţii şi Securitate al Republicii Moldova va prezenta anual Parlamentului, pînă la data de 31 martie, un raport privind implementarea Strategiei şi realizarea Planului de acţiuni, menţionate la art. 1, şi va plasa pe pagina web oficială raportul privind rezultatele implementării acesteia.

Art. 4. – Monitorizarea şi evaluarea implementării Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024 se va realiza prin intermediul instrumentelor prevăzute de către aceasta.

Preşedintele Parlamentului

Anexa nr. 1

STRATEGIA SECURITĂȚII INFORMAȚIONALE A REPUBLICII MOLDOVA PENTRU ANII 2019-2024

I. INTRODUCERE

1. Tehnologiile informaţionale, resursele de informare şi sistemele de comunicare electronică au devenit parte indispensabilă a tuturor domeniilor de activitate a persoanei, societăţii şi statului. Prin dezvoltarea accelerată, tehnologiile informaţionale contribuie la transformări sociale de esenţă, fiind generatorul apariţiei şi consolidării societăţii informaţionale, de nivel naţional, regional şi internaţional, ce depăşesc cadrul juridic al frontierelor de stat sau comunităţi de state.

2. Spaţiul informaţional a devenit un domeniu vital de activitate pentru stat, economie, ştiinţă, societate şi individ, un spaţiu nou de reglementare a drepturilor şi libertăţilor fundamentale ale omului, cu implicare directă şi indirectă asupra mecanismelor de asigurare a politicilor de securitate şi apărare naţională într-o societate democratică.

3. Pe parcursul ultimului deceniu, Republica Moldova a realizat mai multe strategii, programe şi politici de ţară pentru dezvoltarea societăţii informaţionale la nivel naţional, în conformitate cu recomandările forurilor europene şi internaţionale din domeniul tehnologiilor informaţionale şi comunicaţiilor electronice, drepturilor şi libertăţilor fundamentale ale omului în mediul on-line şi off-line.

4. Potrivit Raportului anual cu privire la monitorizarea evoluției societății informaționale la nivel mondial „Measuring the Information Society 2017", lansat de Uniunea Internațională a Telecomunicațiilor, Republica Moldova este plasată pe locul 59 din 176 de state incluse în clasament. La nivel european, Republica Moldova a avansat față de media globală și din regiune, fiind printre primele 10 state cu cele mai dinamice evoluții la nivel mondial[1]. Sînt implementate sau sunt în proces continuu de dezvoltare peste 21 de programe[2] și proiecte on-line de infrastructură și servicii publice digitale, sunt lansate strategii sectoriale în domeniul tehnologiei informației și politici de modernizare tehnologică a guvernării.

5. Interacţiunea tehnologiilor informaţionale, cu diversitatea conţinutului informaţional, pe de o parte, şi fuziunea reţelelor de comunicare publică şi

[1] www.mei.gov.md/ro/content/republica-moldova-urcat-4-pozitii-raportul-mondial-privind-evolutia-societatii;
[2] Potrivit Capitolului II, Secţiunea 2.3, pct.2.3.1 din Strategia naţională de dezvoltare a Societăţii Informaţionale„Moldova Digitală 2020" aprobată prin Hotărîrea Guvernului nr. 857 din 31.10.2013.

socială, cu sistemele electronice guvernamentale, pe de altă parte, contribuie la o extindere şi sinergie a spaţiului informaţional, cu domeniile centrale de securitate şi apărare naţională, responsabile de asigurare a suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

6. Tehnologiile informaţionale generează modificări a dimensiunii de informare şi comunicare, care se transformă într-un ritm accelerat într-o platformă multimedia, fiind dezvoltate noi componente şi mijloace de comunicare on-line şi off-line, iar libera circulaţie a informaţiilor şi ideilor la nivel local, regional şi global devin un imperativ pentru crearea şi promovarea unei societăţi informate într-un stat democratic şi de drept.

7. Tendinţele de dezvoltare continuă a interacţiunii dimensiunii tehnologice cu dimensiunea de informare, în toate formele de structură şi funcţionare, de natură individuală, publică, privată sau de stat, de factură naţională sau globală, conduce la apariţia unei noi configuraţii de comunicare şi schimb de date pe domeniile publice şi private de care depinde nivelul şi starea sectorială sau generală de securitate.

8. Pe lîngă beneficiile incontestabile a tehnologiei moderne, spaţiul informaţional este supus unui şir de vulnerabilităţi, riscuri şi ameninţări de securitate, facilitînd competiţia injustă, confruntarea şi spionajul, dezinformarea şi propaganda, terorismul şi criminalitatea, iar încălcările de confidenţialitate duc la răspîndirea de noi forme de ură şi incitare la violenţă, în special pe motive de gen, rasă, naţionalitate, origine etnică, limbă, religie, apartenenţă politică sau pe orice alt criteriu care rămîn subestimate şi, rareori, remediate sau contracarate.

9. Propagarea informaţiei, fără a ţine seama de limitele frontierelor naţionale, pe lîngă efectele evident benefice, poate duce la sporirea capabilităţii de influenţă din partea actorilor străini guvernamentali sau neguvernamentali cu resurse suficiente.

10. Crimele cibernetice, spionajul, propaganda, diversiunea şi exploatarea excesivă a datelor cu caracter personal prin reţelele de comunicaţii electronice, sînt utilizate ca instrumente de bază la toate etapele de concepere a unei ameninţări hibride de securitate şi cheamă la un răspuns colectiv şi reglementat, bazat pe mecanisme şi acţiuni coordonate, de implementare a politicilor din domeniu, asistenţă tehnică şi legală din perspectiva imperativelor de securitate, orientat la crearea unui mediu informaţional favorabil şi sigur pentru cetăţean, pentru mediul de afaceri de orice nivel şi pentru stat.

11. Campaniile de dezinformare sînt orientate spre accentuarea neîncrederii, confuziei şi destabilizării situaţiei sociopolitice a statului, influenţarea percepţiilor şi preferinţelor existente între diferite comunităţi sociale. Acest fapt poate duce la controlul de către diverşi actori a

comportamentului unei părţi a societăţii, precum şi influenţa politicilor interne şi externe ale statului.

12. Creşterea numărului de utilizatori ai Internetului şi evoluţiile tehnologiilor informaţionale conexe creează provocări substanţiale faţă de starea mediului de securitate, ordinea publică şi apărare, prevenirea criminalităţii şi aplicarea legii în direcţia protecţiei drepturilor în spaţiul informaţional.

13. Concepţia securităţii informaţionale a Republicii Moldova (în continuare – *Concepţie*), aprobată prin Legea nr. 299/2017, reprezintă documentul de bază pentru elaborarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024 (în continuare – *Strategie*) şi documentul de politici ce integrează domeniile centrale şi asociate spaţiului informaţional, oferă noţiuni, defineşte principiile de organizare la nivel de stat, societate şi persoană, precum şi detaliază metodele juridice, tehnico-organizatorice, economice şi contrainformative, pentru asigurarea securităţii informaţionale a Republicii Moldova.

14. Scopul prezentei Strategii este de a corela (juridic) şi de a integra sistemic domeniile prioritare cu responsabilităţi şi competenţe de asigurare a securităţii informaţionale la nivel naţional, bazat pe rezilienţă cibernetică, pluralism multimedia şi convergenţă instituţională în materie de securitate, destinate protejării suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

15. Prezenta Strategie descrie situaţia curentă în domeniul securităţii informaţionale, din perspectiva progreselor înregistrate şi a tendinţelor de dezvoltare a societăţii informaţionale de nivel naţional, problemele existente şi de perspectivă, care generează şi creează riscuri şi ameninţări de securitate inclusiv hibride. Complexul de acţiuni, conform scopului şi obiectivelor specificate sînt compartimentate pe patru piloni:

1) Pilonul I. Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice;

2) Pilonul II. Asigurarea securităţii spaţiului informaţional-mediatic;

3) Pilonul III. Consolidarea capacităţilor operaţionale;

4) Pilonul IV. Eficientizarea procesului de coordonare internă şi cooperare internaţională în domeniul securităţii informaţionale.

16. Scopul şi obiectivele prezentei Strategii se vor realiza în baza Planului de acţiuni pentru implementarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024.

II. DESCRIEREA SITUAȚIEI

17. Republica Moldova, în calitate de parte integrantă a spațiului european, parcurge un proces de tranziție către o societate de tip informațional. Potrivit prevederilor Acordului de Asociere între Republica Moldova, pe de o parte, și Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de altă parte[3], sînt stabilite priorități de încurajare și promovare a punerii în aplicare a instrumentelor tehnologiilor informației și comunicațiilor (în continuare – *TIC*) pentru o mai bună guvernare, e-learning și cercetare, servicii publice de asistență medicală, digitizarea patrimoniului cultural, dezvoltarea conținutului digital și a comerțului electronic, precum și „îmbunătățirea nivelului de securitate a datelor cu caracter personal și a protejării confidențialității în comunicațiile electronice".

18. În cadrul societății informaționale, a estima puterea și viabilitatea sistemului de securitate națională fără a lua în considerare sistemele informaționale și modul de exploatare a informației (colectarea, protecția, transportul, managementul și îngrădirea accesului la informație) reprezintă un risc major, deoarece centrul de greutate al acțiunilor tinde să se deplaseze dinspre dimensiunea materială spre cea informațională. Pe de o parte, utilizarea tehnologiei informației oferă o creștere semnificativă a puterii și viabilității sistemului de securitate națională, iar pe de altă parte reprezintă un factor de risc în situația neprotejării infrastructurii informaționale.

19. Dezvoltarea infrastructurii informaționale, în curs de globalizare, în care se includ și structurile mediatice generează posibilități de comunicare din ce în ce mai sofisticate. Noțiunea de război clasic cedează terenul războiului informațional, care deja are mai multe forme/dimensiuni de manifestare: război psihologic, război imagologic, război de comandă-control, război electronic.

20. Domeniile politic, economic, social și militar sînt ținte ale războiului informațional care tinde, în mod special, spre influențarea proceselor decizionale. În aceste condiții, asigurarea securității informaționale este esențială pentru a întări discernămîntul social, atașamentul și interesul societății. Asigurarea securității informaționale este necesară și pentru contracararea supracomunicării și abuzului informațional, care duc la noncomunicare și pseudocomunicare, elemente ce generează rupturi sociale și dezechilibre în societatea civilă.

21. Interacțiunea în spațiul cibernetic este facilitată de diverși actori: persoane fizice și juridice, autorități de stat și structuri neguvernamentale, grupuri formale și neformale, utilizatori personalizați și anonimi. Unii conectează utilizatorii, permit prelucrarea informațiilor, găzduiesc servicii web,

3 Capitolul 18 „Societatea Informațională", Articolul 98 din Acordul de Asociere între RM și UE.

inclusiv conţinutul generat de utilizatori, alţii cumulează informaţii şi permit căutări, oferind accesul la conţinut, gazdă, indicatori şi servicii create sau operate de persoane terţe. O altă categorie de actori facilitează vînzarea de bunuri şi servicii, inclusiv servicii audiovizuale şi permit alte tranzacţii comerciale, de publicitate şi plăţi.

22. Protecţia drepturilor şi libertăţilor persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal necesită adoptarea de măsuri tehnice şi organizatorice corespunzătoare. În acest sens, operatorul de date cu caracter personal ar trebui să adopte politici interne şi să pună în aplicare măsuri care să respecte în special principiul protecţiei datelor începînd cu momentul conceperii şi cel al protecţiei implicite a datelor, în corespundere cu legislaţia privind protecţia datelor cu caracter personal.

23. Actorii din spaţiul cibernetic pot modera şi pot plasa conţinutul, inclusiv prin prelucrarea automată a datelor cu caracter personal, şi pot exercita alte forme de control care influenţează accesul utilizatorilor la informaţii on-line în moduri similare cu media sau pot îndeplini funcţii asemănătoare celor editoriale. Serviciile de informare on-line sînt oferite şi de mass-media tradiţională, prin intermediul platformelor electronice create în acest sens.

24. Conştientizînd importanţa promovării sectorului TIC pentru dezvoltarea unei societăţi informaţionale avansate în Republica Moldova, crearea şi dezvoltarea unei infrastructuri infocomunicaţionale integrate şi eficiente, orientate spre creşterea competitivităţii economiei naţionale şi asigurarea accesului tuturor cetăţenilor la serviciile societăţii informaţionale, au fost ajustate, completate şi chiar elaborate acte normative, ce reglementează insuficient raporturile subiecţilor spaţiului informaţional.

25. Principalele documente de politici existente la elaborarea prezentei Strategii, valabile pînă în 2020, tangenţiale dimensiunii securităţii informaţionale, care urmează să transpună la nivel naţional modelul european de dezvoltare a societăţii informaţionale sînt: Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020", aprobată prin Hotărîrea Guvernului nr. 857/2013, şi Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărîrea Guvernului nr. 811/2015.

26. Potrivit Planului de acţiuni privind implementarea Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, în perioada de referinţă, sînt prevăzute pentru realizare 50 de acţiuni. Acţiunile din Planul de acţiuni privind implementarea Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 sînt repartizate pe următoarele domenii de intervenţie:

1) procesarea, stocarea şi accesarea în siguranţă a datelor, inclusiv a celor de interes public;

2) securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice;

3) dezvoltarea capacităţilor de prevenire şi reacţie urgentă la nivel naţional (crearea reţelei de CERT naţională);

4) prevenirea şi combaterea criminalităţii informatice;

5) consolidarea capacităţilor de apărare cibernetică;

6) educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice;

7) cooperarea şi interacţiunea internaţională în sferele ce ţin de securitatea cibernetică.

27. Concomitent, în pct. 26 din Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, se remarcă faptul că compartimentul de apărare cibernetică a Republicii Moldova urmează a fi încadrat ca parte componentă a prezentei Strategii. În acest sens, prezenta Strategie propune reglementarea şi abordarea unor segmente ale securităţii informaţionale neelucidate anterior.

28. Subsecvent, constatăm că legislaţia pertinentă la momentul actual nu reglementează prevenirea şi combaterea tentativelor de dezinformare şi/sau de informare manipulatoare, protecţia vieţii private şi a datelor cu caracter personal la plasarea informaţiei în Internet, din considerent că acţiunea acestor legi este restrînsă şi/sau au alt scop de reglementare.

29. În aceste condiţii, Legea nr. 299/2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova poate fi considerată un punct de pornire pentru consolidarea protejării intereselor persoanelor, societăţii şi statului în domeniul informaţional, pentru prevenirea şi contracararea ameninţărilor complexe şi persistente la adresa securităţii informaţionale, a obiectivelor vitale şi de importanţă strategică pentru securitatea naţională, asigurarea protecţiei informaţiei atribuite la secret de stat, de prevenire şi combatere a criminalităţii informatice.

30. Analiza evoluţiei fenomenului mediei de socializare online şi a presei electronice reliefează reglementarea insuficientă a componentei de protecţie a spaţiului mediatic de la ameninţări cu caracter hibrid şi a componentei de securitate. În acest context, este confirmată importanţa şi necesitatea unei strategii care să cuprindă reglementări comprehensive a tuturor vectorilor securităţii informaţionale.

31. Procesul de implementare a tehnologiilor informaţionale în toate domeniile vieţii economice, sociale şi de altă natură a Republicii Moldova, a determinat şi evoluţia criminalităţii informatice. Ca urmare, în ultimii ani s-a

atestat că sistemele, rețelele și datele informatice sînt folosite tot mai frecvent în scopuri criminale, iar materialele ce ar putea constitui probe ale acestor infracțiuni sînt stocate și transmise tot prin intermediul acestor rețele de către făptuitori.

32. Riscurile din spațiul cibernetic sînt proporționale cu gradul de informatizare a societății, iar combaterea fenomenului de criminalitate cibernetică trebuie să constituie o preocupare majoră a tuturor actorilor implicați. Mediul virtual facilitează comiterea infracțiunilor, pune la dispoziția conduitei criminale atît un nou obiect (informația conținută și procesată de sistemele informatice), cît și un nou instrument. Acesta oferă un repertoriu vast de tehnici și strategii de săvîrșire a infracțiunilor, generînd tendințe noi de infracțiuni.

33. Fraudele informatice, atacurile informatice, fraudele cu mijloace de plată electronice și pornografia infantilă în rețeaua globală Internet sînt tipuri de infracțiuni care necesită investigații specializate, o pregătire și dotare corespunzătoare a organelor de drept. Criminalitatea informatică este un fenomen infracțional care alimentează, la rîndul său, foarte multe riscuri și crize în spațiul cibernetic, iar prevenirea și combaterea criminalității informatice trebuie să constituie o preocupare majoră a tuturor actorilor implicați, mai ales la nivel instituțional, unde se concentrează responsabilitatea elaborării și aplicării de politici coerente în domeniu.

34. Adoptarea prezentei Strategii este determinată de necesitatea protecției intereselor persoanelor, societății, statului în spațiul informațional, de gravitatea și multitudinea amenințărilor la adresa securității informaționale în societatea modernă, de necesitatea menținerii unui echilibru între interesele persoanelor, societății și statului pentru asigurarea securității informaționale. Totodată, natura globală a sistemelor informaționale și a rețelelor de comunicații electronice necesită o coordonare strînsă între toate instituțiile responsabile atît la nivelul național, cît și la nivel global.

III. DEFINIREA PROBLEMELOR

3.1. Componenta de securitate cibernetică și investigarea criminalității informatice.

35. În prezent, accesarea neautorizată a rețelelor și serviciilor de comunicații electronice, modificarea, ștergerea sau deteriorarea neautorizată de date informatice, restricționarea ilegală a accesului la aceste date și spionajul cibernetic constituie constrîngeri la nivel global. Rapoartele anuale ale agențiilor internaționale de specialitate constată creșterea costului global al criminalității cibernetice, prejudiciile economice fiind estimate la ordinul sutelor de miliarde de dolari SUA.

36. Ameninţările şi riscurile, atacurile şi incidentele cibernetice, precum şi alte evenimente survenite în spaţiul cibernetic se materializează prin exploatarea vulnerabilităţilor de natură umană, tehnică şi procedurală. Pe aceste căi, în perioada ultimilor ani în Republica Moldova s-au atestat creşteri ai indicatorilor: numărul infracţiunilor şi contravenţiilor informatice; numărul atacurilor cibernetice asupra resurselor informaţionale publicate în reţeaua globala Internet, vulnerabilităţile aplicaţiilor fiind exploatate în scopuri de sustragere/modificare/ ştergere a informaţiei.

37. Pînă în prezent, la nivel naţional nu au fost efectuate procese de audit complexe de securitate cibernetică, nu există studii sau rapoarte[4] care ar reflecta în detalii situaţia privind criminalitatea informatică (riscurile şi ameninţările cibernetice, atacurile şi incidentele cibernetice, alte evenimente survenite în spaţiul cibernetic), cît şi numărul victimelor şi prejudiciilor economice ale materializării acestora.

38. Una dintre problemele de bază este lipsa unui sistem integrat de management al securităţii cibernetice, în cadrul căruia să se efectueze coordonat, planificarea şi utilizarea resurselor disponibile, identificarea vulnerabilităţilor şi riscurilor în urma auditului de securitate cibernetică, a intervenţiilor necesare pentru diminuarea impactului dăunător al criminalităţii, atacurilor şi incidentelor cibernetice asupra dezvoltării sigure a societăţii informaţionale.

39. O altă problemă majoră este lipsa unei entităţi, la nivel naţional, de tip CERT (Centru de reacţie la incidente de securitate cibernetică) responsabile pentru prevenirea şi reacţia la incidente din domeniul securităţii cibernetice, prin coordonarea, planificarea şi utilizarea resurselor disponibile, identificarea vulnerabilităţilor şi riscurilor în urma auditului de securitate cibernetică, a intervenţiilor necesare pentru diminuarea impactului dăunător al criminalităţii, atacurilor şi incidentelor cibernetice asupra dezvoltării sigure a societăţii informaţionale.

40. Lipsa unui sistem integrat de management al securităţii cibernetice la nivel naţional, generează şi lipsa datelor complete, veritabile, actualizate şi structurate, ceea ce, la rîndul său, creează obstacole în identificarea de soluţii optime. De rezultatul soluţionării acestei probleme depinde eficienţa măsurilor ce urmează a fi întreprinse pentru dezvoltarea unei societăţi informaţionale securizate în Republica Moldova, pentru avansarea tehnologică şi ştiinţifică, precum şi dinamica de creştere economică a ţării.

---

[4] *unicele surse oficiale de date statistice privind criminalitatea informatică este Registrul de evidenţă a infracţiunilor, a cauzelor penale, a persoanelor care au săvârşit infracţiuni şi a materialelor cu privire la infracţiuni deţinut de către Ministerul Afacerilor Interne şi Sistemul Informaţional Automatizat „ Urmărire penală: E-dosar" gestionat de Procuratura Generală.*

41. Asigurarea prevenirii riscurilor şi combaterii ameninţărilor în adresa securităţii informaţionale este una dintre sarcinile de bază ale statului, implementate prin instituţiile sale de drept, la acest capitol fiind determinate următoarele probleme care necesită a fi abordate la nivel naţional:

1) insuficienţa specialiştilor calificaţi în domeniul tehnologiilor informaţionale şi nivelul redus de salarizare în special în sectorul public;

2) lipsa programelor de instruire specializate dedicate angajaţilor cu atribuţii de investigare şi urmărire penală, procurorilor, judecătorilor, specialiştilor şi experţilor judiciari în domeniu din cadrul structurilor de aplicare a legii, precum şi a celor dedicate personalului tehnic din cadrul instituţiilor publice în domeniul securităţii cibernetice;

3) dotarea insuficientă cu echipament şi softuri specializate dedicate investigării infracţiunilor informatice,

4) finanţarea redusă pentru participarea specialiştilor la proiectele şi evenimentele internaţionale de consolidare a capacităţilor şi schimbului de bune practici.

42. În cadrul investigării infracţiunilor informatice s-a constatat că tot mai frecvent sînt utilizate tehnologiile care facilitează comiterea infracţiunilor informatice:

1) mijloacele de anonimizare (care ascund datele tehnice de identificare a utilizatorului), punctele de acces wireless cu acces nerestricţionat (deschis) la reţeaua globală Internet în locurile publice;

2) utilizarea algoritmelor complexe asimetrice de criptare a informaţiei critice la estorcarea mijloacelor financiare prin intermediul tehnologiilor informaţionale;

3) utilizarea sistemelor de plată electronice desconcentrate în baza cripto-algoritmelor (criptovaluta);

4) reţelele de schimb direct de date dintre utilizatori, ceea ce nu lasă anumite urme activităţii în conţinutul istoricului înregistrat în sistemul informatic sau în logurile deţinute de furnizorii de servicii;

5) utilizarea web hosting-ului de către infractori;

6) furnizorii „mici de servicii" nu asigură un nivel minim de securitate cibernetică a propriei reţele şi deseori nu duc evidenţa utilizatorilor de servicii şi nu înregistrează metadatele privind accesul la reţeaua Internet;

7) serviciile de Internet fix prestate pe teritoriul Republicii Moldova necontrolat efectiv de autorităţile constituţionale.

43. Consolidarea sistemelor informaţionale şi de comunicaţii electronice speciale într-un mecanism unic pentru funcţionarea sigură şi corectă, nu poate fi efectuată fără existenţa unui cadru normativ actualizat care ar prevedea promovarea dezvoltării a acestor sisteme. La momentul actual, cadrul normativ instituie unele prevederi care produc impedimente în funcţionarea normală a sistemelor informaţionale şi de comunicaţii electronice speciale, inclusiv guvernamentale, ca sisteme informaţionale vitale pentru securitatea statului, prin

introducerea unor constrîngeri în gestionarea, dezvoltarea şi asigurarea securităţii acestora.

44. Resursele disponibile ale instituţiilor de stat sînt insuficiente pentru pregătirea şi instruirea specialiştilor calificaţi, precum şi pentru stimularea acestora, fapt care duce la migrarea specialiştilor în sectorul privat, cu repercusiuni asupra modului de implementare a securităţii cibernetice.

45. Totodată, sistemul de apărare naţională, la fel ca şi alte domenii a devenit dependent de domeniul TIC. Unele componente TIC ale sistemului de apărare naţională sînt integrate cu reţeaua globală Internet, iar reţelele informaţionale de apărare sînt construite pe tehnologii comerciale standarde. Prin urmare, acestea sunt, de asemenea, expuse riscurilor de atacuri cibernetice, prin exploatarea unor vulnerabilităţi.

46. La etapa actuală a progresului tehnologic şi procesului de informatizare a vieţii economice, politice, sociale şi de altă natură, funcţionarea mecanismelor principale ale statului se realizează prin utilizarea produselor program şi schimbului de date digitalizate, care formează în ansamblu infrastructura critică informatică. În contextul dat, este relevant de a elabora şi/sau de a evalua legislaţia deja existentă prin prisma prevederilor Directivei 2008/114/CE privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesităţii de îmbunătăţire a protecţiei acestora, adoptată la 8 decembrie 2008, publicată în Jurnalul oficial al Uniunii Europene L345/75 din 23 decembrie 2008.

3.2. Componenta de securitate a spaţiului mediatic

47. Asigurarea securităţii informaţionale a statului constituie o prioritate pentru securitatea naţională, fiind un obiectiv statuat în mai multe acte legislative şi normative ale Republicii Moldova şi necesită o finanţare suficientă.

48. Conform prevederilor pct. 4.7 din Strategia securităţii naţionale a Republicii Moldova, aprobată prin Hotărîrea Parlamentului nr.153/2011, securitatea informaţională a statului ţine şi de provocările cu caracter mediatic îndreptate împotriva Republicii Moldova, sub formă de dezinformare şi/sau de informare manipulatoare din exterior.

49. Pe parcursul afirmării, consolidării şi dezvoltării sale statale, Republica Moldova a fost supusă în repetate rînduri unor campanii de denigrare informaţională, în special de influenţă externă, cu un impact negativ sporit asupra populaţiei.

50. Intensificarea propagandei şi a dezinformărilor are loc în special în timpul diverselor evenimente de interes naţional, în scopul influenţării deciziei politice atît a statului, cît şi a cetăţeanului. În funcţie de anumite evoluţii interne/externe, se mizează pe crearea unei stări de nemulţumiri sociale.

51. Necesitatea stringentă a protejării securităţii spaţiului informaţional naţional, este conştientizată atît la nivelul autorităţilor administraţiei publice, cît şi reprezintă un deziderat al societăţii civile.

52. Îngrijorarea privind intensificarea atacurilor din exterior la adresa securităţii informaţionale, a fost enunţată inclusiv în Hotărîrea Parlamentului nr. 12/2018 care stipulează că atacurile media din exterior vizează denigrarea Republicii Moldova, a unor instituţii şi a unor oficiali, dar cel mai grav este că vizează denigrarea cetăţenilor ţării.

53. Astfel, Parlamentul constată că „propaganda s-a transformat într-un veritabil instrument de denigrare a Republicii Moldova, fapt menţionat în nenumărate rapoarte prezentate public de către societatea civilă şi organizaţiile internaţionale independente, în special în ultimul an, care au arătat evoluţia tot mai îngrijorătoare a acestui fenomen".

54. Concomitent, subiectul este unul de actualitate atît la nivel internaţional, cît şi regional. În acest sens, prin Rezoluţia din 23 noiembrie2016 referitoare la comunicarea strategică a Uniunii Europene pentru a contracara propaganda părţilor terţe împotriva sa (2016/2030 (INI)), Parlamentul European statuează că „UE, statele sale membre şi cetăţenii săi suportă o presiune crescîndă, sistematică pentru a face faţă campaniilor de informare, de dezinformare, de intoxicare şi de propagandă din partea unor ţări şi actori nestatali, cum ar fi organizaţii teroriste şi criminale transnaţionale din vecinătatea sa, care intenţionează să submineze însăşi noţiunea de informare obiectivă sau de jurnalism etic, difuzînd toate informaţiile sub o formă părtinitoare sau ca instrument de putere politică şi care atacă, de asemenea, valori şi interese democratice".

55. Tehnologiile războiului informaţional sînt folosite pentru a legitima acţiunile care subminează suveranitatea, independenţa şi integritatea teritorială, context în care statele membre UE şi partenerii acestora sînt încurajaţi să realizeze „evaluări critice ale modului în care ar trebui abordate sursele mass-media cu un trecut demonstrat de implicare repetată într-o strategie de înşelăciune sau de dezinformare intenţionată, în special în noile mijloace de informare, reţelele sociale şi sfera digitală".

56. La etapa actuală, propaganda, dezinformarea şi/sau informarea manipulatoare sînt extrem de dinamice, iar resursele alocate în acest scop de către terţi depăşesc cu mult capabilităţile de răspuns şi combatere a fenomenului dat ale Republicii Moldova.

57. Pentru a face faţă provocărilor, Republica Moldova beneficiază de suportul Uniunii Europene, care pentru următorii ani şi-a majorat bugetul pentru

combaterea propagandei şi a dezinformării, un accent separat fiind plasat şi pe statele membre ale Parteneriatului Estic.

58. Conştientizarea riscurilor generate de impactul propagandei externe impune măsuri de armonizare a politicilor naţionale, iar adoptarea prezentei Strategii vine în susţinerea acestui deziderat.

3.3. Componenta contrainformativă şi de securitate

59. Arma informaţională, în calitatea sa de componentă esenţială a ameninţărilor hibride, este utilizată de centre externe subversive (servicii speciale, ONG-uri ghidate de actori statali şi non-statali, instituţii media controlabile ş.a.) în punerea pe rol a unor operaţiuni informaţionale sau atacuri cibernetice, subsumate unui anumit scop strategic.

60. Potrivit Rezoluţiei Parlamentului European din 23 noiembrie 2016 referitoare la comunicarea strategică a Uniunii Europene (2016/2030 (INI), „serviciile de securitate şi de informaţii au concluzionat că anumiţi actori non statali au capacitatea şi intenţia de a desfăşura operaţiuni vizînd destabilizarea statelor, subliniind că acest lucru ia adesea forma unui sprijin acordat extremiştilor politici şi a unor campanii de mass-media şi de dezinformare pe scară largă". Este de accentuat că astfel de societăţi mass-media sînt prezente şi active şi în Republica Moldova.

61. Analiza mediului de securitate intern şi regional relevă extinderea la scara largă de către diferiţi actori, utilizarea mijloacelor de imixiune în treburile interne ale Republicii Moldova prin propagandă şi agresiune mediatică, precum şi de influenţa informaţional-psihologică, cu scopul de a destabiliza situaţia social-politică, submina suveranitatea şi integritatea teritorială a Republicii Moldova.

62. În aceste activităţi de natură informativ-propagandistică pe segmentul spaţiului mediatic, sînt implicate structuri asociative, centre informativ-analitice, agenţii de presă, precum şi grupuri individuale de cetăţeni finanţaţi de către centrele subversive şi serviciile speciale ale ţărilor străine, care prin tehnologii informaţionale utilizează instrumente hibride de putere subtila (soft power).

63. Periculozitatea acestor tipuri de ameninţări este una foarte ridicată din cauza tacticilor, acţiunilor şi mijloacelor diverse folosite pentru atingerea obiectivelor lor. Astfel, se poate vorbi de ameninţări specifice în materie de securitate, cunoaşterea cărora va permite de a lua măsuri eficace de prevenire şi/sau limitare a efectelor nedorite.

64. Pe alt palier, organizaţiile teroriste islamiste desfăşoară campanii active de informare în scopul subminării şi creşterii nivelului de ură împotriva valorilor şi intereselor europene. Este de remarcat utilizarea răspîndită de către

acestea organizații a instrumentelor media sociale și, în special, a rețelelor de socializare pentru a-și promova obiectivele de propagandă și de recrutare, în special în rîndul tinerilor.

65. În context, la nivel european deja este raționalizată necesitatea de a include „strategia de contra-propagandă împotriva organizațiilor teroriste islamiste" într-o strategie regională mai amplă și cuprinzătoare care să combine instrumentele diplomatice, socio-economice, de dezvoltare și de prevenire a conflictelor.

3.4. Definirea problemelor de natură legală

66. Unii actori statali şi non-statali exploatează lipsa unui cadru juridic internaţional în domenii precum securitatea cibernetică, lipsa de responsabilitate în ceea ce priveşte reglementarea mass-mediei din Internet şi profită de pe urma oricărei ambiguităţi în aceste chestiuni.

67. Pe palierul de securitate cibernetică, Republica Moldova a ratificat Convenţia Consiliului Europei privind criminalitatea informatică prin Legea nr.6/2009. Totodată, a fost adoptată Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice, au fost operate modificări şi completări la Codul penal al Republicii Moldova nr. 985/2002 în corespundere cu prevederile Convenţiei ratificate. Cu toate acestea, nu au fost implementate integral multiple prevederi de ordin material şi procesual, precum şi cele ce ţin de dezvoltarea punctului de contact al reţelei 24/7 nu au fost încă implementate.

68. Complementar este de remarcat că, pînă în prezent, nu există un cadru legal privind delimitarea şi armonizarea competenţelor şi responsabilităţilor instituţiilor statului şi a celor private în domeniul securităţii cibernetice, nu se aplică mecanismul obligatoriu de audit al securităţii cibernetice în cadrul instituţiilor publice şi private, prin care pot fi identificate vulnerabilităţile, riscurile şi ameninţările cibernetice în scopul prevenirii sau diminuării, prin măsuri speciale, a impactului atacurilor, incidentelor şi altor evenimente survenite în spaţiul cibernetic, ale căror origine este dificil de stabilit.

69. În urma analizei legislației naționale în domeniul prevenirii și combaterii criminalității informatice au fost atestate un șir de bariere și lacune de ordin normativ ce includ:

1) Codul penal al Republicii Moldova nr. 985/2002:

a) art. 178 „Violarea dreptului la secretul corespondenţei" nu prevede răspunderea penală pentru faptele comise în privința corespondenței (mesageriei) electronice, întrucît noțiunea „trimiteri poștale", conform Legii comunicațiilor poștale nr. 36/2016, prevede numai bunurile fizice expediate și recepționate;

b) art. 208^1 „Pornografia infantilă" nu incriminează obţinerea accesului cu bună ştiinţă, prin intermediul tehnologiilor informaţionale şi a comunicaţiilor, la pornografia infantilă, deşi aceasta este prevăzut în Convenția Consiliului

Europei pentru protecţia copiilor împotriva exploatării sexuale şi a abuzurilor sexuale, încheiată la Lanzarote la 25 octombrie 2007, ratificat prin Legea nr.263/2011;

c) majoritatea infracţiunilor prevăzute la capitolul XI din Partea Specială a Codului penal al Republicii Moldova nr. 985/2002 (Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor) au componenţă materială şi se consumă doar la provocarea unui prejudiciu în proporţii mari;

2) Codul de procedură penală al Republicii Moldova nr. 122/2003:

a) nu este reglementată procedura „Percheziţiei informatice", prevăzută în Convenţia Consiliului Europei privind criminalitatea informatică (Budapesta, 2001);

b) lipseşte măsura specială de investigaţii de interceptare a datelor informatice;

c) cadrul legal nu permite efectuarea măsurilor speciale de investigaţii necesare la documentarea infracţiunilor informatice;

d) nu este prevăzută restricţionarea accesului la paginile web, inclusiv cele găzduite de furnizorul respectiv, ce conţin informaţii care pericliteză viaţa, sănătatea şi dezvoltarea normală a copiilor, informaţii ce fac propagandă războiului sau terorismului, îndeamnă la ură sau discriminare naţională, rasială ori religioasă, la ostilitate sau violenţă.

70. De asemenea, se constată lipsa unui cadru normativ care ar reglementa infrastructura critică naţională, precum şi lipsa unei clasificări clare a sistemelor informaţionale în funcţie de tipul datelor pe care acestea le conţine, tipul de acces la acestea şi destinaţia acestora, definirea incidentelor de securitate cibernetică, evaluarea şi estimarea prejudiciilor cauzate prin aceste incidente, precum şi sancţiunile care pot fi aplicate în context, inclusiv definirea acţiunilor ce pot cauza incidente de securitate cibernetică. Lipseşte reglementarea normativă a mecanismului de schimb de informaţii cu privire la incidentele de securitate cibernetică dintre persoanele juridice, indiferent de tipul de proprietate al acestora şi dintre persoanele juridice şi persoanele fizice.

3.5. Definirea problemelor de conştientizare a maselor

71. La acest capitol se evidenţiază importanţa sensibilizării, educării, competenţei mediatice şi cibernetice în Republica Moldova, pentru a permite cetăţenilor să analizeze în mod critic conţinutul mediatic, în vederea identificării propagandei.

72. Lipsa capacităţii de protecţie contra fenomenului de defăimare prin intermediul platformelor on-line afectează exercitarea drepturilor omului şi a libertăţilor fundamentale. În aceste condiţii, ajustarea cadrului legislativ naţional la standardele europene pe dimensiunea respectării drepturilor omului în spaţiul informaţional constituie o prioritate incontestabilă pentru Republica Moldova.

73. În acest sens sînt necesare acţiuni de consolidare a cunoştinţelor la toate nivelurile sistemului educaţional, cît şi impulsionarea/încurajarea persoanelor să devină cetăţeni activi şi de a dezvolta conştientizarea lor în calitate de consumatori de mass-media.

74. Un alt element de conştientizat este rolul central al instrumentelor oferite de Internet (în special al reţelelor de socializare) în care răspîndirea de informaţii false şi lansarea de campanii de dezinformare sînt uşor de realizat şi adesea nu întîmpină niciun obstacol.

75. Problema ştirilor false pe parcursul anului 2017 a constituit obiect al şedinţelor Comisiei Europene, care a decis crearea unui Grup de lucru la nivel înalt care va elabora şi va prezenta o strategie de combatere a ştirilor false în 2018, cu un an înaintea alegerilor europene. Evaluările sale relevă că „contracararea propagandei prin propagandă este contraproductivă", statele membre UE fiind îndemnate să o combată doar prin demontarea campaniilor de dezinformare şi prin utilizarea mesajelor şi a informaţiilor pozitive. În acest sens, experţii recomandă „dezvoltarea unei strategii eficace care să nu fie adaptată în funcţie de natura actorilor care diseminează propaganda"[5].

IV. VIZIUNE ŞI OBIECTIVE ALE STRATEGIEI

76. Guvernul Republicii Moldova, autorităţile administraţiilor publice, instituţiile, întreprinderile de stat, indiferent de forma de organizare, şi societatea civilă au stabilit următoarea viziune strategică:

Republica Moldova va asigura un spaţiu informaţional sigur, pentru toţi subiecţii de drept, prin armonizarea cadrului legal şi implementarea acestuia, astfel protejînd drepturile şi libertăţile fundamentale ale omului şi promovînd democraţia şi statul de drept.

77. Pentru realizarea acestei viziuni strategice au fost stabilite obiective generale, acţiuni de implementare şi indicatori de progres.

4.1. Pilonul I. Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice

78. Obiectivul nr. 1. Crearea unui sistem integrat de comunicare şi evaluare a ameninţărilor la adresa securităţii informaţionale şi de elaborare a măsurilor operative de răspuns

Obiectivul menţionat urmează a fi realizat prin următoarele acţiuni:

[5] Conform pct.46 din Comunicarea strategică a UE de contracarare a propagandei părţilor terţe împotriva sa.

1) crearea/desemnarea entității care va exercita rolul de Centru național de reacție la incidentele de securitate cibernetică și care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autoritățile publice competente și persoanele fizice și juridice;

2) desemnarea entității care va exercita rolul de Centru Guvernamental de reacție la incidentele de securitate cibernetică și care va constitui punctul de raportare al incidentelor de securitate cibernetică al Guvernului, precum și stabilirea interacțiunii acestuia cu Centrul național de reacție la incidentele de securitate cibernetică;

3) stabilirea de către Centrul național de reacție la incidente de securitate cibernetică a indicatorilor din domeniul securității cibernetice, sistematizarea datelor statistice la capitolul securității cibernetice, analiza și evaluarea acestora;

4) elaborarea mecanismelor de creare și consolidare a centrelor departamentale de reacție la incidentele de securitate cibernetică și informaționale atît de drept public, cît și de drept privat;

5) elaborarea cadrului normativ pentru asigurarea unui nivel înalt de securitate a rețelelor și a sistemelor informatice la nivel național, în baza bunelor practici UE;

6) determinarea politicii privind modalitatea de raportare, stocare și prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale.

79. Obiectivul nr. 2. Monitorizarea permanentă și asigurarea unui nivel înalt de securitate cibernetică

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

1) identificarea și eliminarea surselor de amenințare la adresa securității persoanei, societății și statului în spațiul cibernetic;

a) efectuarea auditului de securitate cibernetică a infrastructurilor de tehnologie a informației de interes național, precum și a altor infrastructuri cibernetice de interes național, în vederea identificării disfuncțiilor și vulnerabilităților și furnizarea soluțiilor/recomandărilor de remediere a acestora;

b) implementarea rezultatelor auditului de securitate cibernetică;

2) asigurarea aplicării cerințelor minime de securitate cibernetică de nivelul II în cadrul prestării serviciilor electronice publice determinarea direcțiilor de activitate prioritare pentru prevenirea și suprimarea amenințărilor respective;

3) elaborarea mecanismelor și metodelor de prevenire și contracarare a pericolelor în spațiul cibernetic, generate de serviciile informaționale prestate de către persoanele fizice și juridice;

4) identificarea unui mecanism legal de interacțiune între autoritățile publice competente și persoanele fizice și juridice, indiferent de tipul de proprietate, în vederea acordării de către acestea a accesului la codul sursă al aplicațiilor elaborate, comercializate și distribuite pentru autoritățile publice;

5) coordonarea cu Centrul Național pentru protecția Datelor cu Caracter Personal a măsurilor de protecție a datelor cu caracter personal care să asigure

aplicarea principiului protecției datelor începînd de la conceperea și protecția implicită a datelor atunci cînd se elaborează, se proiectează, se selectează și se utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal în corespundere cu legislația privind protecția datelor cu caracter personal.

80. Obiectivul nr. 3. Consolidarea capacităților de apărare cibernetică

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

1) delimitarea și atribuirea rolurilor și responsabilităților privind apărarea cibernetică, a sistemului organelor securității statului și a sistemului național de apărare;

2) elaborarea măsurilor de apărare cibernetică pentru protecția infrastructurii critice naționale, precum și din cadrul altor sectoare prioritare pentru stat;

3) elaborarea și implementarea măsurilor de protecție a sistemelor informaționale ce prelucrează informații atribuite la secret de stat și componentei TIC a sistemelor de apărare națională.

81. Obiectivul nr. 4. Protecția rețelelor de comunicații speciale ale Republicii Moldova și a informației cu accesibilitate limitată, pentru menținerea funcțiilor vitale ale statului

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) dezvoltarea mecanismelor de protecție a sistemelor speciale de comunicații electronice prin aplicarea mijloacelor de protecție criptografică și tehnică a informațiilor;

2) efectuarea controalelor asupra sistemelor speciale de comunicații electronice și raportarea autorității responsabile asupra măsurilor tehnice și tehnico-organizatorice întreprinse pentru asigurarea securității cibernetice;

3) actualizarea cadrului normativ în domeniul sistemelor speciale de comunicații electronice;

4) elaborarea sistemului de atestare a obiectelor de informatizare (articole plasate în rețeaua globală Internet, pagini web informative, baze de date sau alte surse cu caracter informațional) privind îndeplinirea cerințelor de asigurare a protecției informației în timpul efectuării lucrărilor ce țin de prelucrarea și păstrarea informației cu accesibilitate limitată, în special a celei atribuite la secret de stat;

5) stabilirea măsurilor de asigurare a protecției datelor cu caracter personal în contextul asigurării securității cibernetice;

6) promovarea cadrului legislativ privind instituirea subdiviziunilor responsabile de protecția datelor cu caracter personal în cadrul autorităților de drept public și privat.

82. Obiectivul nr. 5. Asigurarea controlului asupra importului, certificării și utilizării mijloacelor de protecție a informației

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) certificarea mijloacelor de protecţie tehnică şi criptografică a informaţiei;

2) dezvoltarea sistemelor de monitorizare a importului mijloacelor de protecţie a informaţie;

3) alinierea cadrului legislativ în domeniul protecţiei criptografice a informaţiei la cadrul normativ european;

4) crearea unei baze de date privind mijloacele de protecţie tehnică şi criptografică a informaţiei;

5) exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice.

83. Obiectivul nr. 6. Combaterea criminalităţii informatice

Obiectivul menţionat urmează a fi realizat prin următoarele acţiuni:

1) eficientizarea capacităţilor (mecanismului) de combatere a criminalităţii informatice;

2) acordarea ajutorului metodico-practic subdiviziunilor teritoriale privind investigarea infracţiunilor informatice;

3) implementarea noilor mecanisme la nivelul instituţiilor implicate în combaterea criminalităţii informatice (atragerea companiilor private şi experţilor independenţi, dezvoltarea laboratoarelor);

4) perfecţionarea cadrului legal ce reglementează salarizarea efectivului specializat în combaterea criminalităţii informatice şi investigarea infracţiunilor informatice.

84. Obiectivul nr. 7. Protecţia copiilor în spaţiul on-line de orice formă de abuz

Obiectivul nominalizat urmează a fi realizat prin următoarele acţiuni:

1) combaterea fenomenului de pornografie infantilă în Internet;

2) combaterea fenomenelor de grooming şi hărţuire sexuală a copiilor în Internet;

3) promovarea unui Internet mai sigur pentru copii prin intermediul consilierilor on-line şi încurajarea raportărilor prin proiecte informaţionale specializate;

85. Obiectivul nr. 8. Combaterea fraudelor prin utilizarea mijloacelor de plată electronice

Obiectivul în cauză urmează a fi realizat prin următoarele acţiuni:

1) schimbul de informaţii dintre Centrul pentru combatere a crimelor informatice cu departamentele de securitate ale instituţiilor financiare.

2) promovarea măsurilor de securitate sporită în privinţa ATM-lor la nivel de hardware şi software.

3) identificarea mecanismelor comune de combatere a fraudelor card-present şi card not-present.

86. Obiectivul nr. 9. Dezvoltarea capacităților instituționale în combaterea criminalității informatice

Obiectivul menţionat urmează a fi realizat prin următoarele acțiuni:

1) dezvoltarea subdiviziunilor specializate în cadrul Inspectoratului General de Poliție al Ministerului Afacerilor Interne, Procuraturii Generale, Serviciului de Informații și Securitate al Republicii Moldova în scopul depistării și contracarării a tentativelor infracționale în domeniu;

2) crearea unei baze de date naționale privind evoluția fenomenului criminalităţii informatice;

3) ajustarea activității desfășurate în domeniul criminalității informatice, în Banca centrală de date a Sistemului informațional automatizat „Registrul informațiilor criminalistice și criminologice";

4) elaborarea cadrului normativ care să reglementeze instituirea Sistemului informațional automatizat „E-dosar" în cadrul organelor implicate la efectuarea urmăririi penale și judecării cauzei, precum și implementarea, dezvoltarea și interconectarea acestuia.

87. Obiectivul nr. 10. Efectuarea cercetărilor ştiinţifice aplicative în domeniul securităţii informaţionale

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) planificarea și dezvoltarea activității de cercetare științifică în domeniul tehnologiei informaționale și comunicaționale;

2) crearea/consolidarea laboratoarelor de securitate cibernetică din cadrul instituțiilor de învățământ superior și instituțiile de cercetare științifică.

88. Obiectivul nr. 11. Dezvoltarea capacităţilor de rezilienţă cibernetică și ridicarea nivelului de cultură în domeniul TIC

Obiectivul menţionat urmează a fi realizat prin următoarele acțiuni:

1) desfășurarea acțiunilor de sensibilizare și informare a societății privind amenințările, vulnerabilitățile și riscurile securității cibernetice;

2) realizarea de către Centrul național de reacție la incidentele de securitate cibernetică a analizei strategice, a incidentelor de securitate cibernetică și coordonarea acțiunilor de răspuns la incidente de securitate, inclusiv prin organizarea cursurilor specializate de către experți calificați;

3) desfășurarea exercițiilor și antrenamentelor comune de consolidare a capacităţilor de reacţie la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate;

4) organizarea și efectuarea atelierelor de lucru în domeniul securității cibernetice pentru personalul din sectorul public şi privat, deţinătorii de elemente de infrastructură critică;

5) certificarea specialiștilor în domeniul securității cibernetice de către organizațiile/companiile specializate pornind de la standardele aplicate și cerințele minime obligatorii de securitate cibernetică aprobate;

6) organizarea campaniilor de sensibilizare şi informare privind pericolele în spaţiul cibernetic şi măsurile de protecţie ce pot fi luate de către persoanele fizice şi juridice;

7) introducerea şi promovarea conţinuturilor curriculare privind securitatea informaţională în programele naţionale de studii;

8) organizarea, inclusiv în comun cu partenerii străini, a cursurilor de instruire tematică în domeniul securităţii cibernetice pentru angajaţii din instituţiile publice;

Priorităţile Pilonului I	Indicatori de rezultat
1. Crearea Centrului naţional de reacţie la incidentele de securitate cibernetică (CERT naţional);	1. Centru naţional creat, care va elabora documente de politici şi va asigura interacţiunea dintre toate componentele de asigurare a securităţii cibernetice
2. Desemnarea entităţii care va exercita rolul de Centru guvernamental de reacţie la incidentele de securitate cibernetică al Guvernului (CERT Gov);	2. Asigurarea de către Centrul guvernamental a funcţionării şi protecţiei reţelelor speciale la nivel de Guvern şi autorităţi publice;
3. Consolidarea cooperării CERT-ului naţional, CERT-ului Gov şi CERT-urilor private.	3. Acorduri de colaborare şi sustenabilitate în scopul prevenirii şi soluţionării incidentelor de securitate cibernetică.

4.2. Pilonul II. Asigurarea securităţii spaţiului informaţional-mediatic

89. Obiectivul nr. 1. Dezvoltarea mecanismelor de comunicare strategică pentru realizarea intereselor naţionale ale Republicii Moldova

Obiectivul dat urmează a fi realizat prin următoarele acţiuni:

1) evaluarea sectoarelor vulnerabile ale componentei mediatice a sistemului de securitate informaţională;

2) dezvoltarea politicilor de comunicare strategică pe plan intern şi racordarea la platformele de comunicare strategică externe, ale structurilor sistemului de securitate, apărare şi ordine publică, pentru asigurarea securităţii informaţionale şi promovarea intereselor naţionale ale Republicii Moldova;

3) crearea, în Republica Moldova, a resursei/platformei informaţionale de comunicare strategică, care v-a conţine informaţii privind:

a) incidente de securitate informaţională;

b) ghiduri de comunicare strategică pe subiecte de interes naţional;

c) tentative şi acţiuni de dezinformare şi/sau informare manipulatorii ce afectează securitatea informaţională şi stare generală de securitate.

90. Obiectivul nr. 2. Controlul civic şi consolidarea cooperării societăţii civile cu autorităţile publice cu atribuţii de asigurare a securităţii informaţionale

Obiectivul dat urmează a fi realizat prin următoarele acţiuni:

1) crearea unui mecanism de implicare a experților din rîndul societății civile, organizațiilor neguvernamentale şi mass-mediei în domeniul securității informaționale, prin:

a) desemnarea unui consiliu existent sau crearea unui organ colectiv din rîndul societății civile cu atribuții de evaluare a experților, organizațiilor neguvernamentale şi mass-mediei, din perspectiva implicării în materie de asigurare a securității informaționale;

b) certificarea de către Consiliul societății civile a experților şi reprezentanților societății civile şi mass-mediei ce se vor preocupa de monitorizarea nivelului de asigurare a securității informaționale la nivel național;

2) implicarea reprezentanților societății civile certificați de Consiliul societății civile în cadrul Consiliului coordonator pentru asigurarea securității informaționale;

3) îmbunătățirea sau crearea mecanismelor de implicare a societății civile în procesele de definire, elaborare, monitorizare şi de evaluare a politicilor de asigurare a securității informaționale realizate de autoritățile abilitate în asigurarea securității informaționale;

4) elaborarea și organizarea unor cursuri de instruire tematică pentru radiodifuzori, distribuitori de servicii, formatori de opinie, jurnaliști și ONG-uri de profil cu privire la tehnicile de dezinformare și/sau informare manipulatoare utilizate pentru prejudicierea securității informaționale a statului.

91. Obiectivul nr. 3. Determinarea statutului juridic al publicațiilor periodice, agențiilor de presă și altor subiecți care activează în spațiului media din Internet

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) evaluarea spațiului Internet din perspectiva identificării actorilor implicați în producerea şi diseminarea conținutului media on-line şi alți intermediari şi servicii auxiliare ce au impact pentru securitatea informațională;

2) elaborarea și ajustarea cadrului legal funcțional în scopul reglementării juridice a raporturilor dintre actorii mass-media care colectează și difuzează informații în Internet, societate și autoritățile abilitate cu atribuții de asigurare a securității informaționale, în conformitate cu recomandările Comisiei Europene și bunele practici europene;

3) implementarea cadrului normativ definit prin acțiuni comune de intervenție și gestionare a spațiului media on-line şi off-line.

92. Obiectivul nr. 4. Asigurarea transparenței financiare în activitatea autorităților administrației publice, a asociațiilor obștești şi a societăților comerciale în contextul asigurării securității informaționale

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) Elaborarea, sub egida Consiliului coordonator pentru asigurarea securității informaționale, a criteriilor de calificare a informației ca produs de dezinformare, manipulare şi propagandă, orientate spre subminarea securității

informaționale, în scopul identificării: comanditarilor, surselor de finanțare și a executorilor;

2) ajustarea cadrului legal în vederea eficientizării colectării de date pentru identificarea proveniență mijloacelor financiare și proprietății ale subiecților implicați în activități de dezinformare, manipulare și propagandă ce subminează securitatea informațională;

3) interacțiunea cu instituțiile de drept în ceea ce privește analiza riscurilor și amenințărilor din domeniul mass-mediei, cu scopul de a monitoriza evoluția amenințărilor depistate, de a investiga activitatea subversivă sau penală în spațiul informațional și de a stabili sursele de finanțare a factorilor de risc.

Prioritățile Pilonului II	Indicatori de rezultat
1. Dezvoltarea instrumentelor controlului civic în scopul asigurării securității informaționale	1. Mecanism de interacțiune și implicare a experților în scopul asigurării securității spațiului informațional
2. Elaborarea cadrului legal pentru determinarea statutului juridic al publicațiilor periodice, agențiilor de presă și altor subiecți care activează în spațiului media din Internet	2. Lege pentru modificarea/ completarea cadrului juridic existent
3. Crearea resursei/platformei informaționale de comunicare strategică	3. Resursă de comunicare și informare strategică creată

4.3 Pilonul III. Consolidarea capacităților operaționale

93. Obiectivul nr. 1. Dezvoltarea mecanismelor de prevenire, de depistare, de atenuare și de răspuns la nivel național pentru asigurarea securității informaționale

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) crearea, la nivel național, a entității ce va avea competențe de promovare și coordonare a politicilor de securitate informațională într-o societate democratică, în funcție de dezvoltarea tehnologiei, raporturile juridice și de altă natură din sectorul societății informaționale la nivel național și internațional (Consiliul coordonator pentru asigurarea securității informaționale):

a) identificarea și integrarea componentelor existente cu funcții și atribuții din domeniul cibernetic, mediatic și a autorităților administrației publice și a celor care vor fi create pe parcurs;

b) determinarea liniei de activitate pentru fiecare componentă inclusă în cadrul entității, în funcție de funcțiile și atribuțiile deținute din perspectiva asigurării securității informaționale;

c) elaborarea și adoptarea cadrului normativ de interacțiune pentru realizarea sarcinilor de depistare, prevenire și contracarare a riscurilor și amenințărilor la adresa securității informaționale.

2) elaborarea, promovarea și coordonarea politicilor de securitate informațională conform Concepției, prezentei Strategii și a altor documente de politici de nivel național și internațional ce se referă la societatea informațională;

3) informarea publicului privind modalităţile de prevenire şi contracarare a riscurilor şi ameninţărilor la adresa componentelor sistemice a securităţii informaţionale, inclusiv privind fenomenele nou-apărute la nivel naţional.

94. Obiectivul nr. 2. Dezvoltarea capacităţilor de reacţie în cazul unor ameninţări hibride de securitate

Obiectivul dat urmează a fi realizat prin următoarele acţiuni:

1) crearea unei componente analitico-informaţionale specializată pe ameninţările hibride de securitate în cadrul Serviciului de Informaţii şi Securitate;

2) crearea reţelei naţionale a autorităţilor responsabile de combaterea ameninţărilor hibride de securitate;

3) elaborarea unor protocoale operaţionale de interacţiune între autorităţile responsabile şi factorii de decizie în cazul unor ameninţări hibride de securitate;

4) consolidarea gradului de cunoaştere şi înţelegere a concepţiei ameninţărilor hibride de securitate la nivelul organelor abilitate de asigurarea securităţii informaţionale şi a mediului general de securitate;

5) efectuarea exerciţiilor pentru dezvoltarea capacităţilor autorităţilor specializate în combaterea ameninţărilor hibride de securitate;

6) asocierea Republicii Moldova la Centrul European de Excelenţă pentru combaterea ameninţărilor hibride şi Centrul de Excelenţă privind comunicarea strategică a NATO.

95. Obiectivul nr. 3. Dezvoltarea competenţelor operaţionale de apărare cibernetică

Obiectivul dat urmează a fi realizat prin următoarele acţiuni:

1) crearea entităţii responsabile de apărarea cibernetică la nivelul Forţelor Armate;

2) consolidarea capacităţilor de educaţie cibernetică şi formare prin participarea la exerciţii interstatale şi internaţionale de apărare cibernetică;

3) identificarea, prevenirea şi contracararea factorilor de risc cu potenţial informativ-subversiv în adresa apărării cibernetice a Republicii Moldova prin implementarea unui management integrat al spaţiului virtual şi dezvoltarea unui sistem de avertizare timpurie cu privire la elementele de risc la adresa obiectivelor de infrastructură.

96. Obiectivul nr. 4. Monitorizarea spaţiului informaţional şi de depistare a acţiunilor de dezinformare şi/sau de informare manipulatorie din exteriorul şi interiorul ţării

Obiectivul dat urmează a fi realizat prin următoarele acţiuni:

1) revizuirea cadrului legal existent în direcţia definirii şi uniformizării noţiunilor cu privire la dezinformare, ştirile false şi/sau informare manipulatoare, precum şi prevenirea răspîndirii acestora prin platformele media. Determinarea sectoarelor securităţii naţionale a căror afectare (de către dezinformare) creează

riscuri majore pentru funcționalitatea statului;

2) stabilirea atribuțiilor (organelor competente) pentru depistarea și contracararea mesajelor manipulatorii și de dezinformare din spațiul informațional (Internet);

3) stabilirea unor filtre de depistare și sau/blocare a diverselor produse informaționale și/sau resurse informaționale, care conțin elemente de risc în adresa securității naționale, precum și elaborarea, adoptarea cadrului normativ aferent.

97. Obiectivul nr. 5. Sporirea capacităților de protecție a infrastructurilor critice naționale

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) elaborarea și aprobarea cadrului legal privind identificarea și desemnarea infrastructurilor critice naționale, inclusiv ce țin de sistemele informaționale de importanță vitală;

2) evaluarea și raportarea privind starea și nivelul de securitate a obiectivelor de infrastructură critică din perspectiva asigurării securității informaționale.

98. Obiectivul nr. 6. Dezvoltarea capacităților de prevenire, de depistare și de contracarare a acțiunilor extremiste, teroriste și de altă natură care periclitează securitatea informațională

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) sincronizarea și repartizarea rațională a forțelor instituțiilor Republicii Moldova spre depistarea preventivă a acțiunilor derulate din exteriorul și/sau interiorul țării, concepute ca diversiuni complexe la adresa securității informaționale;

2) raportarea către Serviciul de Informații și Securitate a informațiilor despre starea de risc de la instituțiile statului cu competență în domeniu;

Prioritățile Pilonului III	Indicatorii de rezultat
1. Crearea, la nivel național, a Consiliului coordonator pentru asigurarea securității informaționale, în cadrul căruia se vor identifica proceduri de comunicare strategică	1. Cadru normativ privind crearea Consiliului coordonator pentru asigurarea securității informaționale elaborat și aprobat
2. Crearea entității responsabile de apărarea cibernetică la nivelul Forțelor Armate	2. Cadru normativ privind crearea entității la nivel național responsabilă de apărarea cibernetică la nivelul Forțelor Armate elaborat și aprobat
3. Crearea platformei specializate pe amenințările hibride de securitate	3. Platformă creată și funcțională
4. Elaborarea și promovarea cadrului legal de reglementare a infrastructurii critice naționale	4. Cadru legal elaborat și aprobat

4.4. Pilonul IV. Eficientizarea procesului de coordonare internă și cooperare internațională în domeniul securității informaționale

99. Obiectivul nr. 1. Dezvoltarea sistemului de pregătire a resurselor umane în domeniul securităţii informaţionale

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) evaluarea nivelului actual de pregătire a resurselor umane în domeniul securităţii informaţionale, pe fiecare compartiment în parte: mass-media, tehnologia informaţională, apărare, ordine publică şi contrainformaţii;

2) identificarea categoriilor de beneficiari care urmează, cu prioritate, să fie incluşi în programe noi de instruire a resurselor umane în domeniul vizat;

3) elaborarea unor programe noi de pregătire a resurselor umane în domeniul vizat;

4) dezvoltarea şi implementarea unor programe de instruire dedicate angajaților cu atribuții de investigare și urmărire penală, procurorilor, judecătorilor, specialiştilor şi experţilor judiciari în domeniu, din cadrul structurilor de aplicare a legii, precum și celor dedicate personalului tehnic din cadrul instituțiilor publice.

100. Obiectivul nr. 2. Coordonarea activităţii autorităţilor administraţiei publice, a instituţiilor publice şi private în partea ce ţine de exercitarea atribuţiilor privind asigurarea securităţii informaţionale

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) identificarea cadrului normativ relevant ce reglementează atribuţiile autorităţilor administraţiei publice, a instituţiilor publice şi private privind asigurarea securităţii informaţionale şi ajustarea acestuia, excluzînd lacunele şi dublările de competenţă;

2) reglementarea expresă în legislaţie a atribuţiei de coordonare a activităţii autorităţilor administraţiei publice, a instituţiilor publice şi private în partea ce ţine de exercitarea atribuţiilor privind asigurarea securităţii informaţionale, precum şi a mecanismului de realizare a acesteia, de către autoritatea publică desemnată;

3) elaborarea şi încheierea unor acorduri de cooperare interinstituţionale multilaterale care vor specifica modul de coordonare a activităţii în partea ce ţine de exercitarea atribuţiilor privind asigurarea securităţii informaţionale.

101. Obiectivul nr. 3. Asigurarea cooperării internaţionale în domeniul securităţii informaţionale

Obiectivul dat urmează a fi realizat prin următoarele acțiuni:

1) evaluarea nivelului actual al cooperării Republicii Moldova cu organizaţiile internaţionale ce îşi desfăşoară activitatea în domeniul asigurării securităţii informaţionale şi elaborarea acţiunilor pentru intensificarea cooperării respective;

2) stabilirea cooperării cu statele partenere, în special din cadrul Uniunii Europene, privind schimbul de informaţii, experienţe şi analize în scopul prevenirii, depistării şi contracarării ameninţărilor hibride de securitate în spaţiul informaţional;

3) promovarea, pe plan internaţional, inclusiv în cadrul bilateral, a necesităţii încheierii unor acorduri ce ar unifica conceptul de „armă informaţională", interzicînd elaborarea, răspîndirea şi aplicarea acesteia în relaţiile între state;

4) alinierea şi implementarea instrumentelor internaţionale existente ce ar asigura prevenirea, depistarea şi contracararea accesului neautorizat la informaţiile cu accesibilitate limitată din reţelele de comunicaţii electronice bancare şi din sistemele de comerţ electronic, la informaţiile organelor internaţionale de drept;

102. Obiectivul nr. 4. Dezvoltarea cooperării naţionale şi internaţionale în domeniul apărării cibernetice

Obiectivul dat urmează a fi realizat prin următoarele acţiuni:

1) crearea/implementarea cadrului de cooperare interinstituţional în domeniul apărării cibernetice.

2) intensificarea cooperării cu partenerii externi de dezvoltare, privind schimbul de informaţii şi experienţă în domeniul apărării cibernetice.

3) semnarea acordurilor de colaborare (asistenţă mutuală) în domeniul apărării cibernetice.

103. Obiectivul nr. 5. Consolidarea cooperării internaţionale în domeniul combaterii criminalităţii informatice

Obiectivul dat urmează a fi realizat prin următoarele acţiuni:

1) consolidarea mecanismelor de cooperare internaţională între autorităţile statului cu atribuţii în combaterea criminalităţii informatice şi organismelor internaţionale specializate EMAS (Europol Malware Analysis Service) al EUROPOL;

2) utilizarea, la nivel naţional, a instrumentelor şi metodelor de identificare a victimelor, inclusiv prin utilizarea Sistemului informaţional automatizat „Protecţia Copiilor" şi a bazei de date „ICSE" a OIPC INTERPOL;

3) cooperarea în cadrul punctelor naţionale de contact 24/7 în baza Convenţiei Consiliului Europei privind criminalitatea informatică (Budapesta 2001) şi 24/7 G7;

4) dezvoltarea parteneriatelor existente NCMEC (Centrul Naţional al SUA privind copiii dispăruţi şi exploataţi) şi aderarea la alte iniţiative similare;

5) dezvoltarea parteneriatelor în scopul identificării, blocării, sechestrării şi confiscării produselor şi a instrumentelor provenite din infracţiunile transfrontaliere;

6) participarea la evenimente internaţionale în domeniul prevenirii şi combaterii criminalităţii informatice în scopul formării personalului de specialitate.

Priorităţile Pilonului IV	Indicatori de rezultat
1. Dezvoltarea şi implementarea programelor de instruire dedicate angajaţilor cu atribuţii de	1. Specialişti instruiţi în baza practicilor UE

investigare şi urmărire penală pe spaţiul informaţional	
2. Dezvoltarea cooperării naţionale şi internaţionale în domeniul apărării cibernetice	2. Cadru legal de cooperare negociat şi încheiat
3. Stabilirea mecanismelor de cooperare internaţională între autorităţile statului cu atribuţii în combaterea criminalităţii informatice şi organismele internaţionale pe segmentul asigurării securităţii informaţionale	3. Runde de consultări; acorduri bilaterale/multilaterale semnate şi încheiate

V. ESTIMAREA IMPACTULUI ŞI A COSTURILOR IMPLEMENTĂRII STRATEGIEI

104. Implementarea calitativă a prevederilor prezentei Strategii va spori gradul de protecţie şi securitate în spaţiul informaţional.

105. Impactul realizării se va manifesta în:

1) asigurarea drepturilor şi libertăţilor constituţionale ale cetăţenilor la prelucrarea informaţiilor;

2) protejarea şi promovarea exercitării democraţiei participative şi pluraliste;

3) dezvoltarea societăţii informaţionale naţionale, pe toate formele de structură şi funcţionare, de natură individuală, publică, privată sau de stat;

4) asigurarea prevenirii şi investigării eficiente a crimelor informatice;

5) protecţia împotriva influenţelor informaţionale şi psihologice distructive;

6) protecţia societăţii împotriva dezinformărilor distructive cu scopul incitării la ură naţională şi religioasă, schimbarea orînduirii constituţionale;

7) dezvoltarea mecanismelor de combatere colectivă a ameninţărilor hibride de securitate ce periclitează securitatea informaţională şi mediul general de securitate;

8) asigurarea protecţiei întreprinderilor, instituţiilor şi organizaţiilor în accesul la informaţii corecte şi obiective;

9) asigurarea liberei circulaţii a informaţiilor, pluralismului multi-media şi a platformelor de informare on-line şi off-line, cu excepţia cazurilor prevăzute de lege;

10) dezvoltarea şi protejarea infrastructurii naţionale de informare;

11) consolidarea principiilor de informare a diasporei despre situaţia din Republicii Moldova;

12) funcţionarea şi dezvoltarea în condiţii de siguranţă a spaţiului informaţional naţional şi integrarea sa în spaţiul informaţional european şi mondial;

13) dezvoltarea sistemului de comunicaţii strategice din Republica Moldova;

14) interacţiunea eficientă a autorităţilor publice şi a societăţii civile în procesul de formare şi implementare a politicii de stat în sfera informaţiilor;

15) asigurarea dezvoltării tehnologiilor informației și comunicațiilor și a resurselor informaționale din Republica Moldova;

16) protecția informației cu accesibilitate limitată și a altor informații ale căror cerințe de protecție sînt stabilite prin lege;

17) responsabilizarea operatorilor de date cu caracter personal față de modul în care prelucrează datele cu caracter personal.

18) protecția datelor cu caracter personal precum și a persoanelor, în special a copiilor, în mediul online.

19) determinarea statutului juridic al subiecților spațiului media on-line (informațional din Internet).

106. În scopul realizării rezultatelor trasate supra, este necesar în prim plan consolidarea responsabilităților autorităților administrațiilor publice, instituțiilor, întreprinderilor de stat indiferent de forma de organizare și acționare a acestora într-o direcție unică.

107. Prezenta Strategie presupune alocarea mijloacelor financiare pentru întreaga perioadă de implementare.

108. Finanțarea prezentei Strategii se va realiza din bugetul de stat (resurse generale, venituri colectate și resurse ale proiectelor finanțate din surse externe) și din alte surse conform legislației.

109. Oportunitățile de sprijinire și stimulare a activităților din domeniul tehnologiilor informaționale, oferite de către organizațiile internaționale și regionale vor fi valorificate.

110. Caracterul prezentei Strategii generează riscuri de divulgare a unor date clasificate prin prisma estimării alocațiilor financiare pentru realizarea anumitor obiective şi activităţi-cheie din Planul de acţiuni pentru implementarea prezentei Strategii, fapt ce impune definitivarea, în mod individual, a sumelor necesare la nivelul autorităţilor şi includerea separată pentru fiecare an bugetar.

111. În scopul asigurării protecţiei datelor din perspectiva elaborării de acte normative, politici şi planificării de acţiuni, inclusiv şi a alocaţiilor financiare, autorităţile/instituţiile vor evalua şi vor decide în mod individual reflectarea datelor, care pot fi calificate ca informaţii atribuite la secret de stat.

VI. REZULTATELE SCONTATE ŞI INDICATORII DE PROGRES

112. Implementarea prezentei Strategii va duce la identificarea abordărilor inovatoare ale formării unui sistem de protecție și dezvoltare a spațiului informațional în condițiile globalizării și liberei circulații a informațiilor, și anume:

1) vor fi elaborate soluţii tehnice speciale de sporire a fiabilităţii reţelelor comunicaţionale în cazuri critice;

2) vor fi create arhive şi stocuri de documente electronice în vederea depozitării securizate a bazelor de date de importanţă naţională, în conformitate cu regimul de stocare, păstrare şi de evidenţă stabilit de legislaţie;

3) vor fi consolidate mecanisme de protecţie a datelor cu caracter personal în vederea eliminării utilizării acestora în scopuri ilegale;

4) vor fi dezvoltate capacităţile naţionale necesare pentru efectuarea unui schimb securizat şi pentru stocarea informaţiilor, transmiterea promptă şi eficientă a fluxului de informaţii, inclusiv a celor clasificate, pe plan intern şi extern, în caz de diverse crize ori situaţii excepţionale;

5) va fi creat mecanismul pentru îmbunătăţirea implicării societăţii civile în domenii prioritare de asigurare a securităţii informaţionale;

6) vor fi instituite mecanisme eficiente de monitorizare, de control şi de implementare în vederea diminuării discrepanţelor şi a provocărilor existente, protejării societăţii de eventuale tentative de dezinformare şi/sau de informare manipulatoare din exterior;

7) vor fi stabilite garanţii specifice pentru a proteja cît mai eficient datele cu caracter personal, viaţa intimă, familială şi privată a persoanelor, în special în mediul on-line;

8) vor fi asigurate măsuri de prevenire şi combatere a criminalităţii informatice.

113. Prezenta Strategie are ca element central crearea Consiliului coordonator pentru asigurarea securităţii informaţionale, organism colectiv, cu atribuţii consultative şi operaţionale, ce va fi responsabil şi va asigura integrarea sistemică a componentelor spaţiului informaţional şi susţinerea orientată a unui nivel înalt de securitate informaţională.

1) Consiliul coordonator pentru asigurarea securităţii informaţionale, în condiţiile prezentei Strategii, se propune a fi constituit din 4 paliere de bază, după cum urmează:

a) *Palierul cibernetic* va include reprezentanţi ai Centrului naţional de reacţie la incidentele de securitate cibernetică, Centrului guvernamental de reacţie la incidentele de securitate cibernetică şi Centrului privat de reacţie la incidentele de securitate cibernetică, precum şi din experţi ai unităţilor de securitate cibernetică a altor instituţii de drept public şi drept privat, ce activează în sectorul tehnologiilor informaţionale şi pot contribui la asigurarea securităţii informaţionale a Republicii Moldova;

b) *Palierul mediatic* va fi constituit din reprezentanţi ai spaţiului mediatic naţional, în special din reprezentanţi ai mass-mediei tradiţionale (posturi radio, posturi TV şi presa scrisă), precum şi media din Internet, inclusă în funcţie de caracterul politicilor editoriale, ce vor fi preocupaţi de procese ce ţin de asigurarea securităţii spaţiului mediatic;

c) *Palierul operaţional* va fi format în special din reprezentanţi ai autorităţilor publice cu atribuţii şi competenţe în materie de apărare, informativă,

contrainformativă, investigativă şi procesuală, conform prerogativelor de asigurare a securităţii spaţiului informaţional;

d) *Palierul civic-privat* va fi instituit din reprezentanţi ai societăţii civile conform recomandărilor Consiliu al societăţii civile, asociaţiilor ce reprezintă sectorul IT naţional, companiilor de drept privat din domeniul IT, precum şi experţi internaţionali din rîndul partenerilor strategici de moment şi perspectivă ai Republicii Moldova, specializaţi în materie de consolidare a dimensiunii de securitate cibernetică şi informaţională, la nivel regional, european şi internaţional.

2) Consiliul coordonator pentru asigurarea securității informaționale va funcționa în baza unui statut ce va fi elaborat ca urmare a adoptării prezentei Strategii, avînd ca bază structurală componentele menţionate mai sus, fiind posibile şi modificări de îmbunătăţire.

3) Modul de desemnare a organele de conducere la nivelul Consiliului coordonator pentru asigurarea securității informaționale va fi prevăzut în statut şi va fi bazat pe principiul rotației succesive.

4) Palierele specificate vor activa în mai multe moduri: separat, mixt prin atragerea experţilor din alte paliere, sau integrat la nivelul întregului Consiliu coordonator pentru asigurarea securității informaționale, fiind desemnat un organ de conducere din rîndul componentelor cu atribuţii şi competenţe prioritare reieşind din problematica examinată.

5) Consiliul coordonator pentru asigurarea securității informaționale va avea ca prioritate de activitate examinarea incidentelor de securitate informaţională, a căror soluţionare necesită o abordare integrată, accentul fiind plasat pe operativitate în examinarea cazurilor, determinarea acţiunilor de reacţie timpurie, prevenirea, contracararea sau eliminarea consecinţelor.

6) Serviciul de Informaţii şi Securitate al Republicii Moldova va avea calitatea de coordonator al activităţii Consiliului coordonator pentru asigurarea securității informaționale, fiind responsabil de recepţionarea sesizărilor de incidente de securitate informaţională şi prezentarea către conducătorii palierelor.

VII. PROCEDURI DE MONITORIZARE ŞI EVALUARE

114. Monitorizarea prezentei Strategii are drept scop:

1) urmărirea modului de implementare a prezentei Strategii, a gradului de realizare a obiectivelor şi acțiunilor propuse, precum şi necesitatea modificării acesteia în funcție de evoluția anumitor factori de ordin intern sau extern;

2) asigurarea transparenței şi diseminarea informațiilor cu privire la acțiunile realizate şi rezultatele obținute.

115. Procesul de implementare a prezentei Strategii va fi însoţit de monitorizarea permanentă a realizării acţiunilor propuse şi a rezultatelor obţinute, cu operarea, în caz de necesitate, a modificărilor de rigoare în politicile publice promovate de către Guvern în contextul prezentei Strategii.

116. Monitorizarea şi coordonarea procesului de realizare a prezentei Strategii şi Planului de acţiuni privind implementarea acesteia se pune în sarcina Serviciului de Informaţii şi Securitate al Republicii Moldova.

117. Ministerele, instituţiile şi alte autorităţi administrative centrale, conform competenţelor atribuite, vor asigura întreprinderea măsurilor necesare în vederea realizării integrale şi în termenele stabilite a acţiunilor incluse în Planul de acţiuni privind implementarea prezentei Strategii.

Anexa nr. 2

PLAN DE ACŢIUNI
pentru implementarea Strategiei Securităţii informaţionale a Republicii Moldova pentru anii 2019-2024

Nr. crt.	Obiectivele	Denumirea acţiunilor	Instituţiile responsabile	Parteneri	Surse de finanţare/costul	Termen de realizare	Indicatorii de progres
1	2	3	4	5	6	7	8
PILONUL I. Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice							
1.	Crearea unui sistem integrat de comunicare şi evaluare a ameninţărilor la adresa securităţii informaţionale şi de elaborare a măsurilor operative de răspuns	1) crearea/desemnarea entităţii care va exercita rolul de Centru naţional de reacţie la incidentele de securitate cibernetică şi care va constitui punctul unic de raportare a incidentelor de securitate cibernetică pentru autorităţile publice competente şi persoanele fizice şi juridice: a) elaborarea şi promovarea cadrului normativ; b) crearea Centrului naţional de reacţie la incidentele de securitate cibernetică	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Cancelaria de Stat; Ministerul Finanţelor; Ministerul Economiei şi Infrastructurii	Serviciul de Informaţii şi Securitate; Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei a Republicii Moldova; Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal; Agenţia de Guvernare Electronică Agenţia de Stat Pentru Proprietatea Intelectuală; furnizorii serviciilor de comunicaţii	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2019-2021	Cadrul normativ elaborat şi aprobat; Centru naţional de reacţie la incidentele de securitate cibernetică creat
		2) desemnarea entităţii care va exercita rolul de Centru	Serviciul Tehnologia	Centrul Naţional pentru Protecţia	Bugetul instituţiilor, în limitele alocaţiilor	2019-2020	Cadrul normativ aprobat (act de desemnare)

1	2	3	4	5	6	7	8
		guvernamental de reacție la incidentele de securitate cibernetică și care va constitui punctul de raportare al incidentelor de securitate cibernetică al Guvernului, precum și stabilirea interacțiunii acestuia cu Centrul național de reacție la incidentele de securitate cibernetică	Informației și Securitate Cibernetică; Cancelaria de Stat	Datelor cu Caracter Personal; Ministerul Economiei și Infrastructurii; Serviciul de Informații și Securitate; Ministerul Afacerilor Interne; Procuratura Generală	aprobate; asistență externă		
		3) stabilirea de către Centrul național de reacție la incidente de securitate cibernetică a indicatorilor din domeniul securității cibernetice: a) sistematizarea, analiza și evaluarea datelor statistice la capitolul securității cibernetice	Serviciul Tehnologia Informației și Securitate Cibernetică	Serviciul de Informații și Securitate; Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală; Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2023	Acte normative elaborate și aprobate; produs de analiză privind starea în domeniul securității cibernetice naționale
		4) elaborarea mecanismelor de creare și consolidare a centrelor departamentale de reacție la incidentele de securitate cibernetică și informațională atît de drept public, cît și de drept privat	Serviciul Tehnologia Informației și Securitate Cibernetică	Serviciul de Informații și Securitate; Ministerul Apărării; Ministerul Afacerilor Interne; Procuratura Generală; Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2023	Mecanisme identificate și aprobate
		5) elaborarea cadrului normativ pentru asigurarea unui nivel înalt de securitate a	Ministerul Economiei și Infrastructurii	Serviciul Tehnologia Informației și	Bugetul instituțiilor, în limitele alocațiilor aprobate;	2021-2024	Cadru normativ aprobat

1	2	3	4	5	6	7	8
		rețelelor și a sistemelor informatice la nivel național, în baza bunelor practici UE		Securitate Cibernetică	asistenţă externă		
		6) determinarea politicii privind modalitatea de raportare, stocare și prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	Serviciul de Informaţii şi Securitate; Procuratura Generală	Bugetul instituţiilor, în limitele alocaţiilor aprobate; Asistenţa externă	2021-2022	Cadru normativ aprobat
2.	Monitorizarea permanentă și asigurarea nivelului înalt de securitate cibernetică	1) identificarea și eliminarea surselor de amenințare la adresa securității persoanei, societății şi statului în spaţiul cibernetic a) efectuarea auditului de securitate cibernetică a infrastructurilor de tehnologie a informației și a Sistemului de telecomunicații al AAP, precum și a altor infrastructuri cibernetice de interes național, în vederea identificării disfuncțiilor și vulnerabilităților și furnizarea soluțiilor/recomandărilor de remediere a acestora; b) implementarea rezultatelor auditului de securitate cibernetică;	Agenția de Guvernare Electronică; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	Serviciul de Informaţii şi Securitate; Agenția Servicii Publice; Ministerul Economiei şi Infrastructurii; Ministerul Afacerilor Interne; Procuratura Generală	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Raport de audit a stării securității cibernetice elaborat; raport privind implementarea propunerilor auditului efectuat
		2) asigurarea aplicării Cerințelor minime de securitate cibernetică de nivelul II în cadrul prestării serviciilor electronice publice	Agenția de Guvernare Electronică	Autoritățile administrației publice	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Raport privind modul de aplicare a Cerinţelor minime de securitate
		3) elaborarea mecanismelor și metodelor de prevenire și contracarare a pericolelor în	Serviciul de Informaţii şi Securitate	Ministerul Economiei și Infrastructurii;	Bugetul instituţiilor, în limitele alocaţiilor aprobate;	2020-2021	Mecanisme elaborate

1	2	3	4	5	6	7	8
		spațiul cibernetic, generate de serviciile informaţionale prestate de către persoanele fizice şi juridice		Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Ministerul Afacerilor Interne; Centrul Național pentru Protecția Datelor cu Caracter Personal	asistenţă externă		
		4) identificare unui mecanism legal de interacțiune între autoritățile publice competente şi persoanele fizice şi juridice, indiferent de tipul de proprietate, în vederea acordării de către acestea a accesului la codul sursă al aplicațiilor elaborate, comercializate şi distribuite pentru autoritățile publice	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Ministerul Economiei şi Infrastructurii	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2022	Cadru normativ elaborat și aprobat
		5) coordonarea cu Centrul Național pentru Protecția Datelor cu Caracter Personal a măsurilor de protecție a datelor cu caracter personal care să asigure aplicarea principiului protecției datelor începînd de la conceperea și protecția implicită a datelor atunci cînd se elaborează, se proiectează, se selectează și se utilizează aplicații, servicii și produse care se bazează pe prelucrarea datelor cu caracter personal sau care prelucrează date cu caracter personal în	Autoritățile administrației publice	Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	Cadru normativ modificat și completat

1	2	3	4	5	6	7	8
		corespundere cu legislația privind protecția datelor cu caracter personal					
3.	Consolidarea capacităților de apărare cibernetică	1)delimitarea şi atribuirea rolurilor şi responsabilităţilor privind apărarea cibernetică, a sistemului organelor securității statului și sistemului național de apărare	Ministerul Apărării; Serviciul de Informaţii şi Securitate	Ministerul Afacerilor Interne; Procuratura Generală	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	Cadru normativ modificat și completat
		2)elaborarea măsurilor de apărare cibernetică pentru protecţia infrastructurii critice naționale, precum și din cadrul altor sectoare prioritare pentru stat;	Serviciul de Informaţii şi Securitate; Ministerul Apărării	Ministerul Afacerilor Interne; Procuratura Generală; Ministerul Economiei şi Infrastructurii; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2023	Măsuri de apărare cibernetică pentru protecţia infrastructurii critice naționale elaborate și aprobate
		3)elaborarea și implementarea măsurilor de protecție a sistemelor informaționale ce prelucrează informații atribuite la secret de stat și componentei TIC a sistemelor de apărare națională	Serviciul de Informaţii şi Securitate	Ministerul Apărării; Ministerul Afacerilor Interne; Procuratura Generală; Ministerul Economiei și Infrastructurii; Serviciul Tehnologia Informației și Securitate Cibernetică; Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2022	Măsuri de protecție a sistemelor informaționale ce prelucrează informații atribuite la secret de stat elaborate și aprobate
4.	Protecţia reţelelor	1) dezvoltarea mecanismelor	Serviciul de	Serviciul	Bugetul instituţiilor,	Permanent	Mecanisme

1	2	3	4	5	6	7	8
	de comunicaţii speciale ale Republicii Moldova şi a informaţiei cu accesibilitate limitată, pentru menţinerea funcţiilor vitale ale statului	de protecție a sistemelor speciale de comunicații electronice prin aplicarea mijloacelor de protecție criptografică și tehnică a informațiilor;	Informaţii şi Securitate	Tehnologia Informaţiei şi Securitate Cibernetică	în limitele alocaţiilor aprobate; asistenţă externă		implementate
		2) efectuarea controalelor asupra sistemelor speciale de comunicații electronice și raportarea autorității responsabile asupra măsurilor tehnice și tehnico-organizatorice întreprinse pentru asigurarea securității cibernetice	Serviciul de Informaţii şi Securitate	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Număr de controale efectuate
		3)actualizarea cadrului normativ în domeniul sistemelor speciale de comunicații electronice	Serviciul de Informaţii şi Securitate	Ministerul Afacerilor Interne (Serviciul Tehnologia Informației)	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2023	Cadrul normativ modificat și completat
		4) elaborarea sistemului de atestare a obiectelor de informatizare privind îndeplinirea cerințelor de asigurare a protecției informației în timpul efectuării lucrărilor ce țin de prelucrarea și păstrarea informației cu accesibilitate limitată, în special a celei atribuite la secret de stat	Serviciul de Informaţii şi Securitate		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2024	Sistem de atestare elaborat și implementat
		5) stabilirea măsurilor de asigurare a securității datelor cu caracter personal în contextul asigurării securității cibernetice	Centrul Național pentru Protecția Datelor cu Caracter Personal	Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate; Procuratura Generală; Serviciul	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	Cadrul normativ modificat și completat

1	2	3	4	5	6	7	8
				Tehnologia Informaţiei şi Securitate Cibernetică			
		6) promovarea cadrului normativ privind instituirea subdiviziunilor responsabile de protecția datelor cu caracter personal în cadrul autorităților de drept public și privat	Centrul Național pentru Protecția Datelor cu Caracter Personal	Autorităţile administraţiei publice	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020	Cadrul normativ promovat
5.	Asigurarea controlului asupra importului, certificării şi utilizării mijloacelor de protecţie a informaţiei	1) certificarea mijloacelor de protecţie tehnică şi criptografică a informaţiei	Serviciul de Informaţii şi Securitate	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	Bugetul instituţiilor, în limitele alocaţiilor aprobate;	Permanent	Număr de mijloace certificate
		2) dezvoltarea sistemelor de monitorizare a importului mijloacelor de protecție a informație	Serviciul Vamal; Serviciul de Informaţii şi Securitate	Ministerul Economiei și Infrastructurii	În limita bugetului instituțiilor.	2020-2023	Sistem elaborat și implementat
		3) alinierea cadrului legislativ în domeniul protecției criptografice a informației la cadrul normativ european	Serviciul de Informaţii şi Securitate	Ministerul Justiţiei; Ministerul Afacerilor Externe și Integrării Europene; Ministerul Economiei și Infrastructurii	În limitele bugetului instituțiilor	2021	Cadru normativ modificat și completat
		4) crearea unei baze de date privind mijloacele de protecție tehnică și criptografică a informației	Serviciul de Informaţii şi Securitate	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Agenția de Guvernare Electronică; Ministerul	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2022	Bază de date creată și completată

1	2	3	4	5	6	7	8
				Economiei și Infrastructurii			
		5) exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice	Serviciul de Informaţii şi Securitate		Bugetul instituţiilor, în limitele alocaţiilor aprobate	Permanent	Registru completat
6.	Combaterea criminalității informatice (investigarea infracțiunilor informatice)	1) eficientizarea capacităților (mecanismului) de combatere a criminalității informatice	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală		Bugetul instituţiilor, în limitele alocaţiilor aprobate	Permanent	Număr de personal instruit
		2) acordarea ajutorului metodico-practic subdiviziunilor teritoriale privind investigarea infracțiunilor informatice	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală		Bugetul instituţiilor, în limitele alocaţiilor aprobate	Permanent	Număr de personal din subdiviziunile teritoriale instruit
		3) implementarea noilor mecanisme la nivelul instituțiilor implicate în combaterea criminalității informatice (atragerea companiilor private și experților independenți, dezvoltarea laboratoarelor)	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Serviciul de Informaţii şi Securitate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	Mecanisme funcțional implementate
		4) perfecționarea cadrului legal ce reglementează salarizarea efectivului specializat în combaterea criminalității informatice și investigarea infracțiunilor informatice	Ministerul Finanţelor; Ministerul Afacerilor Interne	Ministerul Sănătății, Muncii și Protecției Sociale	Bugetul instituţiilor, în limitele alocaţiilor aprobate	2020	Cadru legal cu privire la majorarea cu 30% în raport cu salariul net aprobat
7.	Protecția copiilor în spațiul on-line de orice formă de abuz	1) combaterea fenomenului de pornografie infantilă în Internet	Ministerul Afacerilor Interne (Inspectoratul General al Poliției);	Ministerul Sănătății, Muncii și Protecției Sociale; Ministerul	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Număr de măsuri realizate/cazuri investigate

1	2	3	4	5	6	7	8
			Procuratura Generală	Educaţiei, Culturii şi Cercetării; organizaţiile nonguvernamentale; societatea civilă; mass-media			
		2) combaterea fenomenelor de grooming şi hărţuire sexuală a copiilor în Internet	Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală	Ministerul Educaţiei, Culturii şi Cercetării; organizaţiile nonguvernamentale; societatea civilă; Ministerul Sănătăţii, Muncii şi Protecţiei Sociale; furnizori de servicii	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Număr de măsuri realizate/cazuri investigate
		3) promovarea unui Internet mai sigur pentru copii prin intermediul consilierilor on-line şi încurajarea raportărilor prin proiecte informaţionale specializate	Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală	Ministerul Educaţiei, Culturii şi Cercetării; organizaţiile nonguvernamentale; societatea civilă; Ministerul Sănătăţii, Muncii şi Protecţiei Sociale;	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Număr de campanii de informare
8.	Combaterea fraudelor prin utilizarea mijloacelor de plată electronice	1) schimbul de informaţii dintre Centrul pentru combatere a crimelor informatice cu departamentele de securitate ale instituţiilor financiare	Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală	Banca Naţională a Moldovei; instituţiile financiare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Acord privind schimbul de informaţii
		2) promovarea măsurilor de securitate sporită în privinţa ATM-lor la nivel de hardware şi software.	Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura	Banca Naţională a Moldovei; instituţiile financiare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Număr de măsuri de securitate implementate.

1	2	3	4	5	6	7	8
			Generală				
		3) identificarea mecanismelor comune de combatere a fraudelor card-present şi card not-present	Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală	Banca Naţională a Moldovei; instituţiile financiare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	Mecanism identificat şi implementat
9.	Dezvoltarea capacităţilor instituţionale în combaterea criminalităţii informatice	1) dezvoltarea subdiviziunilor specializate în cadrul Inspectoratului General al Poliţiei al Ministerului Afacerilor Interne, Procuraturii Generale, Serviciului de Informaţii şi Securitate în scopul depistării şi contracarării a tentativelor infracţionale în domeniu;	Ministerul Afacerilor Interne (Inspectoratul General al Poliţiei); Procuratura Generală; Serviciul de Informaţii şi Securitate		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Număr de subdiviziuni create/specializate
		2) crearea unei baze de date naţionale privind evoluţia fenomenului criminalităţii informatice	Procuratura Generală; Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne	Centrul Naţional Anticorupţie; Serviciul Vamal; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2022	Bază de date creată
		3) ajustarea activităţii desfăşurate în domeniul criminalităţii informatice, în banca centrală de date a Sistemului informaţional automatizat „Registru informaţii criminalistice şi criminologice”	Ministerul Afacerilor Interne (Serviciul Tehnologia Informaţiei)	Procuratura Generală; Serviciul de Informaţii şi Securitate; Serviciul Vamal; Centrul Naţional Anticorupţie; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Mecanisme ajustate/ implementate/
		4) elaborarea cadrului normativ care să reglementeze instituirea Sistemului	Procuratura Generală	Ministerul Afacerilor Interne; Serviciul de	Bugetul instituţiilor, în limitele alocaţiilor aprobate;	2019-2021	Cadru normativ elaborat

1	2	3	4	5	6	7	8
		informațional automatizat „E-dosar" în cadrul organelor implicate la efectuarea urmăririi penale și judecării cauzei, precum și implementarea, dezvoltarea și interconectarea acestuia		Informaţii şi Securitate; Centrul Naţional Anticorupţie; Serviciul Vamal, Centrul Național pentru Protecția Datelor cu Caracter Personal	asistenţă externă		
10.	Efectuarea cercetărilor ştiinţifice aplicative în domeniul securităţii informaţionale	1) planificarea și dezvoltarea activității de cercetare științifică în domeniul tehnologiei informaționale și comunicaționale;	Ministerul Educaţiei, Culturii și Cercetării; Academia de Științe a Moldovei; Agenția Națională de Dezvoltare și Cercetare		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Plan de acțiuni elaborat și aprobat
		2) crearea/consolidarea laboratoarelor de securitate cibernetică din cadrul instituțiilor de învățământ superior și instituțiilor de cercetare științifică	Academia de Științe a Moldovei	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; mediul privat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2022-2024	Număr de laboratoare de securitate cibernetică create și consolidate
11.	Dezvoltarea capacităţilor de rezilienţă cibernetică și ridicarea nivelului de cultură în domeniul TIC	1) desfășurarea acțiunilor de sensibilizare și informare a societății privind amenințările, vulnerabilitățile și riscurile securității cibernetice	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	Agenția de Guvernare Electronică; Serviciul de Informaţii şi Securitate; Ministerul Educaţiei, Culturii și Cercetării; Ministerul Economiei și Infrastructurii	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Număr de campanii de informare realizate

1	2	3	4	5	6	7	8
		2) realizarea de către Centrul național de reacție la incidentele de securitate cibernetică a analizei strategice a incidentelor de securitate cibernetică și coordonarea acțiunilor de răspuns la incidente de securitate, inclusiv prin organizarea cursurilor specializate de către experți calificați	Serviciul Tehnologia Informației și Securitate Cibernetică	Serviciul de Informații și Securitate; Agenția de Guvernare Electronică; Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2024	Raport a incidentelor de securitate cibernetică elaborat
		3) desfășurarea exercițiilor și antrenamentelor comune de consolidare a capacităților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate	Serviciul Tehnologia Informației și Securitate Cibernetică	Ministerul Apărării; Agenția de Guvernare Electronică; Ministerul Afacerilor Interne; Serviciul de Informații și Securitate; Procuratura Generală; Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2020-2024	Număr de exerciții realizate
		4) organizarea și efectuarea atelierelor de lucru în domeniul securității cibernetice pentru personalul din sectorul public și privat, deținătorii de elemente de infrastructură critică;	Serviciul Tehnologia Informației și Securitate Cibernetică	Ministerul Apărării; Agenția de Guvernare Electronică; Serviciul de Informații și Securitate; Ministerul Afacerilor Interne; Procuratura Generală; Centrul Național	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2020-2024	Număr de ateliere de lucru organizate

1	2	3	4	5	6	7	8
				pentru Protecția Datelor cu Caracter Personal; mediul privat; societatea civilă			
		5) certificarea specialiștilor în domeniul securității cibernetice de către organizațiile /companiile specializate în baza standardelor aplicate și cerințele minime obligatorii de securitate cibernetică aprobate;	Agenția de Guvernare Electronică	Ministerul Economiei și Infrastructurii; Serviciul Tehnologia Informației și Securitate Cibernetică; autoritățile administrației publice	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2020-2024	Număr de specialiști certificați
		6) crearea platformelor web de sensibilizare și informare privind pericolele în spațiul cibernetic și măsurile de protecție ce pot fi luate de către persoanele fizice și juridice	Serviciul Tehnologia Informației și Securitate Cibernetică	Agenția de Guvernare Electronică; Ministerul Afacerilor Interne; Procuratura Generală; mediul privat	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2020-2022	Platforme create
		7) introducerea și promovarea conținuturilor curriculare privind securitatea informațională în programele naționale de studii	Ministerul Educației, Culturii și Cercetării	Serviciul Tehnologia Informației și Securitate Cibernetică; Agenția de Guvernare Electronică; Serviciul de Informații și Securitate; Ministerul Afacerilor Interne; Procuratura	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2020-2021	Număr de instituții de învățământ în care au fost introduse conținuturile curriculare

1	2	3	4	5	6	7	8
				Generală; Centrul Național pentru Protecția Datelor cu Caracter Personal; societatea civilă			
		8) organizarea, inclusiv în comun cu partenerii străini, a cursurilor de instruire tematică în domeniul securității cibernetice pentru angajații din instituțiile publice	Agenția de Guvernare Electronică	Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	Permanent	Număr de cursuri de instruire realizate
PILONUL II: Asigurarea securității spațiului informațional-mediatic							
12.	Dezvoltarea mecanismelor de comunicare strategică pentru realizarea intereselor naționale ale Republicii Moldova	1) evaluarea sectoarelor vulnerabile ale componentei mediatice a sistemului de securitate informațională	Autoritățile administrației publice		Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2020-2021	Raport de evaluare a sectoarelor vulnerabile a comunicării strategice
		2) dezvoltarea politicilor de comunicare strategică pe plan intern și racordarea la platformele de comunicare strategică externe, ale structurilor sistemului de securitate, apărare și ordine publică, pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova	Consiliul Coordonator al Audiovizualului	Autoritățile administrației publice; societatea civilă; organizațiile mass-media	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2020-2024	Acorduri elaborate și aprobate
		3) crearea, în Republica Moldova, a resursei /platformei informaționale de comunicare strategică, care va conține informații privind: a) incidentele de securitate informațională; b) ghiduri de comunicare	Serviciul de Informații și Securitate	Societatea civilă; organizațiile mass-media	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2024	Resursă/platformă informațională creată și prezentată

1	2	3	4	5	6	7	8
		strategică pe subiecte de interes naţional; c) tentative şi acţiuni de dezinformare şi sau informare manipulatore ce afectează securitatea informaţională şi stare generală de securitate					
13.	Controlul civic şi consolidarea cooperării societăţii civile cu autorităţile publice cu atribuţii de asigurare a securităţii informaţionale	1) crearea unui mecanism de implicare a experţilor din rîndul societăţii civile, organizaţiilor nonguvernamentale şi mass-mediei în domeniul securităţii informaţionale, prin: a) desemnarea unui Consiliu al societăţii civile sau crearea unui organ colectiv din rîndul societăţii civile cu atribuţii de evaluare a experţilor, organizaţiilor nonguvernamentale şi mass-mediei, din perspectiva implicării în materie de asigurarea a securităţii informaţionale şi naţionale; b) certificarea de către Consiliul societăţii civile a experţilor şi reprezentanţilor societăţii civile şi ai mass-mediei ce se vor preocupa de monitorizarea nivelului de asigurare a securităţii informaţionale la nivel naţional	Societatea civilă, organizaţii mass-media	Autorităţile statului ale sistemului de securitate şi apărare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	
		2) implicarea reprezentanţilor societăţii civile certificaţi de Consiliului societăţii civile în cadrul	Societatea civilă, organizaţii mass-media	Autorităţile statului ale sistemului de securitate şi apărare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Perioada implementării Strategiei securităţii	

1	2	3	4	5	6	7	8
		Consiliului coordonator pentru asigurarea securităţii informaţionale				informaţionale a Republicii Moldova pentru anii 2019-2024	
		3) îmbunătăţirea sau crearea mecanismelor de implicare a societăţii civile în procesele de definire, elaborare, monitorizare şi de evaluare a politicilor de asigurare a securităţii informaţionale realizate de autorităţile abilitate în asigurarea securităţii informaţionale	Societatea civilă, organizaţii mass-media	Autorităţile statului ale sistemului de securitate şi apărare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Perioada implementării Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024	
		4) elaborarea şi organizarea unor cursuri de instruire tematică pentru radiodifuzori, distribuitori de servicii, formatori de opinie, jurnalişti şi ONG-uri de profil cu privire la tehnicile de dezinformare şi/sau informare manipulatoare utilizate pentru prejudicierea securităţii informaţionale a statului.	Societatea civilă, organizaţii mass-media	Autorităţile statului ale sistemului de securitate şi apărare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Perioada implementării Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024	
14.	Determinarea statutului juridic al publicaţiilor periodice, agenţiilor de presă şi altor subiecţi care activează în spaţiului media din Internet	1) evaluarea spaţiului Internet din perspectiva identificării actorilor implicaţi în producerea şi diseminarea conţinutului media on-line şi alţi intermediari şi servicii auxiliare ce au impact pentru securitatea informaţională	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; autorităţile	Societatea civilă, Organizaţii mass-media	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2024	Raport/studiu realizat.

1	2	3	4	5	6	7	8
			administrației publice				
		2) elaborarea și ajustarea cadrului legal funcțional în scopul reglementării juridice a raporturilor dintre actorii mass-media care colectează și difuzează informații în Internet, societate și autoritățile abilitate cu atribuții de asigurare a securității informaționale, în conformitate cu recomandările Comisiei Europene și bunele practici europene	Serviciul de Informații și Securitate; Ministerul Justiției; Consiliul Coordonator al Audiovizualului; autoritățile administrației publice	Societatea civilă, Organizații mass-media	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2024	Cadru normativ elaborat și aprobat
		3) implementarea cadrului normativ definit prin acțiuni comune de intervenție și gestionarea spațiului media on-line și off-line	Autoritățile administrației publice; societatea civilă	Mediul privat	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2024	Raport privind gradul de implementare a cadrului normativ aprobat
15.	Asigurarea transparenței financiare în activitatea autorităților publice, a asociațiilor obștești și a societăților comerciale în contextul asigurării securității informaționale	1) elaborarea sub egida Consiliului coordonator pentru asigurarea securității informaționale a criteriilor de calificare a informației ca produs de dezinformare, manipulare și propagandă, orientate spre subminarea securității informaționale, în scopul identificării: comanditarilor, surselor de finanțare și a executorilor	Serviciul de Informații și Securitate; Ministerul Justiției; Centrul Național Anticorupție; Consiliul Coordonator al Audiovizualului	Societatea civilă; organizații mass-media	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2024	Criterii de calificare elaborate
		2) ajustarea cadrului legal în vederea eficientizării colectării de date pentru identificarea proveniență mijloacelor financiare și	Serviciul de Informații și Securitate; Ministerul Justiției; Centrul Național	Societatea civilă; organizații mass-media	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2019-2024	Cadru normativ elaborat și aprobat

1	2	3	4	5	6	7	8
		proprietății ale subiecților implicați în activități de dezinformare, manipulare și propagandă ce subminează securitatea informațională	Anticorupţie; Consiliul Coordonator al Audiovizualului				
		3) interacțiunea cu instituțiile de drept în ceea ce privește analiza riscurilor și amenințărilor din domeniul mass-mediei, în scopul monitorizării evoluţiei amenințărilor depistate, investigării activității subversive sau penale în spaţiul informaţional, stabilirii surselor de finanțare a factorilor de risc	Serviciul de Informaţii şi Securitate	Serviciul de Informaţii şi Securitate; Procuratura Generală; Ministerul Afacerilor Interne; Centrul Naţional Anticorupţie	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Mecanism de cooperare implementat; cadru normativ elaborat și aprobat
Pilonul III. Consolidarea capacităților operaționale							
16.	Dezvoltarea mecanismelor de prevenire, de depistare, de atenuare şi de răspuns la nivel naţional pentru asigurarea securităţii informaţionale	1) crearea, la nivel național, a entității ce va avea competenţe de promovare şi coordonare a politicilor de securitate informaţională într-o societate democratică, în funcţie de dezvoltarea tehnologiei, raporturile juridice şi de altă natură din sectorul societății informaționale la nivel național și internațional (Consiliul coordonator pentru asigurarea securităţii informaţionale): a) identificarea și integrarea componentelor existente cu funcții și atribuții din domeniul cibernetic, mediatic și a autorităților	Serviciul de Informaţii şi Securitate	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; autoritățile administrației publice; societatea civilă; organizații mass-media; mediul privat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2019-2021	Act normativ de creare a entității elaborat și aprobat

1	2	3	4	5	6	7	8
		administrației publice locale și a celor care vor fi create pe parcurs; b) determinarea domeniului de activitate pentru fiecare componentă inclusă în cadrul entității, în funcție de funcțiile și atribuțiile deținute din perspectiva asigurării securității informaționale; c) elaborarea și adoptarea cadrului normativ de interacțiune pentru realizarea sarcinilor de depistare, prevenire și contracarare a riscurilor și amenințărilor la adresa securității informaționale					
		2) elaborarea, promovarea și coordonarea politicilor de securitate informațională conform Concepției, prezentei Strategii și a altor documente de politici de nivel național și internațional ce se referă la societatea informațională	Serviciul de Informații și Securitate	Serviciul Tehnologia Informației și Securitate Cibernetică; autoritățile administrației publice; societatea civilă; organizații mass-media; mediul privat	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2024	Mecanisme clare de interacțiune inter-instituționale elaborate și aprobate
		3) informarea publicului privind modalitățile de prevenire și contracarare a riscurilor și amenințărilor la adresa componentelor sistemice a securității informaționale, inclusiv	Serviciul de Informații și Securitate	Autoritățile administrației publice; societatea civilă; organizații mass-media	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021-2024	Număr de campanii de informare

1	2	3	4	5	6	7	8
		privind fenomenele nou-apărute la nivel național					
17.	Dezvoltarea capacităților de reacție în cazul unor amenințări hibride de securitate	1) crearea unei componente analitico-informaționale specializată pe amenințările hibride de securitate în cadrul Serviciului de Informații și Securitate;	Serviciul de Informaţii şi Securitate	Ministerul Afacerilor Externe și Integrării Europene; Ministerul Afacerilor Interne; Procuratura Generală; Ministerul Apărării	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2024	Act privind crearea componentei analitico-informaționale elaborat și aprobat
		2) crearea rețelei naționale a autorităților responsabile de combaterea amenințărilor hibride de securitate;	Serviciul de Informaţii şi Securitate		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Acord privind crearea unei rețele naționale
		3) elaborarea unor protocoale operaționale de interacțiune între autoritățile responsabile şi factorii de decizie în cazul unor amenințări hibride de securitate;	Serviciul de Informaţii şi Securitate	Autoritățile administrației publice; societatea civilă; organizații mass-media; mediul privat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Număr de protocoale elaborate și semnate
		4) consolidarea gradului de cunoaştere şi înţelegere a concepţiei ameninţărilor hibride de securitate la nivelul organelor abilitate de asigurarea securităţii informaţionale şi a mediului general de securitate	Serviciul de Informaţii şi Securitate	Autoritățile administrației publice; societatea civilă; organizații mass-media; mediul privat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Număr de protocoale interinstituționale încheiate
		5) efectuarea exercițiilor pentru dezvoltarea capacităților autorităților specializate în combaterea amenințărilor hibride de securitate	Serviciul de Informaţii şi Securitate	Autoritățile administrației publice; societatea civilă; organizații mass-media	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Număr de exerciții de cercetare și expertizare
		6) asocierea Republicii	Serviciul de	Autoritățile	Bugetul instituţiilor,	2022-2024	Act normativ (acord)

1	2	3	4	5	6	7	8
		Moldova la Centrul European de Excelență pentru combaterea amenințărilor hibride	Informaţii şi Securitate	administrației publice; societatea civilă; organizații mass-media; mediul privat	în limitele alocaţiilor aprobate; asistenţă externă		elaborat și încheiat
18.	Dezvoltarea competențelor operaţionale de apărare cibernetică	1) crearea entităţii responsabile de apărarea cibernetică la nivelul Forțelor Armate	Ministerul Apărării	Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021	Entitate creată
		2) consolidarea capacităților de educație cibernetică și formare prin participarea la exerciții interstatale și internaționale de apărare cibernetică	Ministerul Apărării; Serviciul de Informaţii şi Securitate	Ministerul Afacerilor Externe și Integrării Europene; Ministerul Afacerilor Interne (Serviciul Tehnologia Informației)	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2019-2024	Număr de personal instruit, exerciţii desfăşurate
		3) identificarea, prevenirea şi contracararea factorilor de risc cu potenţial informativ-subversiv în adresa apărării cibernetice a Republicii Moldova prin implementarea unui management integrat al spaţiului virtual și dezvoltarea unui sistem de avertizare timpurie cu privire la elementele de risc la adresa obiectivelor de infrastructură	Serviciul de Informaţii şi Securitate	Ministerul Apărării; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Ministerul Economiei și Infrastructurii	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Raport privind riscurile identificate şi/sau prevenite

1	2	3	4	5	6	7	8
19.	Monitorizarea spațiului informațional și de depistare a acțiunilor de dezinformare și /sau de informare manipulatoare din exteriorul și interiorul țări	4) revizuirea cadrului legal existent în direcția definirii și uniformizării noțiunilor cu privire la dezinformare, știrile false și/sau informare manipulatoare, precum și prevenirea răspîndirii acestora prin platformele media. Determinarea sectoarelor securității naționale a căror afectare (de către dezinformare) creează riscuri majore pentru funcționalitatea statului	Ministerul Justiţiei; Consiliul Coordonator al Audiovizualului	Serviciul de Informaţii şi Securitate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2024	Cadru normativ revizuit; comunicate privind sectoarele de risc ale securităţii naţionale identificate
		5) stabilirea atribuțiilor (organelor competente) pentru depistarea și contracararea mesajelor manipulatorii și de dezinformare din spațiul informațional (Internet)	Serviciul de Informaţii şi Securitate	Academia de Ştiinţe a Moldovei; organizațiile societății civile; mass-media	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Cadrul legal modificat
		6) stabilirea unor filtre de depistare și sau/blocare a diverselor produse informaționale și/sau resurse informaționale, care conțin elemente de risc în adresa securității naționale, precum și elaborarea, adoptarea cadrului normativ aferent	Serviciul de Informaţii şi Securitate	Academia de Ştiinţe a Moldovei; organizațiile societății civile, mass-media	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Cadru normativ elaborat şi adoptat
20.	Sporirea capacităților de protecție a infrastructurilor critice naționale	1) elaborarea și aprobarea cadrului legal privind identificarea și desemnarea infrastructurilor critice naționale, inclusiv ce țin de sistemele informaționale de importanță vitală	Serviciul de Informaţii şi Securitate	Autoritățile administrației publice	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2019-2021	Cadru legal elaborat și aprobat

1	2	3	4	5	6	7	8
		2) evaluarea și raportarea privind starea și nivelul de securitate a obiectivelor de infrastructură critică din perspectiva asigurării securității informaționale	Serviciul de Informaţii şi Securitate	Autoritățile administrației publice	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021-2024	Mecanism de evaluare și raportare realizat
21.	Dezvoltarea capacităților de prevenire, de depistare și de contracarare a acțiunilor extremiste, teroriste și de altă natură care periclitează securitatea informațională	1) sincronizarea și repartizarea rațională a forțelor instituțiilor Republicii Moldova spre depistarea preventivă a acțiunilor derulate din exteriorul și/sau interiorul țării, concepute ca diversiuni complexe la adresa securității informaționale;	Serviciul de Informaţii şi Securitate	Ministerul Afacerilor Interne; Procuratura Generală; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2022	Mecanisme de interacţiune inter-instituţională elaborate; schimb sistematic de informaţii implementat
		2) raportarea către Serviciul de Informaţii şi Securitate a informaţiei despre starea de risc de la instituţiile statului cu competenţă în domeniu;	Autoritățile administrației publice	Serviciul de Informaţii şi Securitate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Număr de rapoarte transmise/recepționate
Pilonul IV. Eficientizarea procesului de coordonare internă și cooperare internațională în domeniul securității informaționale							
22.	Dezvoltarea sistemului de pregătire a resurselor umane în domeniul securităţii informaţionale	1) evaluarea nivelului actual de pregătire a resurselor umane în domeniul securităţii informaţionale, pe fiecare compartiment în parte: mass-media, tehnologia informaţională, apărare, ordine publică şi contrainformaţii.	Autoritățile administrației publice; Consiliul Coordonator al Audiovizualului; Ministerul Economiei și Infrastructurii; Ministerul Apărării; Ministerul Afacerilor Interne; Procuratura Generală; Serviciul de Informaţii şi Securitate;	Ministerul Educației, Culturii și Cercetării	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	Studiu efectuat

1	2	3	4	5	6	7	8
			organizații nonguvernamentale				
		2) identificarea categoriilor de beneficiari care urmează, cu prioritate, să fie incluşi în programe noi de instruire a resurselor umane în domeniul vizat.	Autoritățile administrației publice	Consiliul Coordonator al Audiovizualului; Ministerul Economiei și Infrastructurii; Ministerul Apărării; Ministerul Afacerilor Interne; Procuratura Generală; Serviciul de Informaţii şi Securitate; organizații nonguvernamentale din domeniul media	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2021	Număr de beneficiari identificați și instruiți
		3) elaborarea unor programe noi de pregătire a resurselor umane în domeniul vizat	Ministerul Educaţiei, Culturii și Cercetării; Academia de Științe a Moldovei	Consiliul Coordonator al Audiovizualului; Ministerul Economiei și Infrastructurii; Ministerul Apărării; Ministerul Afacerilor Interne; Procuratura Generală; Serviciul de Informaţii şi Securitate; Centrul Național pentru Protecția Datelor cu Caracter Personal; organizații nonguvernamentale din domeniul media	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2022	Număr de programe elaborate

1	2	3	4	5	6	7	8
		4) dezvoltarea și implementarea unor programe de instruire dedicate angajaților cu atribuții de investigare și urmărire penală, procurorilor, judecătorilor, specialiştilor şi experţilor judiciari în domeniu, din cadrul structurilor de aplicare a legii, precum și celor dedicate personalului tehnic din cadrul instituțiilor publice	Academia de Științe a Moldovei; Institutul Național al Justiției; Ministerul Afacerilor Interne (Academia Ștefan cel Mare)	Ministerul Educației, Culturii și Cercetării; Consiliul Coordonator al Audiovizualului; Ministerul Economiei și Infrastructurii; Ministerul Apărării; Procuratura Generală; Serviciul de Informații și Securitate; Centrul Național pentru Protecția Datelor cu Caracter Personal; organizații nonguvernamentale din domeniul media	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2022-2024	Număr de programe elaborate
23.	Coordonarea activităţii autorităţilor administraţiei publice, a instituţiilor publice şi private în ceea ce priveşte exercitarea atribuţiilor privind asigurarea securităţii informaţionale	1) identificarea cadrului normativ relevant ce reglementează atribuţiile autorităţilor administraţiei publice, a instituţiilor publice şi private privind asigurarea securităţii informaţionale şi ajustarea acestuia, excluzînd lacunele şi dublările de competenţă	Autorităţile menţionate în Concepţie, în limitele lor de competenţă		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020	Cadrul normativ revizuit
		2) reglementarea expresă în legislaţie a atribuţiei de coordonare a activităţii autorităţilor administraţiei publice, a instituţiilor publice şi private în ceea ce priveşte exercitarea atribuţiilor privind asigurarea securităţii	Autorităţile menţionate în Concepţie, în limitele lor de competenţă		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020	Cadrul normativ revizuit, activitatea instituției responsabile reglementată

1	2	3	4	5	6	7	8
		informaţionale, precum şi a mecanismului de realizare a acesteia, de către autoritatea publică desemnată					
		3) elaborarea şi încheierea unor acorduri de cooperare interinstituţionale multilaterale care vor specifica modul de coordonare a activităţii în partea ce ţine de exercitarea atribuţiilor privind asigurarea securităţii informaţionale	Autorităţile menţionate în Concepţie, în limitele lor de competenţă		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	Număr de acorduri de colaborare încheiate
24.	Asigurarea cooperării internaţionale în domeniul securităţii informaţionale.	1) evaluarea nivelului actual al cooperării Republicii Moldova cu organizaţiile internaţionale ce îşi desfăşoară activitatea în domeniul asigurării securităţii informaţionale şi elaborarea acţiunilor pentru intensificarea cooperării respective	Autorităţile administraţiei publice		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2021	Studiu de evaluare elaborat
		2) stabilirea cooperării cu statele partenere, în special din cadrul Uniunii Europene, privind schimbul de informaţii, experienţe şi analize în scopul prevenirii, depistării şi contracarării ameninţărilor hibride de securitate în spaţiul informaţional	Autorităţile administraţiei publice	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2024	Număr de runde de consultări organizate
		3) Promovarea pe plan internaţional, inclusiv în cadru bilateral, a necesităţii încheierii unor tratate internaţionale ce ar unifica	Autorităţile administraţiei publice	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2024	Număr de tratate internaţionale negociate/semnate

1	2	3	4	5	6	7	8
		conceptul de „armă informaţională", interzicînd elaborarea, răspîndirea şi aplicarea acesteia în relaţiile între state					
		4) alinierea şi implementarea instrumentelor internaţionale existente ce ar asigura prevenirea, depistarea şi contracararea accesului neautorizat la informaţiile cu accesibilitate limitată din reţelele de comunicaţii electronice bancare şi din sistemele de comerţ electronic, la informaţiile organelor internaţionale de drept	Autorităţile administraţiei publice	Ministerul Justiţiei; Ministerul Afacerilor Externe şi Integrării Europene	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2024	Cadrul normativ modificat şi completat
25.	Dezvoltarea cooperării naţionale şi internaţionale în domeniul apărării cibernetice.	1) crearea/implementarea cadrului de cooperare interinstituţională pe domeniul apărării cibernetice	Ministerul Apărării; Serviciul de Informaţii şi Securitate; Ministerul Economiei şi Infrastructurii; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică; Procuratura Generală; Ministerul Afacerilor Interne	Autorităţile administraţiei publice	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2024	Număr de runde de consultări organizate
		2) intensificarea cooperării cu partenerii externi de dezvoltare privind schimbul	Ministerul Apărării	Ministerul Afacerilor Externe şi Integrării	Bugetul instituţiilor, în limitele alocaţiilor aprobate;	2020-2024	Număr de acorduri negociate/semnate

1	2	3	4	5	6	7	8
		de informaţii şi experienţă în domeniul apărării cibernetice		Europene; Serviciul de Informaţii şi Securitate; Ministerul Economiei şi Infrastructurii; Serviciul Tehnologia Informaţiei şi Securitate Cibernetică	asistenţă externă		
		3) semnarea acordurilor de colaborare (asistenţă mutuală) în domeniul apărării cibernetice	Ministerul Apărării; Serviciul de Informaţii şi Securitate	Centru național de reacție la incidentele de securitate cibernetică; Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	2020-2024	Număr de acorduri negociate/semnate
26.	Consolidarea cooperării internaționale în domeniul prevenirii criminalității informatice	1) consolidarea mecanismelor de cooperare internațională între autoritățile statului cu atribuții în combaterea criminalității informatice și organismelor internaționale specializate EMAS (Europol Malware Analysis Service) al EUROPOL	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Mecanisme instituite/ consolidate
		2) utilizarea, la nivel național, a instrumentelor și metodelor de identificare a victimelor, inclusiv prin utilizarea Sistemului Informațional "Protecția Copiilor" și a bazei de date „ICSE" a OIPC INTERPOL	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală		Bugetul instituţiilor, în limitele alocaţiilor aprobate; asistenţă externă	Permanent	Instrumente și metode identificate și utilizate

1	2	3	4	5	6	7	8
		3) cooperarea în cadrul punctelor naționale de contact 24/7 în baza Convenției Consiliului Europei privind criminalitatea informatică (Budapesta 2001) și 24/7 G7	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	Permanent	Act de cooperare stabilit
		4) dezvoltarea parteneriatelor existente NCMEC (Centrul Național al SUA privind copiii dispăruți și exploatați) și aderarea la alte inițiative similare	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	La necesitate	Număr de acorduri și parteneriate stabilite
		5) dezvoltarea parteneriatelor în scopul identificării; blocării, sechestrării şi confiscării produselor şi a instrumentelor provenite din infracțiunile transfrontaliere	Ministerul Afacerilor Interne; Procuratura Generală; Serviciul de Informații și Securitate	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	2021	Mecanism identificat și implementat
		6) participarea la evenimente internaționale în domeniul prevenirii și combaterii criminalității informatice în scopul formării personalului de specialitate	Ministerul Afacerilor Externe și Integrării Europene; Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală; Serviciul de Informații și Securitate		Bugetul instituțiilor, în limitele alocațiilor aprobate; asistență externă	Permanent	Număr de evenimente frecventate; experți instruiți

Nota informativă

la proiectul Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și Planul de acțiuni pentru implementarea acesteia

I. Autorul proiectului și condițiile ce au impus elaborarea acestuia

Legea nr. 299 din 21.12.2017 privind aprobarea Concepției securității informaționale a Republicii Moldova, stabilește la art. 3 că, în termen de 6 luni de la data intrării în vigoare, urmează a fi elaborată și prezentată spre examinare Strategia securității informaționale a Republicii Moldova și Planul de acțiuni pentru implementarea acesteia.

În acest context, în scopul realizării acțiunilor stabilite de Legea nr. 299/2017, a fost creat Grupul de lucru interinstituțional, format din 12 autorități/instituții. Sarcina convocării grupului de lucru, a fost stabilită Serviciului de Informații și Securitate al Republicii Moldova.

Conștientizând importanța, complexitatea și scopul major propus de către documentul de politici, Grupul de lucru, convocat în mai multe ședințe, a elaborat – proiectele Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 *(în continuare - Strategie)* și a Planului de acțiuni pentru implementarea acesteia *(în continuare - Plan)*.

Ținând cont de prevederile Concepției securității informaționale, în cadrul Grupului de lucru a fost luată decizia de a proiecta Strategia într-un spațiu temporal mediu de 5 ani, fiind determinată perioada 2019-2024.

Scopul Strategiei este ***corelarea juridică și integrarea sistemică a domeniilor prioritare cu responsabilități și competențe de asigurare a securității informaționale la nivel național, bazat pe reziliență cibernetică, pluralism multimedia și convergență instituțională în materie de securitate, destinate protejării suveranității, independenței și integrității teritoriale a Republicii Moldova.***

Totodată, Legea nr.299/2017 prevede la art. 2, elaborarea Programului de măsuri pentru implementarea Concepției securității informaționale, iar Strategia 2018-2023 este parte componentă a acestui document. Ca proces definitoriu, Programul prevede acțiuni de raportare, armonizare și eficientizare a documentului, iar în perioada 2019-2024 se va efectuata o evaluare integrală a gradului de realizare a scopului, măsurilor și acțiunilor propuse prin Strategie.

Strategia este structurată în **7 Capitole** și compusă din **117 puncte**.

Capitolul I – Introducere

Descrie evoluția curentă a tehnologiilor informaționale și a sistemelor de comunicare electronică la nivel global, european, național și stabilește parcursul Republicii Moldova în partea dezvoltării și realizării programelor și politicilor de dezvoltare a spațiului informațional, dezvăluie beneficiile incontestabile a tehnologiei moderne, precum și evidențiază principalele vulnerabilități, riscuri și amenințări la adresa societății informaționale și a mediul național și general de securitate.

Capitolul II – Descrierea Situației

Capitolul doi conține o descriere detaliată a parcursului Republicii Moldova în partea dezvoltării societății informaționale, actelor naționale și internaționale adoptate până în prezent care reglementează totalitatea raporturilor juridice apărute între subiecții, obiectul și interacțiunea spațiului informațional.

La descrierea situației, au fost expuse principalele documente de politici ce reglementează domeniile societăţii informaţionale existente la momentul elaborării prezentei Strategii, tangențiale dimensiunii de securitate informațională, în special: *Strategia națională de dezvoltare a societății informaționale „Moldova Digitală 2020" aprobată prin Hotărârea Guvernului nr. 857 din 31.10.2013* și *Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 aprobat prin Hotărârea Guvernului nr. 811 din 29.10.2015.*

În descrierea situației, s-a făcut referire la importanţa majoră de adoptare a Strategiei, care este determinată de necesitatea protecţiei intereselor persoanelor, societăţii, statului în spaţiul informaţional, de gravitatea şi multitudinea ameninţărilor la adresa securităţii informaţionale în societatea modernă, de necesitatea menţinerii unui echilibru între interesele persoanelor, societăţii şi statului pentru asigurarea securităţii informaţionale.

Totodată, legislația pertinentă la moment nu reglementează și respectiv nu asigură suficient așa deziderate precum tentative de dezinformare și/sau de informare manipulatoare, protecția vieții private și a datelor cu caracter personal la plasarea informației în Internet, din considerent că acțiunea acestor legi este restrânsă și/sau au alt scop de reglementare.

Or, menţinerea unui echilibru între componentele de bază în cadrul unui stat de drept, poate fi realizat doar cu condiția existenței și funcționării cadrului legislativ-normativ în domeniu, a instrumentelor și metodelor clare, a mecanismelor de interacţiune sistemică la nivel naţional şi colaborare eficientă la nivel internaţional.

Capitolul III – Definirea Problemelor

Făcând o sinteză amplă asupra proiectului Strategiei, reliefăm coroborarea directă a capitolului III și capitolul IV, și anume în partea ce vizează descrierea problemelor reale din Republica Moldova la capitolul asigurării securității spațiului informațional și propunerea soluțiilor de ameliorare *(prin obiective și măsuri concrete).* În acest sens, scopul enunțat al Strategiei de a corela juridic și a integra sistemic, constă în următoarele:

1) Una din problemele majore este lipsa unui sistem integrat de management al securităţii cibernetice, de tip CERT (Centru de reacţie la incidente de securitate cibernetică), în cadrul căruia să se efectueze coordonarea, planificarea şi utilizarea resurselor disponibile, identificarea vulnerabilităţilor şi riscurilor în urma auditului de securitate cibernetică. Respectiv, prin acțiunile propuse în Strategie urmează să se proiecteze intervenţiile necesare pentru diminuarea impactului negativ al criminalităţii, atacurilor şi incidentelor cibernetice asupra dezvoltării sigure a societăţii informaţionale.

Prin mecanismele stabilite la Pilonul I din Strategie, se propune crearea unui cadru legal eficient care va asigura securitatea statului prin prisma fiecărei componente stabilite, diminuarea riscurilor, ameninţărilor sau chiar excluderea într-o perspectivă a acestora, şi crearea sau desemnarea a unei entităţi la nivel naţional de tip CERT şi elaborarea mecanismelor de creare şi consolidare a centrelor departamentale de reacţie la incidentele de securitate cibernetică şi informaţionale atât de drept public cât şi de drept privat.

2) Accesarea neautorizată a reţelelor şi serviciilor de comunicaţii electronice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice, restricţionarea ilegală a accesului la aceste date şi spionajul cibernetic constituie constrângeri la nivel global. În acest context, se evidenţiază problemele cu care se confruntă Republica Moldova şi anume: creşterea numărului infracţiunilor şi contravenţiilor informatice, a numărului atacurilor cibernetice asupra resurselor informaţionale publicate în reţeaua globala Internet precum şi a deficitului de resurse umane competente.

În acest sens, prin acţiunile trasate la Pilonul I şi parţial Pilonul IV expuse în Strategie, se propune iniţierea unor modificări la principalele acte legislative de prevenire şi combatere a criminalităţii informatice, în scopul armonizării legislaţiei în domeniu, precum şi dezvoltarea programelor sectoriale dedicate angajaţilor cu atribuţii de investigare şi urmărire penală.

3) O atenţie specială a fost atrasă componentei de securitate a spaţiului mediatic. În acest context, dezinformarea, propaganda şi informarea manipulatoare din exterior constituie una din problemele de bază.

Ca soluţii de ameliorare statuate în Pilonul II, se propune elaborarea şi ajustarea unor mecanisme legale funcţionale în scopul contracarării fenomenului de dezinformare şi/sau informare manipulatorie care periclitează direct securitatea spaţiului informaţional.

4) Componenta contrainformativă şi de securitate defineşte problemele ce vizează extinderea la scara largă de către diferiţi actori a utilizării mijloacelor de imixtiune în raporturile interne ale Republicii Moldova prin propagandă şi agresiune mediatică, precum şi de influenţa informaţional-psihologică, cu scopul de a destabiliza situaţia social-politică, submina suveranitatea şi integritatea teritorială a Republicii Moldova. Totodată, se punctează campaniile active de informare realizate, de organizaţiile teroriste internaţionale, în scopul subminării şi creşterii nivelului de ură împotriva intereselor statutului de drept şi a valorilor universal acceptate de comunitatea internaţională.

Prin soluţiile trasate în Pilonul III, se propune perfectarea cadrului juridic întru depistarea, prevenirea şi contracararea acţiunilor de promovare a diverselor produse informaţionale şi/sau resurse informaţionale, care conţin elemente de risc şi pot genera ameninţări la adresa securităţii naţionale.

5) Importanţa sensibilizării şi educării societăţii într-un spirit valoric este una din prerogativele stabilite în Strategie, care urmează într-o perspectivă a fi mediatizată şi dezvoltată. La moment, se atestă lipsa capacităţii de protecţie contra fenomenului de defăimare prin intermediul platformelor on-line, fapt ce afectează exercitarea drepturilor omului şi a libertăţilor fundamentale. De asemenea, se evidenţiază importanţa sensibilizării, educării, competenţei

mediatice și cibernetice în Republica Moldova, pentru a permite cetățenilor să analizeze în mod critic conținutul mediatic, în vederea identificării propagandei.

În acest sens, autorii Strategiei propun acțiuni spre realizare în direcția ameliorării problemelor la acest compartiment prin acțiunile trasate la Pilonul II și IV. Astfel, prerogativa armonizării cadrului normativ și elaborarea politicilor de comunicare între autoritățile statului și societatea civilă, ar permite consolidarea implicării tuturor subiecților de drept în procesul consultativ și decizional. Ca rezultat va spori gradul de încredere în acțiunile autorităților statului în contextul apărării drepturilor și libertăților fundamentale ale cetățenilor, precum și va permite conștientizarea acestora referitor la necesitatea adoptării unui comportament civic.

Capitolul IV - Viziune și Obiective ale Strategiei

Acest capitol, reglementează viziunea strategică a documentului de politici, care stabilește că în contextul implementării cu succes, **Republica Moldova va asigura un spațiu informațional sigur, pentru toți subiecții de drept, prin armonizarea cadrului legal și implementarea acestuia, astfel protejând drepturile și libertățile fundamentale ale omului și promovând democrația și statul de drept.**

Tot aici, sunt descrise obiectivele[1] și acțiunile concrete pentru realizarea scopului Strategiei, care sunt repartizate pe 4 piloane, definitivate din perspectiva principalelor componente de structură și funcționalitate a societății informaționale. Este important de specificat că în urma analizei detaliate a situației mediului de securitate informațională, Grupul de lucru a determinat complexul de acțiuni reale menite să redreseze problemele identificate și elucidate în Capitolul III. Respectiv, s-a accentuat necesitate de a evita abordarea superficială și înaintarea unor mecanisme nelucrative, în special în contextul în care asigurarea securității informaționale reprezintă unul din dezideratele propuse și la nivel internațional.

Astfel, **Pilonul I** vizează asigurarea securității spațiului informațional-cibernetic și investigarea criminalității informatice, care se va realiza prin 11 obiective specifice.

Printre prioritățile de bază stabilite în Pilonului I sunt:

- Crearea Centrului național de reacție la incidentele de securitate cibernetică (CERT național), care va asigura interacțiunea dintre toate componentele de asigurare a securității cibernetice.
- Desemnarea entității care va exercita rolul de Centru Guvernamental de reacție la incidentele de securitate cibernetică al Guvernului (CERT Gov) care va asigura funcționarea și protecția rețelelor speciale la nivel de Guvern și autorități publice.
- Consolidarea cooperării CERT-ului Național, CERT-ului Guvernamental și CERT-urilor private, în scopul prevenirii și soluționării incidentelor de securitate cibernetică.

Pilonul II implică asigurarea securității spațiului informațional-mediatic, prin 3 obiective specifice.

[1] Obiectivele în mare parte sunt preluate din Concepția securității informaționale.

Măsurile statuate în acest Pilon, creează și dezvoltă capacitatea statului de reacționarea în timp util, prin intermediul organelor specializate, la amenințările parvenite din mediul care la moment este greu de asigurat și anume, spațiul mediatic din Internet și audiovizualului.

În urma realizării acțiunilor stabilite de Pilonul II, va fi creat(ă):

➢ Un mecanism de interacțiune și implicare a experților în scopul asigurării securității spațiului informațional prin dezvoltarea controlului civic în direcția asigurării securității informaționale.

➢ Cadrul legal pentru determinarea statutului juridic al publicațiilor periodice, agențiilor de presă și altor subiecți care activează în spațiului media din Internet, în scopul identificării actorilor implicați în producerea și diseminarea conținutului media on-line și alți intermediari și servicii auxiliare ce au impact negative pentru securitatea informațională.

➢ Resursa informațională de comunicare și informare strategică, precum și un sistem unic de protecție a informației ce întrunește măsurile legale, organizaționale, tehnice, tehnologice și fizice de protecție.

Pilonul III se referă la consolidarea capacităților operaționale, care se va realiza prin 6 obiective specifice.

Avînd în vedere că securitatea informațională reprezintă o componentă inseparabilă a securității naționale, aceasta poate fi asigurată doar printr-o eficientă conlucrare a tuturor autorităților statului în limita competențelor stabilite de lege. Prin Pilonul III, propunem realizarea următoarele sarcini prioritare:

➢ Crearea la nivel național a entității ce va avea competențe de promovare și coordonare a politicilor de securitate informațională într-o societate democratică, în funcție de dezvoltarea tehnologiei, raporturile juridice și de altă natură din sectorul societății informaționale la nivel național și internațional - Consiliul coordonator pentru asigurarea securității informaționale.

➢ Crearea entității responsabile de apărarea cibernetică la nivelul Forțelor Armate, cu rol de coordonator la nivel strategic a activităților destinate apărării securității cibernetice a Republicii Moldova.

➢ Crearea platformei specializate pe amenințările hibride de securitate, element important din perspectiva construcției sistemului de contracarare a amenințărilor hibride la adresa securității informaționale, va corela informația disponibilă și va facilita răspunsul direct la situație de criză a autorităților relevante.

➢ Elaborarea și promovarea cadrului legal de reglementare a infrastructurii critice naționale în scopul sporirii capacităților de protecție a infrastructurilor critice naționale, dezvoltării capacităților de prevenire, de depistare și de contracarare a acțiunilor extremiste, teroriste și de altă natură care periclitează securitatea informațională.

În contextul elaborării Strategiei, un accent deosebit a fost stabilit pe necesitatea eficientizării procesului de coordonare internă și cooperare internațională în domeniul securității informaționale.

În acest sens, **Pilonul IV** Fiind compus din 5 obiective specifice are drept scop:

➢ Perfecţionarea şi coordonarea activităţii autorităţilor publice responsabile de asigurarea securităţii spaţiului informaţional.

➢ Crearea programelor sectoriale de instruire a resurselor umane în domeniul securităţii informaţionale, pe fiecare compartiment în parte: mass-media, tehnologia informaţională, apărare, ordine publică şi contrainformaţii.

➢ Asigurarea şi dezvoltarea cooperării internaţionale pe două domenii distincte cel al apărării cibernetice şi cel al criminalităţii informatice.

Capitolul V – Estimarea impactului și a costurilor implementării Strategiei.

Capitolul V din Strategie, face o descriere a impactului şi a costurilor implementării acesteia. Astfel, implementarea calitativă a prevederilor Strategiei, va spori gradul de protecţie şi securitate în spaţiul informaţional, iar cheltuielile aferente vor fi acoperite din mijloace financiare interne publice, private, precum şi externe.

Caracterul prezentei Strategii generează anumite riscuri de divulgare a unor date clasificate prin prisma estimării alocaţiilor financiare pentru realizarea anumitor obiective şi activităţi – cheie din Planul de acţiuni, fapt ce impune definitivarea în mod individual a sumelor necesare la nivelul autorităţilor şi includerea separată pentru fiecare an bugetar.

Capitolele VI - Rezultatele scontate și indicatorii de progres și VII - Proceduri de monitorizare și evaluare, descriu rezultatele scontate, indicatorii de progres, mecanismul de monitorizare şi evaluare a Strategiei. Implementarea prezentei Strategii va duce la identificarea abordărilor inovatoare ale formării unui sistem de protecţie şi dezvoltare a spaţiului informaţional în condiţiile globalizării şi liberei circulaţii a informaţiilor. Unul din elementele centrale ale Strategiei este crearea Consiliului coordonator pentru asigurarea securităţii informaţionale, organism colectiv, cu atribuţii consultative şi operaţionale, ce va fi responsabil şi va asigura integrarea sistemică a componentelor spaţiului informaţional şi susţinerea orientată a unui nivel înalt de securitate informaţională.

Procesul de implementare a Strategiei va fi însoţit de monitorizarea permanentă a realizării acţiunilor propuse şi a rezultatelor obţinute, cu operarea în caz de necesitate, a modificărilor de rigoare în politicile publice promovate de către Cancelaria de Stat, în contextul acestei Strategii.

Autorii proiectului propun ca responsabil de procesul de monitorizare şi implementare a Planului de acţiuni la Strategia Securităţii Informaţionale a Republicii Moldova pentru anii 2019-2024, să fi desemnată Cancelaria de Stat.

Cu referire la Planul de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024.

Planul de acţiuni este divizat pe piloane şi obiective, conform enunţării acestora în textul Strategiei. Concomitent, în scopul realizării fiecărui obiectiv sunt prevăzute acţiuni şi măsuri concrete, fiind determinate instituţiile responsabile şi partenerii. De asemenea, fiecare acţiune are stabilită termene concrete de realizare.

În concluzie, reieşind din cele descrise, adoptarea prezentei Strategii este determinată de necesitatea protecţiei intereselor persoanelor, societăţii, statului în spaţiul informaţional, de gravitatea şi multitudinea ameninţărilor la adresa securităţii informaţionale în societatea modernă, de necesitatea menţinerii unui echilibru între interesele persoanelor, societăţii şi statului pentru asigurarea securităţii informaţionale. Totodată, natura globală a sistemelor informaţionale şi a reţelelor de comunicaţii electronice necesită o coordonare strânsă între toate instituţiile responsabile atât la nivelul naţional, cît şi la nivel global, fapt pentru care solicităm respectuos susţinerea proiectului respectiv.

II. Modul de încorporare a proiectului în sistemul actelor normative în vigoare

Proiectul se integrează în sistemul legislaţiei şi este corelat cu prevederile actelor legislative în vigoare, cu care se află în conexiune, iar modificările şi completările propuse nu afectează concepţia generală.

III. Fundamentarea economică-financiară

Acţiunile propuse spre realizare vor fi acoperite din contul bugetului instituţiilor, în limitele alocaţiilor aprobate precum şi din asistenţa externă la acest capitol. Costurile estimative ale acţiunilor vor fi ajustate pe perioada implementării Planului, ţinând cont de volumele alocaţiilor disponibile în bugetul de stat.

Autorii proiectului au stabilit că, în scopul asigurării protecţiei datelor din perspectiva elaborării de acte normative, politici şi planificării de acţiuni, inclusiv şi a alocaţiilor financiare, autorităţile/instituţiile vor evalua şi decide în mod individual reflectarea datelor, care pot fi calificate ca informaţii atribuite la secret de stat.

IV. Avizarea și consultarea publică

În scopul respectării prevederilor Legii nr. 239 din 13.11.2008 privind transparenţa în procesul decizional, proiectul Hotărârii a fost plasat pe pagina web a Serviciului la adresa www.sis.md, în directoriul „Transparenţa", compartimentul „Transparenţa decizională".

V. Constatările expertizei anticorupție

În temeiul art. 28 alin. (2) lit. a) din Legea integrităţii nr. 82 din 25.05.2017, entităţile publice cu drept de iniţiativă legislativă, alte entităţi publice care elaborează şi promovează proiecte de acte legislative şi normative, precum şi Secretariatul Parlamentului, în cazul iniţiativelor legislative ale deputaţilor, au obligaţia de a supune expertizei anticorupţie proiectele de acte, cu excepţia - documentelor de politici.

În acest context, proiectul Strategiei şi a Planului, nu urmează a fi supus expertizei anticorupţie.

VI. Constatările expertizei de compatibilitate

Reieșind din faptul că proiectul actului, nu are drept scop armonizarea legislației naționale cu legislația Uniunii Europene precum și nu contravine legislației UE, expertiza de compatibilitate nu se efectuează.

VII. Constatările expertizei juridice

Proiectul Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia, a fost supus expertizei juridice, fiind înaintate recomandări luate în calcul de către autori.

VIII. Constatările altor expertize

Proiectul Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia, nu a fost supus altor expertize. Or, reieșind din obiectul de reglementarea, acesta nu se referă la reglementarea activității de întreprinzător sau alte activități economice pentru a fi necesar prezentarea unor concluzii de specialitate suplimentare.

Vasile BOTNARI
Director
VBotnari