



Republica Moldova

PARLAMENTUL

HOTĂRÎRE Nr. 257
din 22-11-2018

**privind aprobarea Strategiei securității informaționale
a Republicii Moldova pentru anii 2019–2024 și
a Planului de acțiuni pentru implementarea acesteia**

Publicat : 18-01-2019 în Monitorul Oficial Nr. 13-21 art. 80

Parlamentul adoptă prezenta hotărîre.

Art. 1. – Se aprobă:

– Strategia securității informaționale a Republicii Moldova pentru anii 2019–2024, prevăzută în anexa nr. 1;

– Planul de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024, prevăzut în anexa nr. 2.

Art. 2. – Începînd cu anul 2020, ministerele, instituțiile și alte autorități administrative centrale vor prezenta anual, pînă în data de 1 martie, la Serviciul de Informații și Securitate informația privind realizarea Planului de acțiuni menționat la art. 1, conform competențelor stabilite.

Art. 3. – Anual, pînă în data de 31 martie, Serviciul de Informații și Securitate va prezenta Parlamentului un raport privind implementarea Strategiei și realizarea Planului de acțiuni menționate la art. 1 și îl va publica pe pagina sa web oficială.

Art. 4. – Monitorizarea și evaluarea implementării Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 se vor realiza prin intermediul instrumentelor prevăzute de către aceasta.

PREȘEDINTELE PARLAMENTULUI

Andrian CANDU

Nr. 257. Chișinău, 22 noiembrie 2018.

STRATEGIA SECURITĂȚII INFORMAȚIONALE A REPUBLICII MOLDOVA PENTRU ANII 2019–2024

I. INTRODUCERE

1. Tehnologiile informaționale, resursele de informare și sistemele de comunicare electronică au devenit parte indispensabilă a tuturor domeniilor de activitate ale persoanei, societății și statului. Prin dezvoltarea lor accelerată, tehnologiile informaționale contribuie la transformări sociale de esență, fiind un generator pentru apariția și consolidarea societății informaționale de nivel național, regional și internațional, depășind cadrul juridic al frontierelor de stat sau al comunităților de state.

2. Spațiul informațional a devenit un domeniu de activitate vital pentru stat, economie, știință, societate și individ, un spațiu nou de reglementare a drepturilor și libertăților fundamentale ale omului, cu implicare directă și indirectă asupra mecanismelor de asigurare a politicilor de securitate și apărare națională într-o societate democratică.

3. Pe parcursul ultimului deceniu, Republica Moldova a realizat mai multe strategii, programe și politici de țară pentru dezvoltarea societății informaționale la nivel național, în conformitate cu recomandările forurilor europene și internaționale din domeniul tehnologiilor informaționale și comunicațiilor electronice, al drepturilor și libertăților fundamentale ale omului în mediile on-line și off-line.

4. Potrivit raportului anual cu privire la monitorizarea evoluției societății informaționale la nivel mondial „Measuring the Information Society 2017”, lansat de către Uniunea Internațională a Telecomunicațiilor, Republica Moldova este plasată pe locul al 59-lea din cele 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 mondial¹. Sînt implementate ori sîntîn proces continuu de dezvoltare peste 21 de programe² și proiecte on-line de infrastructură și servicii publice digitale, sînt lansate strategii sectoriale în domeniul tehnologiei informației și politici de modernizare tehnologică a guvernării.

5. Interacțiunea tehnologiilor informaționale cu diversitatea conținutului informațional, pe de o parte, și fuziunea rețelelor de comunicare publică și socială cu sistemele electronice guvernamentale, pe de altă parte, contribuie la o extindere și sinergie a spațiului informațional cu domeniile centrale de securitate și apărare națională, responsabile de asigurarea suveranității, independenței și integrității teritoriale a Republicii Moldova.

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

¹ www.mei.gov.md/ro/content/republica-moldova-urcat-4-pozitii-raportul-mondial-privind-evolutia-societatii

² Potrivit pct.2.3.1 secț. 2.3 cap. II din Strategia națională de dezvoltare a societății informaționale „Moldova digitală 2020”, aprobată prin Hotărîrea de Guvern nr. 857/2013.

7. Tendințele de dezvoltare continuă a interacțiunii dintre dimensiunea tehnologică și dimensiunea de informare în toate formele de structură și funcționare, de natură individuală, publică, privată sau de stat, de factură națională sau globală, conduc la apariția unei noi configurații de comunicare și schimb de date pe domeniile publice și private de care depind nivelul și starea sectorială sau generală de securitate.

8. Pe lângă beneficiile incontestabile ale tehnologiei moderne, spațiul informațional este supus unui șir de vulnerabilități, riscuri și amenințări de securitate, facilitând competiția injustă, confruntarea și spionajul, dezinformarea și propaganda, terorismul și criminalitatea, iar încălcările de confidențialitate determină răspîndirea de noi forme de ură și incitare la violență, în special pe criteriile de gen, rasă, naționalitate, origine etnică, limbă, religie, apartenență politică sau pe orice alte criterii, care rămîn subestimate și rareori remediate sau contracarate.

9. Propagarea informației fără a ține seama de limitele frontierelor naționale, pe lângă efectele evident benefice, poate conduce la sporirea capacității de influență din partea actorilor străini guvernamentali sau neguvernamentali cu resurse suficiente.

10. Crimele cibernetice, spionajul, propaganda, diversiunea și exploatarea excesivă a datelor cu caracter personal prin rețelele de comunicații electronice sînt utilizate ca instrumente de bază la toate etapele de concepere a unei amenințări hibride de securitate și cheamă la un răspuns colectiv și reglementat, bazat pe mecanisme și acțiuni coordonate, de implementare a politicilor din domeniu, asistență tehnică și legală din perspectiva imperativelor de securitate, orientat spre crearea unui mediu informațional favorabil și sigur pentru cetățean, pentru mediul de afaceri de orice nivel și pentru stat.

11. Campaniile de dezinformare sînt orientate spre accentuarea neîncrederii, a confuziei și a destabilizării situației sociopolitice a statului, spre influențarea percepțiilor și a preferințelor existente în diferite comunități sociale. Acest fapt poate duce la controlul, de către diverși actori, al comportamentului unei părți a societății, precum și la influențarea politicilor interne și externe ale statului.

12. Creșterea numărului de utilizatori ai Internetului și evoluțiile tehnologiilor informaționale conexe creează provocări substanțiale în ceea ce privește starea mediului de securitate, ordinea publică și apărarea, prevenirea criminalității și aplicarea legii în direcția protecției drepturilor în spațiul informațional.

13. Concepția securității informaționale a Republicii Moldova (în continuare – *Concepție*), aprobată prin Legea nr. 299/2017, reprezintă documentul de bază pentru elaborarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 (în continuare – *Strategie*) și documentul de politici ce integrează domeniile centrale și asociate spațiului informațional, ce oferă noțiuni, definește principiile de organizare la nivel de stat, societate și persoană, precum și detaliază metodele juridice, tehnico-organizatorice, economice și contrainformative pentru asigurarea securității informaționale a Republicii Moldova.

14. Scopul prezentei Strategii este de a corela juridic și de a integra sistemic domeniile prioritare cu responsabilități și competențe de asigurare a securității informaționale la nivel național, fiind bazat pe reziliența cibernetică, pluralismul multimedia și convergența instituțională în materie de securitate, destinate protejării suveranității, independenței și integrității teritoriale a Republicii Moldova.

15. Prezenta Strategie descrie situația curentă în domeniul securității informaționale din perspectiva progreselor înregistrate și a tendințelor de dezvoltare a societății informaționale la nivel național, a problemelor existente și de perspectivă, care generează și creează riscuri și amenințări de securitate, inclusiv hibride. Complexul de acțiuni, conform scopului și obiectivelor specificate, este compartimentat pe patru piloni:

- 1) Pilonul I. Asigurarea securității spațiului informațional-cibernetice și investigarea criminalității informatice;
- 2) Pilonul II. Asigurarea securității spațiului informațional-mediatic;
- 3) Pilonul III. Consolidarea capacităților operaționale;
- 4) Pilonul IV. Eficientizarea proceselor de coordonare internă și de cooperare internațională în domeniul securității informaționale.

16. Scopul și obiectivele prezentei Strategii se vor realiza în baza Planului de acțiuni pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024.

II. DESCRIEREA SITUAȚIEI

17. Republica Moldova, ca 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 parte³, 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, pentru e-learning și cercetare, pentru servicii publice de asistență medicală, pentru digitalizarea patrimoniului cultural, pentru dezvoltarea conținutului digital și a comerțului electronic, precum și pentru „îmbunătățirea nivelului de securitate a datelor cu caracter personal și protejarea 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 gestionare 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 a 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 în fața 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, să influențeze procesele decizionale. În aceste condiții, asigurarea

³Art. 98 cap. 18 „Societatea Informațională” din Acordul 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.

securității informaționale este esențială pentru a întări discernământul social, atașamentul social și interesul social. Asigurarea securității informaționale este necesară și pentru contracararea supracomunicării și a abuzului informațional, care duc la noncomunicare și pseudocomunicare, elemente ce generează rupturi sociale și dezechilibre în societate.

21. Interacțiunea în spațiul cibernetic este facilitată de diverși actori: persoane fizice și juridice, autorități de stat și structuri neguvernamentale, grupuri formale și informale, utilizatori personalizați și anonimi. Unii îi conectează pe utilizatori, permit prelucrarea informațiilor, găzduiesc servicii web, inclusiv conținutul generat de utilizatori, alții cumulează informații și permit căutări, oferind acces la conținut, gazdă, indicatori și servicii create sau operate de către persoane terțe. O altă categorie de actori ai spațiului cibernetic facilitează vânzarea de bunuri și servicii, inclusiv servicii audiovizuale, de asemenea permit alte tranzacții comerciale, de publicitate și plăți.

22. Protecția drepturilor și libertăților persoanelor fizice în ceea ce privește prelucrarea datelor lor cu caracter personal necesită adoptarea de măsuri tehnice și organizatorice corespunzătoare. În acest sens, operatorul de date cu caracter personal ar trebui să adopte politici interne și să pună în aplicare măsuri care să respecte, în special, principiul protecției datelor, începând din momentul conceperii acestora, și pe cel al protecției implicite a datelor, în corespundere cu legislația privind protecția datelor cu caracter personal.

23. Actorii spațiului cibernetic pot modera și pot plasa conținutul, inclusiv prin prelucrarea automată a datelor cu caracter personal, pot exercita alte forme de control care influențează accesul utilizatorilor la informații on-line în moduri similare cu mass-media sau pot îndeplini funcții asemănătoare celor editoriale. Serviciile de informare on-line sînt oferite și de mass-media tradițională prin intermediul platformelor electronice create în acest sens.

24. Dată fiind importanța promovării sectorului TIC pentru dezvoltarea unei societăți informaționale avansate în Republica Moldova, pentru crearea și dezvoltarea unei infrastructuri infocomunicaționale integrate și eficiente, orientate spre creșterea competitivității economiei naționale și asigurarea accesului tuturor cetățenilor la serviciile societății informaționale, au fost ajustate, completate și chiar elaborate acte normative ce reglementează totuși insuficient raporturile subiecților și entităților din spațiul informațional.

25. Principalele documente de politici care au stat la baza elaborării prezentei Strategii, valabile pînă în anul 2020 și tangențiale dimensiunii securității informaționale, care urmează să transpună la nivel național modelul european de dezvoltare a societății informaționale, sînt Strategia națională de dezvoltare a societății informaționale „Moldova Digitală 2020”, aprobată prin Hotărîrea de Guvern nr. 857/2013, și Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016–2020, aprobat prin Hotărîrea de Guvern nr. 811/2015.

26. Potrivit Planului de acțiuni privind implementarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016–2020, în perioada de referință sînt prevăzute să fie realizate 50 de acțiuni. Acțiunile din Planul menționat sînt repartizate pe următoarele domenii de intervenție:

- 1) procesarea, stocarea și accesarea în siguranță a datelor, inclusiv a celor de interes public;
- 2) securitatea și integritatea rețelelor și a serviciilor de comunicații electronice;
- 3) dezvoltarea capacităților de prevenire și de reacție urgentă la nivel național (crearea rețelei CERT naționale);

- 4) prevenirea și combaterea criminalității informatice;
- 5) consolidarea capacităților de apărare cibernetică;
- 6) educația, formarea și informarea continuă în domeniul securității cibernetice;
- 7) cooperarea și interacțiunea internațională în domeniile ce țin de securitatea cibernetică.

27. Concomitent, la pct. 26 din Programul național 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 și abordarea unor segmente ale securității informaționale neelucidate anterior.

28. Subsecvent, constatăm că, în prezent, legislația în materie nu reglementează prevenirea și combaterea tentativelor de dezinformare și/sau de informare manipulatorie, protecția vieții private și a datelor cu caracter personal la plasarea informației pe Internet din considerentul că acțiunea acestor legi este restrânsă și/sau scopul reglementării este diferit.

29. În aceste condiții, Legea nr. 299/2017 privind aprobarea Concepției securității informaționale a Republicii Moldova poate fi considerată un punct de pornire pentru consolidarea protejării intereselor persoanelor, ale societății și ale statului în domeniul informațional, pentru prevenirea și contracararea amenințărilor complexe și persistente la adresa securității informaționale, a obiectivelor vitale și de importanță strategică pentru securitatea națională, pentru asigurarea protecției informației atribuite la secret de stat, pentru prevenirea și combaterea criminalității informatice.

30. Analiza evoluției fenomenului rețelelor de socializare on-line și a presei electronice pune în evidență reglementarea insuficientă a componentei de protecție a spațiului mediatic față de amenințările cu caracter hibrid și a componentei de securitate. În acest context, este confirmată importanța și necesitatea unei strategii care să cuprindă reglementări comprehensive ale tuturor vectorilor securității informaționale.

31. Procesul de implementare a tehnologiilor informaționale în toate domeniile vieții (economic, social etc.) în Republica Moldova a determinat și evoluția criminalității informatice. Ca urmare, în ultimii ani s-a constatat 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 fie 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. Acest mediu oferă un repertoriu vast de tehnici și strategii de săvîrșire a infracțiunilor, generînd tendințe noi în domeniul infracționalității.

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 o dotare corespunzătoare a organelor de ocrotire a normelor 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 și ale statului în spațiul informațional, de gravitatea și multitudinea amenințărilor la adresa securității informaționale în societatea modernă, de necesitatea menținerii unui echilibru între interesele persoanelor, ale societății și ale statului pentru asigurarea securității informaționale. Totodată, natura globală a sistemelor informaționale și a rețelelor de comunicații electronice necesită o coordonare strânsă între toate instituțiile responsabile atât la nivelul național, cât 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 sînt niște probleme de 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. Amenințările și riscurile, atacurile și incidentele cibernetice, precum și alte evenimente survenite în spațiul cibernetic se materializează prin exploatarea vulnerabilităților de natură umană, tehnică și procedurală. Pe aceste căi, în ultimii ani în Republica Moldova s-au constatat creșteri ale indicatorilor privind numărul de infracțiuni și contravenții informatice, numărul de atacuri cibernetice asupra resurselor informaționale publicate în rețeaua globală Internet, vulnerabilitățile aplicațiilor fiind exploatate în scopuri de sustragere/modificare/ștergere a informației.

37. Pînă în prezent, la nivel național nu au fost efectuate procese de audit complexe de securitate cibernetică, nici nu există studii sau rapoarte⁴ care ar reflecta în detaliu situația privind criminalitatea informatică (riscurile și amenințările cibernetice, atacurile și incidentele cibernetice, alte evenimente survenite în spațiul cibernetic), precum și numărul victimelor și valoarea prejudiciilor economice ale acestora.

38. Una dintre problemele de bază este lipsa unei entități de tip CERT (Centru de reacție la incidente de securitate cibernetică), la nivel național, responsabile de prevenirea și reacția la incidente din domeniul securității cibernetice.

39. O altă problemă majoră este lipsa unui sistem integrat de management al securității cibernetice în cadrul căruia să se efectueze coordonat planificarea și utilizarea resurselor disponibile, identificarea vulnerabilităților și a riscurilor în urma auditului de securitate cibernetică, precum și a intervențiilor necesare pentru diminuarea impactului dăunător al

⁴Singurele surse oficiale de date statistice privind criminalitatea informatică sînt Registrul de evidență a infracțiunilor, a cauzelor penale, a persoanelor care au săvîrșit infracțiuni și a materialelor cu privire la infracțiuni, deținut de Ministerul Afacerilor Interne și Sistemul informațional automatizat „Urmărirea penală: E-dosar”, gestionat de Procuratura Generală.

criminalității, al atacurilor și al incidentelor cibernetice asupra dezvoltării sigure a societății informaționale.

40. Lipsa unui sistem integrat de management al securității cibernetice la nivel național generează și lipsa unor date complete, veritabile, actualizate și structurate, ceea ce, la rândul său, creează obstacole în identificarea de soluții optime. De soluționarea acestei probleme depinde eficiența măsurilor ce urmează a fi întreprinse pentru dezvoltarea unei societăți informaționale securizate în Republica Moldova, pentru avansarea tehnologică și științifică, precum și dinamica de creștere economică a țării.

41. Asigurarea prevenirii riscurilor și combaterii amenințărilor la adresa securității informaționale este una dintre sarcinile de bază ale statului, implementate prin instituțiile sale de drept, la acest capitol fiind determinate următoarele probleme care necesită a fi soluționate la nivel național:

1) insuficiența de specialiști calificați în domeniul tehnologiilor informaționale și nivelul redus de salarizare, în special în sectorul public;

2) lipsa unor programe de instruire specializate adresate angajaților cu atribuții de investigare și urmărire penală, procurorilor, judecătorilor, specialiștilor și experților judiciari în domeniu din cadrul structurilor de aplicare a legii, precum și a celor adresate personalului tehnic din cadrul instituțiilor publice în domeniul securității cibernetice;

3) dotarea insuficientă cu echipament și softuri specializate pentru investigarea infracțiunilor informatice;

4) finanțarea redusă pentru participarea specialiștilor la proiectele și evenimentele internaționale de consolidare a capacităților și schimbului de bune practici.

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

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

2) utilizarea algoritmilor complexe asimetrici de criptare a informației critice la estorcare mijloacelor financiare prin intermediul tehnologiilor informaționale;

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

4) rețelele de schimb direct de date dintre utilizatori, ceea ce nu lasă anumite urme ale activității în conținutul istoricului înregistrat în sistemul informatic sau în logurile deținute de furnizorii de servicii;

5) utilizarea web hostingului de către infractori;

6) furnizorii mici de servicii nu asigură un nivel minim de securitate cibernetică a propriei rețele și deseori nu duc evidența utilizatorilor de servicii, nici nu înregistrează metadatele privind accesul la rețeaua Internet;

7) serviciile de Internet fix prestate pe teritoriul Republicii Moldova care nu este controlat efectiv de către autoritățile constituționale.

43. Consolidarea sistemelor informaționale și de comunicații electronice speciale într-un mecanism unic de funcționare sigură și corectă nu poate fi efectuată fără existența unui cadru normativ actualizat care ar prevedea promovarea dezvoltării acestor sisteme. În momentul de față, cadrul normativ instituie unele prevederi ce produc impedimente în funcționarea normală a sistemelor informaționale și de comunicații electronice speciale, inclusiv a celor guvernamentale,

ca sisteme informaționale vitale pentru securitatea statului, prin introducerea unor constrângeri în gestionarea, dezvoltarea și asigurarea securității acestora.

44. Resursele disponibile ale instituțiilor de stat sînt insuficiente pentru pregătirea și instruirea unor specialiști calificați, precum și pentru stimularea acestora, fapt care determină migrarea specialiștilor în sectorul privat, cu repercusiuni asupra modului de implementare a securității cibernetice.

45. Totodată, sistemul de apărare națională, la fel ca și alte domenii, a devenit dependent de TIC. Unele componente TIC ale sistemului de apărare națională sînt integrate cu rețeaua globală Internet, iar rețelele informaționale de apărare sînt construite pe tehnologii comerciale standard. Prin urmare, acestea sînt, de asemenea, expuse unor riscuri de atacuri cibernetice prin exploatarea unor vulnerabilități.

46. La etapa actuală a progresului tehnologic și a procesului de informatizare a vieții economice, politice, sociale etc., funcționarea mecanismelor principale ale statului se realizează prin utilizarea produselor program și schimbul de date digitalizate, care formează în ansamblu infrastructura critică informatică. În acest context este relevantă elaborarea și/sau evaluarea legislației deja existente prin prisma prevederilor Directivei 2008/114/CE privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției 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 spațiului mediatic

47. Asigurarea securității informaționale a statului constituie o prioritate pentru securitatea națională, fiind un obiectiv statuat în mai multe acte normative ale Republicii Moldova și necesitînd o finanțare suficientă.

48. Conform prevederilor pct. 4.7 din Strategia securității naționale a Republicii Moldova, aprobată prin Hotărîrea Parlamentului nr.153/2011, securitatea informațională a statului ține și de provocările cu caracter mediatic îndreptate împotriva Republicii Moldova sub formă de dezinformare și/sau de informare manipulatorie din exterior.

49. Pe parcursul afirmării, consolidării și dezvoltării sale ca stat, Republica Moldova a fost supusă în repetate rînduri unor campanii de denigrare informațională, în special de influență externă, cu un impact negativ sporit asupra populației.

50. Intensificarea propagandei și a dezinformărilor are loc în special în timpul unor evenimente de interes național, în scopul influențării deciziei politice atît a statului, cît și a cetățeanului. În funcție de anumite evoluții interne/externe, se mizează pe crearea unei stări de nemulțumire socială.

51. Necesitatea stringentă de a proteja securitatea spațiului informațional național este conștientizată și la nivelul autorităților administrației publice, dar și reprezintă un deziderat al societății civile.

52. Îngrijorarea privind intensificarea atacurilor din exterior la adresa securității informaționale a fost enunțată inclusiv în Declarația Parlamentului Republicii Moldova privind condamnarea atacurilor provenite din Federația Rusă asupra securității informaționale naționale

și amestecul abuziv în activitatea politică din Republica Moldova, aprobată prin Hotărârea Parlamentului nr. 12/2018, care stipulează că atacurile media din exterior vizează denigrarea Republicii Moldova, a unor instituții și a unor oficiali, dar cel mai grav este că vizează denigrarea cetățenilor țării.

53. Astfel, Parlamentul constată că „propaganda s-a transformat într-un veritabil instrument de denigrare a Republicii Moldova, fapt menționat în nenumărate rapoarte prezentate public de către societatea civilă și organizațiile internaționale independente, în special în ultimul an, care au arătat evoluția tot mai îngrijorătoare a acestui fenomen”.

54. Concomitent, subiectul este unul de actualitate atât la nivel internațional, cât și regional. În acest sens, prin Rezoluția sa din 23 noiembrie 2016 referitoare la comunicarea strategică a Uniunii Europene pentru a contracara propaganda părților terțe împotriva sa (2016/2030 (INI)), Parlamentul European statuează că „UE, statele sale membre și cetățenii săi suportă o presiune crescândă și sistematică pentru a face față campaniilor de informare, de dezinformare, de intoxicare și de propagandă din partea unor țări și entități/subiecți nestatali, cum ar fi organizații teroriste și criminale transnaționale din vecinătatea sa, care intenționează să submineze însăși noțiunea de informare obiectivă sau de jurnalism etic, difuzând toate informațiile sub o formă părtinitoare sau ca instrument de putere politică și care atacă, de asemenea, valori și interese democratice”.

55. Tehnologiile războiului informațional sînt folosite pentru a legitima acțiuni care subminează suveranitatea, independența și integritatea teritorială, context în care statele membre ale UE și partenerii acestora sînt încurajați 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 înșelăciune sau de dezinformare intenționată, în special în noile mijloace de informare, în rețelele sociale și în sfera digitală”.

56. La etapa actuală, propaganda, dezinformarea și/sau informarea manipulatorie sînt extrem de dinamice, iar resursele alocate în acest scop de către terți depășesc cu mult capacitățile de răspuns și de combatere a fenomenului respectiv ale Republicii Moldova.

57. Pentru a face față provocărilor, Republica Moldova beneficiază de suportul Uniunii Europene care, pentru următorii ani, și-a majorat bugetul pentru combaterea propagandei și a dezinformării, un accent separat fiind pus și pe statele membre ale Parteneriatului Estic.

58. Conștientizarea riscurilor generate de impactul propagandei externe impune măsuri de armonizare a politicilor naționale, iar adoptarea prezentei Strategii vine în susținerea acestui deziderat.

3.3. Componenta contrainformativă și de securitate

59. Arma informațională, în calitatea ei de componentă esențială a amenințărilor hibride, este utilizată de către centre externe subversive (servicii speciale, ONG-uri ghidate de actori statali și nonstatali, instituții media controlabile etc.) în punerea pe rol a unor operațiuni informaționale sau atacuri cibernetice subsumate unui anumit scop strategic.

60. Potrivit Rezoluției Parlamentului European din 23 noiembrie 2016 referitoare la comunicarea strategică a Uniunii Europene pentru a contracara propaganda părților terțe împotriva sa (2016/2030 (INI)), „serviciile de securitate și de informații au concluzionat că anumiți actori nestatali au capacitatea și intenția de a desfășura operațiuni vizînd destabilizarea

statelor, subliniind că acest lucru ia adesea forma unui sprijin acordat extremiștilor politici și a unor campanii de mass-media și de dezinformare pe scară largă”. Este de accentuat că astfel de societăți media sînt prezente și active și în Republica Moldova.

61. Analiza mediului de securitate intern și regional relevă extinderea la scară largă a propagandei din partea unor subiecți/entități, de asemenea utilizarea mijloacelor de imixiune în treburile interne ale Republicii Moldova prin propagandă și agresiune mediatică, precum și influența informațional-psihologică cu scopul de a destabiliza situația social-politică, a submina suveranitatea și integritatea teritorială a Republicii Moldova.

62. În aceste activități de natură informativ-propagandistică pe segmentul spațiului mediatic sînt implicate structuri asociative, centre informativ-analitice, agenții de presă, precum și grupuri separate de cetățeni finanțați de către centre subversive și servicii speciale ale țărilor străine, care prin tehnologii informaționale utilizează instrumente hibride de putere subtilă (soft power).

63. Periculozitatea acestor tipuri de amenințări este una foarte ridicată din cauza tacticilor, acțiunilor și a mijloacelor diverse folosite pentru atingerea obiectivelor lor. Astfel, se poate vorbi de amenințări specifice în materie de securitate, cunoașterea cărora va permite luarea unor măsuri eficiente de prevenire și/sau de limitare a efectelor nedorite.

64. Pe alt palier, organizațiile teroriste islamiste desfășoară campanii active de informare în scopul subminării și al creșterii nivelului de ură împotriva valorilor și intereselor europene. Este de remarcat utilizarea răspîndită de către aceste organizații a instrumentelor de comunicare socială, 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, socioeconomice, de dezvoltare și de prevenire a conflictelor.

3.4. Definirea problemelor de natură legală

66. Unii actori statali și nonstatali exploatează lipsa unui cadru juridic internațional în domeniul precum securitatea cibernetică, lipsa de responsabilitate în ceea ce privește reglementarea mass-mediei digitale și profită de pe urma oricărei ambiguități în aceste chestiuni.

67. Pe palierul de securitate cibernetică, Republica Moldova a ratificat Convenția Consiliului Europei privind criminalitatea informatică prin Legea nr.6/2009. Totodată, a fost adoptată Legea nr. 20/2009 privind prevenirea și combaterea criminalității informatice și au fost operate modificări la Codul penal al Republicii Moldova nr. 985/2002 în corespundere cu prevederile Convenției ratificate. Cu toate acestea, nu au fost implementate integral multiple prevederi de ordin material și procesual, inclusiv cele ce țin de dezvoltarea punctului de contact al rețelei 24/7.

68. Complementar, este de remarcat că, pînă în prezent, nu există un cadru legal privind delimitarea și armonizarea competențelor și responsabilităților instituțiilor statului și ale celor private în domeniul securității cibernetică, nu se aplică mecanismul obligatoriu de audit al securității cibernetică în cadrul instituțiilor publice și private, prin care pot fi identificate

vulnerabilitățile, riscurile și amenințările cibernetice în scopul prevenirii sau diminuării, prin măsuri speciale, a impactului atacurilor, incidentelor și a altor evenimente survenite în spațiul cibernetic, a căror origine este dificil de stabilit.

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

1) în Codul penal al Republicii Moldova nr. 985/2002, și anume:

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

b) articolul 208¹ din cod, „Pornografia infantilă”, nu incriminează obținerea accesului cu bună știință, prin intermediul tehnologiilor informaționale și a comunicațiilor, la pornografia infantilă, deși acest lucru este prevăzut în Convenția Consiliului European pentru protecția copiilor împotriva exploatării sexuale și a abuzurilor sexuale, încheiată la Lanzarote la 25 octombrie 2007 și ratificată prin Legea nr. 263/2011;

c) majoritatea infracțiunilor prevăzute la capitolul XI din partea specială a codului, „Infracțiuni informatice și infracțiuni în domeniul telecomunicațiilor”, au componentă materială și se consumă doar la provocarea unui prejudiciu în proporții mari;

2) în Codul de procedură penală al Republicii Moldova nr. 122/2003, și anume:

a) nu este reglementată procedura „Percheziției informatice”, prevăzută în Convenția Consiliului European privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001;

b) lipsește măsura specială de investigații de interceptare a datelor informatice;

c) cadrul legal nu permite efectuarea măsurilor speciale de investigații necesare la documentarea infracțiunilor informatice;

d) nu este prevăzută restricționarea accesului la paginile web, inclusiv cele găzduite de furnizorul respectiv, ce conțin informații care periclitează viața, sănătatea și dezvoltarea normală a copiilor, informații ce fac propagandă războiului sau terorismului, îndeamnă la ură sau discriminare națională, rasială ori religioasă, la ostilitate sau violență.

70. De asemenea, se constată lipsa unui cadru normativ care ar reglementa infrastructura critică națională, precum și lipsa unei clasificări clare a sistemelor informaționale în funcție de tipul datelor pe care acestea le conțin, de tipul de acces la acestea și de destinația acestora, lipsa unei definiții a incidentelor de securitate cibernetică, inclusiv evaluarea și estimarea prejudiciilor cauzate prin aceste incidente, precum și sancțiunile ce pot fi aplicate în context, precum și lipsa definiții acțiunilor ce pot cauza incidente de securitate cibernetică. Lipsește reglementarea normativă a mecanismului de schimb de informații cu privire la incidentele de securitate cibernetică dintre persoanele juridice, indiferent de tipul de proprietate al acestora, precum și dintre persoanele juridice și persoanele fizice.

3.5. Definierea problemelor de conștientizare a maselor

71. La acest capitol se evidențiază importanța sensibilizării publicului privind siguranța on-line, a educației și a competenței mediatică și cibernetice în Republica Moldova, care le-ar permite cetățenilor să analizeze în mod critic conținutul mediatic în vederea identificării propagandei.

72. Lipsa capacității de protecție contra fenomenului de defăimare prin intermediul platformelor on-line afectează exercitarea drepturilor omului și a libertăților fundamentale. În aceste condiții, ajustarea cadrului legal național la standardele europene pe dimensiunea respectării drepturilor omului în spațiul informațional constituie o prioritate incontestabilă pentru Republica Moldova.

73. În acest sens sînt necesare acțiuni de consolidare a cunoștințelor la toate nivelurile sistemului educațional, cât și impulsivarea/încurajarea persoanelor să devină cetățeni activi și să se conștientizeze în calitate lor de consumatori de mass-media.

74. Un alt element de conștientizat este rolul central al instrumentelor oferite de Internet (în special al rețelelor de socializare), spațiu în care răspîndirea de informații false și lansarea de campanii de dezinformare sînt ușor de realizat și adesea nu întîmpină niciun obstacol.

75. Problema știrilor false, pe parcursul anului 2017, a constituit obiectul ședințelor Comisiei Europene, care a decis crearea unui Grup de lucru la nivel înalt care să elaboreze și să prezinte strategie de combatere a știrilor false în 2018, cu un an înainte alegerilor europene. Evaluările sale relevă că „contracarea propagandei prin propagandă este contraproductivă”, statele membre UE fiind îndemnate să o combată doar prin demontarea campaniilor de dezinformare și prin utilizarea mesajelor și a informațiilor pozitive. În acest sens, experții recomandă „dezvoltarea unei strategii eficiente care să nu fie adaptată în funcție de natura actorilor care diseminează propaganda”⁵.

IV. VIZIUNE ȘI OBIECTIVE ALE STRATEGIEI

76. Guvernul, autoritățile administrațiilor publice, instituțiile și întreprinderile de stat, indiferent de forma de organizare, și societatea civilă au stabilit următoarea viziune strategică:

Republica Moldova va asigura un spațiu informațional sigur pentru toți subiecții de drept prin armonizarea cadrului legal și implementarea acestuia, astfel protejînd drepturile și libertățile fundamentale ale omului și promovînd democrația și statul de drept.

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

4.1. Pilonul I. Asigurarea securității spațiului informațional-cibernetice și investigarea criminalității informatice

78. Obiectivul nr. 1. Crearea unui sistem integrat de comunicare și evaluare a amenințărilor la adresa securității informaționale și de elaborare a măsurilor operative de răspuns

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

1) crearea/desemnarea entității care va exercita rolul de Centru național de reacție la incidente 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;

⁵Conform pct.46 din Rezoluția Parlamentului European din 23 noiembrie 2016 referitoare la comunicarea strategică a Uniunii Europene pentru a contracara propaganda părților terțe împotriva sa (2016/2030 (INI)).

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

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

4) elaborarea mecanismelor de creare și consolidare a centrelor departamentale de reacție la incidente de securitate cibernetică și informațională, atât de drept public, cât 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 ale UE;

6) determinarea politicii privind modalitatea de raportare, de stocare și de 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, a societății și a statului în spațiul cibernetic:

a) efectuarea auditului de securitate cibernetică a infrastructurilor de tehnologie a informației de interes național și a Sistemului de telecomunicații al autorităților administrației publice, precum și a altor infrastructuri cibernetică de interes național, în vederea identificării disfuncțiilor și vulnerabilităților; 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 a 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 începând de la conceperea acestora și protecția implicită a datelor atunci când 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 astfel de date 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 a responsabilităților privind apărarea cibernetică ce revin sistemului de organe ale securității statului și sistemului național de apărare;

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

3) elaborarea și implementarea măsurilor de protecție a sistemelor informaționale ce prelucrează informații atribuite la secret de stat și a componentei TIC din sistemele 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 în cauză 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 către autoritatea responsabilă cu privire la măsurile 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 normativ privind instituirea subdiviziunilor responsabile de protecția datelor cu caracter personal în cadrul persoanelor juridice de drept public și de drept 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 protecție tehnică și criptografică a informației;
- 2) dezvoltarea sistemelor de monitorizare a importului mijloacelor de protecție a informației;
- 3) alinierea cadrului normativ în domeniul protecției criptografice a informației la cadrul normativ european;
- 4) crearea unei baze de date privind mijloacele de protecție tehnică și criptografică a informației;
- 5) exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice.

83. *Obiectivul nr. 6. Combaterea criminalității informatice (investigarea infracțiunilor informatice)*

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

- 1) eficientizarea capacităților (mecanismului) de combatere a criminalității informatice;
- 2) acordarea ajutorului metodico-practic subdiviziunilor teritoriale privind investigarea infracțiunilor informatice;
- 3) implementarea de noi mecanisme la nivelul instituțiilor implicate în combaterea criminalității informatice (atragera companiilor private și a experților independenți, dezvoltarea laboratoarelor);
- 4) perfecționarea cadrului legal ce reglementează salarizarea efectivului specializat în combaterea criminalității informatice și investigarea infracțiunilor informatice.

84. Obiectivul nr. 7. Protecția copiilor față de orice formă de abuz în spațiul on-line

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

- 1) combaterea fenomenului de pornografie infantilă pe Internet;
- 2) combaterea fenomenelor de ademenire (grooming) și hărțuire sexuală a copiilor prin intermediul Internetului;
- 3) promovarea unui Internet mai sigur pentru copii prin intermediul consilierilor on-line și încurajarea raportărilor prin proiecte informaționale specializate.

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

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

- 1) schimbul de informații între Centrul pentru combaterea crimelor informatice din cadrul Ministerului Afacerilor Interne și departamentele de securitate ale instituțiilor financiare;
- 2) promovarea unor măsuri de securitate sporită în privința bancomatelor (ATM-urilor) la nivel de hardware și software;
- 3) identificarea mecanismelor comune de combatere a fraudelor în tranzacțiile cu card și fără card (card-present și card not-present).

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

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

- 1) dezvoltarea unor subdiviziuni specializate în cadrul Inspectoratului General de Poliție al Ministerului Afacerilor Interne, al Procuraturii Generale și al Serviciului de Informații și Securitate în scopul depistării și contracarării tentativelor infracționale în domeniu;
- 2) crearea unei baze de date naționale privind evoluția fenomenului criminalității 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 în efectuarea urmăririi penale și judecarea cauzelor, precum și implementarea, dezvoltarea și interconectarea acestuia.

87. Obiectivul nr.10. Efectuarea unor cercetări științifice aplicative în domeniul securității informaționale

Obiectivul în cauză 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 al instituțiilor de cercetare științifică.

88. Obiectivul nr. 11. Dezvoltarea capacităților de reziliență cibernetică și ridicarea nivelului de cultură în domeniul TIC

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

- 1) desfășurarea unor acțiuni de sensibilizare și informare a societății privind amenințările, vulnerabilitățile și riscurile la adresa securității cibernetică;
- 2) realizarea de către Centrul național de reacție la incidente de securitate cibernetică a analizei strategice privind incidentele de securitate cibernetică și coordonarea acțiunilor de

răspuns la astfel de incidente, inclusiv prin organizarea unor cursuri specializate de către experți calificați;

3) desfășurarea unor exerciții și antrenamente comune de consolidare a capacităților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate;

4) organizarea și desfășurarea atelierelor de lucru în domeniul securității cibernetice pentru personalul din sectorul public și privat deținători de elemente de infrastructură critică;

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

6) organizarea unor campanii de sensibilizare și informare privind pericolele din spațiul cibernetic și măsurile de protecție ce pot fi luate de către persoanele fizice și juridice;

7) introducerea și promovarea unor conținuturi curriculare privind securitatea informațională în programele naționale de studii;

8) organizarea, inclusiv împreună cu partenerii străini, a cursurilor de instruire tematică în domeniul securității cibernetice pentru angajații instituțiilor publice.

Prioritățile pilonului I	Indicatori de rezultat
1. Crearea Centrului național de reacție la incidente de securitate cibernetică (CERT național)	1. Centrul național creat, care elaborează documente de politici și asigură interacțiunea dintre toate componentele de asigurare a securității cibernetice
2. Desemnarea entității care va exercita rolul de Centru guvernamental de reacție la incidente de securitate cibernetică al Guvernului (CERT Gov)	2. Centrul guvernamental asigură funcționarea și protecția rețelelor speciale la nivel de Guvern și autorități publice
3. Consolidarea cooperării dintre CERT-ul național, CERT Gov și CERT-urile private	3. Acorduri de colaborare și sustenabilitate în scopul prevenirii și soluționării incidentelor de securitate cibernetică

4.2. Pilonul II. Asigurarea securității spațiului informațional-mediatic

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

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) evaluarea sectoarelor vulnerabile la componenta mediatică din cadrul sistemului de securitate informațională;

2) dezvoltarea unor politici 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;

3) crearea, în Republica Moldova, a resursei/platformei informaționale de comunicare strategică care va conține informații privind:

a) incidentele de securitate informațională;

b) ghidurile de comunicare strategică pe subiecte de interes național;

c) tentativele și acțiunile de dezinformare și/sau de informare manipulatorii ce afectează securitatea informațională și starea generală de securitate.

90. Obiectivul nr. 2. Controlul civic și consolidarea cooperării societății civile cu autoritățile publice cu atribuții de asigurare a securității informaționale

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

- 1) crearea unui mecanism de implicare a experților din rîndul societății civile, a organizațiilor neguvernamentale și a 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, a organizațiilor neguvernamentale și a mass-mediei din perspectiva implicării în materie de asigurare a securității informaționale și naționale – Consiliul societății civile;
 - b) certificarea de către Consiliul societății civile a experților și a reprezentanților societății civile și ai mass-mediei ce se vor preocupa de monitorizarea nivelului de asigurare a securității informaționale la nivel național;
- 2) implicarea reprezentanților societății civile certificați de către Consiliul societății civile în activitatea Consiliului coordonator pentru asigurarea securității informaționale;
- 3) îmbunătățirea sau crearea mecanismelor de implicare a societății civile în procesele de definire, de elaborare, de monitorizare și de evaluare a politicilor de asigurare a securității informaționale realizate de către autoritățile abilitate în asigurarea securității informaționale;
- 4) elaborarea și organizarea unor cursuri de instruire tematică pentru radiodifuzori, distribuitorii de servicii, formatorii de opinie publică, jurnaliști și ONG-urile de profil cu privire la tehnicile de dezinformare și/sau de informare manipulatorie utilizate pentru prejudicierea securității informaționale a statului.

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

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

- 1) evaluarea spațiului Internet din perspectiva identificării entităților/subiecților implicați în producerea și diseminarea conținutului media on-line și a altor intermediari și serviciilor auxiliare ce au impact pentru securitatea informațională;
- 2) elaborarea și ajustarea cadrului legal funcțional în scopul reglementării juridice a raporturilor dintre reprezentanții mass-media care colectează și difuzează informații în Internet, societate și autoritățile cu atribuții de asigurare a securității informaționale, în conformitate cu recomandările Comisiei Europene și bunele practici europene;
- 3) implementarea cadrului normativ care prevede acțiuni comune de intervenție și de gestionare a spațiului media on-line și off-line.

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

Obiectivul menționat 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, de manipulare sau de propagandă, orientat spre subminarea securității informaționale, în scopul identificării comanditarilor, a surselor de finanțare și a executorilor;
- 2) ajustarea cadrului legal în vederea eficientizării colectării de date pentru identificarea provenienței mijloacelor financiare și a 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 a 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 de control civic în scopul asigurării securității informaționale	1. Mecanism de interacțiune și implicare a experților în scopul asigurării securității spațiului informațional
2. Elaborarea cadrului juridic pentru determinarea statutului juridic al publicațiilor periodice, al agențiilor de presă și al altor entități care activează în spațiul media din Internet	2. Lege de modificarea cadrului juridic existent
3. Crearea resursei/platformei informaționale de comunicare strategică	3. Resursă/platformă informațională de comunicare 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 menționat urmează a fi realizat prin următoarele acțiuni:

1) crearea, la nivel național, a entității cu 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 informațional, atât la nivel național cât și internațional (Consiliul coordonator pentru asigurarea securității informaționale):

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

b) determinarea liniei de activitate pentru fiecare componentă inclusă în cadrul Consiliului coordonator pentru asigurarea securității informaționale în funcție de atribuțiile și funcțiile 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 a amenințărilor la adresa securității informaționale;

2) elaborarea, promovarea și coordonarea politicilor de securitate informațională în conformitate cu Concepția, cu prezenta Strategie și cu alte documente de politici de nivel național și internațional ce se referă la societatea informațională;

3) informarea publicului privind modalitățile de prevenire și contracarare a riscurilor și a amenințărilor la adresa componentelor sistemice ale securității informaționale, inclusiv privind fenomenele nou-apărute la nivel național.

94. Obiectivul nr. 2. Dezvoltarea capacităților de reacție în cazul unor amenințări hibride de securitate

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

1) crearea unei componente analitico-informaționale, specializată pe amenințările hibride de securitate în cadrul Serviciului de Informații și Securitate;

2) crearea rețelei naționale a autorităților responsabile de combaterea amenințărilor hibride de securitate;

3) elaborarea unor protocoale operaționale de interacțiune între autoritățile responsabile și factorii de decizie în cazul unor amenințări hibride de securitate;

4) consolidarea gradului de cunoaștere și înțelegere a concepției amenințărilor hibride de securitate la nivelul organelor abilitate cu asigurarea securității informaționale și a mediului general de securitate;

5) efectuarea exercițiilor pentru dezvoltarea capacităților autorităților specializate în combaterea amenințărilor hibride de securitate;

6) asocierea Republicii Moldova la Centrul European de Excelență pentru Combaterea Amenințărilor Hibrice și Centrul de Excelență pentru Comunicare Strategică al NATO.

95. Obiectivul nr. 3. Dezvoltarea competențelor operaționale de apărare cibernetică

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) crearea în cadrul Forțelor Armate a entităților responsabile de apărarea cibernetică la nivel național;

2) consolidarea capacităților de instruire și formare cibernetică prin participarea la exerciții interstatale și internaționale de apărare cibernetică;

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

96. Obiectivul nr. 4. Monitorizarea spațiului informațional și depistarea acțiunilor de dezinformare și/sau de informare manipulatorie din exteriorul și din interiorul țării

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) revizuirea cadrului legal existent în sensul definirii și uniformizării noțiunilor cu privire la dezinformare, știrile false și/sau informarea manipulatorie, precum și în vederea prevenirii răspândirii acestora prin platformele media; determinarea sectoarelor din cadrul securității naționale a căror afectare (prin dezinformare) ar crea riscuri majore pentru funcționalitatea statului;

2) stabilirea atribuțiilor organelor competente pentru depistarea și contracararea mesajelor manipulatorii și de dezinformare din rețeaua globală Internet;

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

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

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) elaborarea și aprobarea cadrului legal privind identificarea și desemnarea infrastructurilor critice naționale, inclusiv ale celor 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 securității informaționale.

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

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

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

2) raportarea din partea instituțiilor statului cu competențe în domeniu către Serviciul de Informații și Securitate a informațiilor privind starea de risc la adresa securității informaționale.

Prioritățile pilonului III	Indicatori de rezultat
----------------------------	------------------------

1. Crearea, la nivel național, a Consiliului coordonator pentru asigurarea securității informaționale, în cadrul căruia vor fi identificate proceduri de comunicare strategică	1. Cadrul normativ privind crearea Consiliului coordonator pentru asigurarea securității informaționale, elaborat și aprobat
2. Crearea în cadrul Forțelor Armate a entității responsabile de apărarea cibernetică la nivel național	2. Cadrul normativ privind crearea în cadrul Forțelor Armate a entității responsabile de apărarea cibernetică la nivel național, elaborat și aprobat
3. Crearea unei platforme specializate pe amenințările hibride la adresa securității	3. Platformă creată și funcțională
4. Elaborarea și promovarea cadrului legal de reglementare a infrastructurii critice naționale	4. Cadrul legal de reglementare a infrastructurii critice naționale elaborat și aprobat

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

99. Obiectivul nr. 1. Dezvoltarea sistemului de pregătire a resurselor umane în domeniul securității informaționale

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) evaluarea nivelului actual de pregătire a resurselor umane în domeniul securității informaționale, pe fiecare compartiment în parte: mass-media, tehnologia informațională, apărare, ordine publică și contrainformații;

2) identificarea categoriilor de beneficiari care urmează să fie incluși cu prioritate în programele noi de instruire a resurselor umane în domeniul securității informaționale;

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

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

100. Obiectivul nr. 2. Coordonarea activității autorităților administrației publice, a instituțiilor publice și private în exercitarea atribuțiilor privind asigurarea securității informaționale

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) identificarea cadrului normativ relevant ce reglementează atribuțiile autorităților administrației publice, ale instituțiilor publice și private privind asigurarea securității informaționale și modificarea acestuia excluzând lacunele și dublările de competențe;

2) reglementarea expresă în legislație a atribuției de coordonare a activității autorităților administrației publice, a instituțiilor publice și private în exercitarea atribuțiilor privind asigurarea securității informaționale, precum și a mecanismului de realizare a acestei activități de către autoritatea publică desemnată;

3) elaborarea și încheierea unor acorduri de cooperare interinstituționale multilaterale care ar specifica modul de coordonare a activității în exercitarea atribuțiilor privind asigurarea securității informaționale.

101. Obiectivul nr. 3. Asigurarea cooperării internaționale în domeniul securității informaționale

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) evaluarea nivelului actual al cooperării dintre Republica Moldova și organizațiile internaționale ce își desfășoară activitatea în domeniul asigurării securității informaționale și elaborarea unor acțiuni privind intensificarea cooperării respective;

2) stabilirea cooperării dintre Republica Moldova și statele partenere, în special cele din cadrul Uniunii Europene, privind schimbul de informații, experiențe și analize în scopul prevenirii, depistării și contracarării amenințărilor hibride la adresa securității în spațiul informațional;

3) promovarea pe plan internațional, inclusiv în cadru bilateral, a necesității de a încheia acorduri ce ar unifica conceptul de „armă informațională”, interzicând elaborarea, răspândirea și aplicarea acesteia în relațiile dintre state;

4) alinierea la și implementarea instrumentelor internaționale existente ce ar asigura prevenirea, depistarea și contracararea accesului neautorizat la informațiile cu accesibilitate limitată din rețelele de comunicații electronice bancare și din sistemele de comerț electronic, precum și la informațiile organelor internaționale de ocrotire a normelor de drept.

102. Obiectivul nr. 4. Dezvoltarea cooperării naționale și internaționale în domeniul apărării cibernetice

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) crearea/implementarea cadrului de cooperare interinstituțională pe domeniul apărării cibernetice;

2) intensificarea cooperării cu partenerii de dezvoltare externi privind schimbul de informații și de experiență în domeniul apărării cibernetice;

3) semnarea unor acorduri de colaborare (asistență mutuală) în domeniul apărării cibernetice.

103. Obiectivul nr. 5. Consolidarea cooperării internaționale în domeniul prevenirii și combaterii criminalității informatice

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) consolidarea mecanismelor de cooperare internațională între autoritățile statului cu atribuții în combaterea criminalității informatice și organismul internațional specializat EMAS (Europol Malware Analysis Solution) al EUROPOL;

2) utilizarea, la nivel național, a instrumentelor și metodelor de identificare a victimelor, inclusiv prin utilizarea Sistemului informațional automatizat „Protecția Copiilor” și a Bazei de date privind exploatarea sexuală a copiilor (ICSE) a OIPC INTERPOL;

3) cooperarea în cadrul punctelor naționale de contact 24/7 în baza Convenției Consiliului Europei privind criminalitatea informatică (Budapesta, 2001) și G7 24/7;

4) dezvoltarea parteneriatelor existente cu NCMEC (Centrul Național al SUA privind Copiii Dispăruți și Exploatați) și aderarea la alte inițiative similare;

5) dezvoltarea unor parteneriate în scopul identificării, blocării, sechestrării și confiscării produselor și a instrumentelor provenite din infracțiunile transfrontaliere;

6) participarea la evenimente internaționale în domeniul prevenirii și combaterii criminalității informatice în scopul formării personalului de specialitate.

Prioritățile pilonului IV	Indicatori de rezultat
1. Dezvoltarea și implementarea programelor de instruire adresate angajaților cu atribuții de investigare și urmărire penală în spațiul informațional	1. Specialiști instruiți în baza practicilor UE
2. Dezvoltarea cooperării naționale și	2. Cadrul legal de cooperare negociat și

internaționale în domeniul apărării cibernetice	încheiat
3. Stabilirea mecanismelor de cooperare internațională între autoritățile statului cu atribuții în combaterea criminalității informatice și organisme internaționale pe segmentul asigurării securității informaționale	3. Runde de consultări; acorduri bilaterale/multilaterale semnate și încheiate

V. ESTIMAREA IMPACTULUI ȘI A COSTURILOR IMPLEMENTĂRII STRATEGIEI

104. Implementarea calitativă a prevederilor prezentei Strategii va spori gradul de protecție și de securitate în spațiul informațional.

105. Impactul realizării implementării Strategiei se va manifesta prin:

- 1) asigurarea drepturilor și a libertăților constituționale ale cetățenilor la prelucrarea datelor acestora;
- 2) protejarea și promovarea democrației participative și pluraliste;
- 3) dezvoltarea societății informaționale naționale, sub toate aspectele structurale și funcționale, de natură individuală, publică, privată sau de stat;
- 4) asigurarea prevenirii și a investigării eficiente a crimelor informatice;
- 5) protecția societății împotriva influențelor informaționale și psihologice distructive;
- 6) protecția societății împotriva dezinformărilor distructive având drept scop incitarea la ură națională și religioasă, schimbarea orânduirii constituționale;
- 7) dezvoltarea mecanismelor de combatere colectivă a amenințărilor hibride de securitate ce periclitează securitatea informațională și mediul general de securitate;
- 8) asigurarea protecției întreprinderilor, instituțiilor și a organizațiilor în accesul acestora la informații corecte și obiective;
- 9) asigurarea liberei circulații a informațiilor, a pluralismului media și a platformelor de informare on-line și off-line, cu excepția cazurilor prevăzute de lege;
- 10) dezvoltarea și protejarea infrastructurii naționale de informare;
- 11) consolidarea principiilor de informare a diasporei cu privire la situația din Republica Moldova;
- 12) funcționarea și dezvoltarea în condiții de siguranță a spațiului informațional național și integrarea acestuia în spațiul informațional european și cel mondial;
- 13) dezvoltarea sistemului de comunicații strategice din Republica Moldova;
- 14) interacțiunea eficientă a autorităților publice și a societății civile în procesul de formare și implementare a politicii de stat în domeniul informațiilor;
- 15) asigurarea dezvoltării tehnologiilor informației și comunicațiilor și a resurselor informaționale ale Republicii 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 persoanelor, în special a copiilor, precum și a datelor cu caracter personal, în mediul on-line.
- 19) determinarea statutului juridic al entităților/subiecților din spațiul informațional al Internetului.

106.În scopul obținerii rezultatelor trasate la pct. 105, este necesar, întâi de toate, să fie consolidate într-o direcție unică responsabilitățile autorităților administrațiilor publice, ale instituțiilor și ale întreprinderilor de stat, indiferent de forma de organizare și acționare a acestora.

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 de finanțare conform legii.

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

110.Estimarea alocațiilor financiare necesare pentru realizarea anumitor obiective și activități-cheie stabilite în Planul de acțiuni pentru implementarea prezentei Strategii generează riscul divulgării unor date clasificate, fapt ce impune definitivarea, în mod individual, la nivelul autorităților/instituțiilor, a sumelor necesare pentru fiecare an bugetar și reglementarea acestora prin actele normative care urmează a fi elaborate în contextul Strategiei.

VI.REZULTATELE SCONTATEȘI INDICATORII DE PROGRES

111.Implementarea prezentei Strategii va conduce la identificarea unor abordări inovatoare în formarea unui sistem de protecție și dezvoltare a spațiului informațional în condițiile globalizării și ale liberei circulații a informațiilor, și anume:

- 1) vor fi elaborate soluții tehnice speciale de sporire a fiabilității rețelelor comunicaționale în cazuri critice;
- 2) vor fi create arhive și stocuri de documente electronice în vederea depozitării securizate a bazelor de date de importanță națională, în conformitate cu regimul de stocare, păstrare și evidență stabilit de legislație;
- 3) vor fi consolidate mecanismele de protecție a datelor cu caracter personal în vederea eliminării utilizării acestora în scopuri ilegale;
- 4) vor fi dezvoltate capacitățile naționale necesare efectuării unui schimb securizat și stocării informațiilor, transmiterii prompte și eficiente a fluxului de informații, inclusiv a celor clasificate, pe plan intern și extern, în cazul unor crize ori situații excepționale;
- 5) va fi creat mecanismul pentru îmbunătățirea implicării societății civile în domeniile prioritare de asigurare a securității informaționale;
- 6) vor fi instituite mecanisme eficiente de monitorizare, de control și de implementarea Strategiei în vederea diminuării discrepanțelor și a provocărilor existente, în vederea protejării societății de eventuale tentative de dezinformare și/sau de informare manipulatorie din exterior;
- 7) vor fi stabilite garanții specifice pentru a proteja cât mai eficient datele cu caracter personal, viața intimă, familială și privată a persoanelor, în special în mediul on-line;
- 8) vor fi asigurate măsuri de prevenire și combatere a criminalității informatice.

112.Prezenta Strategie are ca element central crearea Consiliului coordonator pentru asigurarea securității informaționale, organism colectiv, cu atribuții consultative și operaționale, ce va fi responsabil și va asigura integrarea sistemică a componentelor spațiului informațional și susținerea unui nivel înalt de securitate informațională.

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

a) *Palierul cibernetic*, care va include reprezentanți ai Centrului național de reacție la incidente de securitate cibernetică, ai Centrului guvernamental de reacție la incidente de securitate cibernetică și ai Centrului privat de reacție la incidente de securitate cibernetică, precum și experți ai unităților de securitate cibernetică ale altor instituții de drept public și de drept privat ce activează în sectorul tehnologiilor informaționale și pot contribui la asigurarea securității informaționale a Republicii Moldova;

b) *Palierul mediatic*, care va fi constituit din reprezentanți ai spațiului mediatic național, în special din reprezentanți ai mass-mediei tradiționale (posturi radio, posturi TV și presa scrisă), dar și ai media din Internet, incluși în funcție de caracterul politicilor editoriale ce vor avea drept preocupări procesele ce țin de asigurarea securității spațiului mediatic;

c) *Palierul operațional*, care va fi format în special din reprezentanți ai autorităților publice cu atribuții și competențe în materie de apărare, informații, contrainformații, investigații și procesuală, conform prerogativelor acestora de asigurare a securității spațiului informațional;

d) *Palierul civic-privat*, care va fi constituit din reprezentanți ai societății civile, potrivit recomandărilor Consiliului societății civile, ai asociațiilor ce reprezintă sectorul IT național, ai companiilor de drept privat din domeniul IT, precum și din experți internaționali din rândul partenerilor strategici actuali și de perspectivă ai Republicii Moldova, specializați în consolidarea dimensiunii de securitate cibernetică și informațională la nivel regional, european și internațional.

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

3) Modul de desemnare a organelor de conducere ale Consiliului coordonator pentru asigurarea securității informaționale va fi prevăzut în statut și va fi bazat pe principiul rotației succesive.

4) Palierele specificate vor activa în mai multe moduri: separat, mixt, prin atragerea experților de pe alte paliere, sau integrat, la nivelul întregului Consiliu coordonator pentru asigurarea securității informaționale, fiind desemnat un organ de conducere din rândul componentelor cu atribuții și competențe prioritare, reieșind din problematica examinată.

5) Consiliul coordonator pentru asigurarea securității informaționale va avea ca prioritate de activitate examinarea incidentelor de securitate informațională a căror soluționare necesită o abordare integrată, accentul fiind plasat pe operativitate în examinarea cazurilor, determinarea acțiunilor de reacție timpurie, prevenirea, contracararea sau eliminarea consecințelor.

6) Serviciul de Informații și Securitate va avea calitatea de coordonator al activității Consiliului coordonator pentru asigurarea securității informaționale, fiind responsabil de recepționarea sesizărilor de incidente de securitate informațională și prezentarea acestora către conducătorii palierelor.

VII. PROCEDURI DE MONITORIZARE ȘI EVALUARE

113. Monitorizarea prezentei Strategii are drept scop:

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

2) asigurarea transparenței și difuzarea informațiilor cu privire la acțiunile realizate și rezultatele obținute.

114.Procesul de implementare a prezentei Strategii va fi însoțit de monitorizarea permanentă a realizării acțiunilor propuse și a rezultatelor obținute, fiind operate, în caz de necesitate, modificările de rigoare în politicile publice promovate de Guvern în contextul prezentei Strategii.

115.Monitorizarea și coordonarea procesului de implementarea prezentei Strategii și de realizare a Planului de acțiuni pentru implementarea acesteia se pun în sarcina Serviciului de Informații și Securitate.

116.Ministerele, instituțiile și alte autorități administrative centrale vor asigura întreprinderea măsurilor necesare în vederea realizării integrale, în termenele stabilite și conform competențelor ce le sînt atribuite, a acțiunilor incluse în Planul de acțiuni pentru implementarea prezentei Strategii.

PLAN DE ACȚIUNI
pentru implementarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024

Nr. crt.	Obiective	Acțiuni	Instituții responsabile	Parteneri	Surse de finanțare/ costuri	Termene de realizare	Indicatori de progres
1	2	3	4	5	6	7	8
PILONUL I. Asigurarea securității spațiului informațional-cibernetice și investigarea criminalității informatice							
1	Crearea unui sistem integrat de comunicare și evaluare a amenințărilor la adresa securității informaționale și de elaborare a măsurilor operative de răspuns	1) Crearea/desemnarea entității care va exercita rolul de Centru național de reacție la incidente 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: a)elaborarea și promovarea cadrului normativ relevant; b) crearea Centrului național de reacție la incidente de securitate cibernetică	Serviciul Tehnologia Informației și Securitate Cibernetică; Cancelaria de Stat; Ministerul Finanțelor; Ministerul Economiei și Infrastructurii	Serviciul de Informații și Securitate; Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației; Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală; Centrul Național pentru Protecția Datelor cu Caracter Personal; Agenția de Guvernare Electronică;	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2019–2021	Cadrul normativ elaborat și aprobat; Centrul național de reacție la incidente de securitate cibernetică, creat

1	2	3	4	5	6	7	8
				Agenția de Stat pentru Proprietatea Intelectuală; furnizorii de servicii de comunicații electronice			
		2) Desemnarea entității care va exercita rolul de Centru guvernamental de reacție la incidente de securitate cibernetică și care va constitui punctul de raportare a incidentelor de securitate cibernetică al Guvernului; stabilirea interacțiunii acestuia cu Centrul național de reacție la incidente de securitate cibernetică	Serviciul Tehnologia Informației și Securitate Cibernetică; Cancelaria de Stat	Centrul Național pentru Protecția Datelor cu Caracter Personal; Ministerul Economiei și Infrastructurii; Serviciul de Informații și Securitate; Ministerul Afacerilor Interne; Procuratura Generală	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2019	Cadrul normativ (actul de desemnare) aprobat
		3) Stabilirea de către Centrul național de reacție la incidente de securitate cibernetică a indicatorilor din domeniul securității cibernetică: a) sistematizarea datelor statistice la capitolul securității cibernetică, analiza și evaluarea acestora	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	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2023	Acte normative elaborate și aprobate; produsul de analiză privind starea în domeniul securității cibernetică

1	2	3	4	5	6	7	8
				Personal			
		4) Elaborarea mecanismelor de creare și consolidare a centrelor departamentale de reacție la incidente de securitate cibernetică și informațională, atât de drept public, cât 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 limita alocațiilor aprobate; asistență externă	2021–2023	Mecanismele identificate și aprobate
		5) Elaborarea cadrului normativ pentru asigurarea unui nivel înalt de securitate a rețelelor și a sistemelor informatice la nivel național în baza bunelor practici ale UE	Ministerul Economiei și Infrastructurii	Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Cadrul normativ aprobat
		6) Determinarea politicii privind modalitatea de raportare, de stocare și de prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale	Serviciul Tehnologia Informației și Securitate Cibernetică	Serviciul de Informații și Securitate; Procuratura Generală	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2022	Cadrul normativ aprobat
2	Monitorizarea permanentă și asigurarea unui nivel înalt de	1) Identificarea și eliminarea surselor de amenințare la adresa securității persoanei, a	Agenția de Guvernare Electronică; Serviciul	Serviciul de Informații și Securitate; Agenția Servicii	Bugetul instituțiilor, în limita alocațiilor aprobate;	Permanent	Raportul de audit privind starea de securitate cibernetică

1	2	3	4	5	6	7	8
	securitate cibernetică	<p>societății și a statului în spațiul cibernetic:</p> <p>a) efectuarea auditului de securitate cibernetică a infrastructurilor de tehnologie a informației de interes național și a Sistemului de telecomunicații al autorităților administrației publice, precum și a altor infrastructuri cibernetic de interes național, în vederea identificării disfuncțiilor și vulnerabilităților; furnizarea soluțiilor/recomandărilor de remediere a acestora;</p> <p>b) implementarea rezultatelor auditului de securitate cibernetică</p>	Tehnologia Informației și Securitate Cibernetică	Publice; Ministerul Economiei și Infrastructurii; Ministerul Afacerilor Interne; Procuratura Generală	asistență externă		elaborat; raportul privind implementarea propunerilor auditului, realizat
		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	Agenția de Guvernare Electronică	Autoritățile administrației publice	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Raportul privind modul de aplicare a Cerințelor minime de securitate cibernetică, realizat

1	2	3	4	5	6	7	8
		suprimarea amenințărilor respective					
		3) Elaborarea mecanismelor și a metodelor de prevenire și contracarare a pericolelor în spațiul cibernetic, generate de serviciile informaționale prestate de către persoanele fizice și juridice	Serviciul de Informații și Securitate	Ministerul Economiei și Infrastructurii; Serviciul Tehnologia Informației și Securitate Cibernetică; Ministerul Afacerilor Interne; Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Mecanismele elaborate
		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	Serviciul de Informații și Securitate; Ministerul Afacerilor Interne	Serviciul Tehnologia Informației și Securitate Cibernetică; Ministerul Economiei și Infrastructurii	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2022	Cadrul normativ elaborat și aprobat
		5) Coordonarea cu Centrul Național pentru	Autoritățile administrației	Centrul Național pentru Protecția	Bugetul instituțiilor, în	2019–2020	Cadrul normativ modificat

1	2	3	4	5	6	7	8
		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 acestora 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 astfel de date în corespundere cu legislația privind protecția datelor cu caracter personal	publice	Datelor cu Caracter Personal	limita alocațiilor aprobate; asistență externă		
3	Consolidarea capacităților de apărare cibernetică	1) Delimitarea și atribuirea rolurilor și a responsabilităților privind apărarea cibernetică ce revin sistemului de organe ale securității statului și sistemului național de apărare	Ministerul Apărării; Serviciul de Informații și Securitate	Ministerul Afacerilor Interne; Procuratura Generală	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2019–2020	Cadrul normativ modificat
		2) Elaborarea măsurilor	Serviciul de	Ministerul Afacerilor	Bugetul	2021–2023	Măsurile de

1	2	3	4	5	6	7	8
		de apărare cibernetică pentru protecția infrastructurii critice naționale, precum și a altor sectoare prioritare pentru stat	Informații și Securitate; Ministerul Apărării	Interne; Procuratura Generală; Ministerul Economiei și Infrastructurii; Serviciul Tehnologia Informației și Securitate Cibernetică	instituțiilor, în limita alocațiilor aprobate; asistență externă		apărare cibernetică pentru protecția 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 a componentei TIC din sistemele de apărare națională	Serviciul de Informații și 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 instituțiilor, în limita alocațiilor aprobate; asistență externă	2022	Măsurile de protecție a sistemelor informaționale ce prelucrează informații atribuite la secret de stat, elaborate și aprobate
4	Protecția rețelelor de comunicații speciale ale Republicii Moldova și a	1) Dezvoltarea mecanismelor de protecție a sistemelor speciale de comunicații electronice prin aplicarea	Serviciul de Informații și Securitate	Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Mecanismele implementate

1	2	3	4	5	6	7	8
	informației cu accesibilitate limitată, pentru menținerea funcțiilor vitale ale statului	mijloacelor de protecție criptografică și tehnică a informațiilor					
		2) Efectuarea controalelor asupra sistemelor speciale de comunicații electronice și raportarea către autoritatea responsabilă cu privire la măsurile tehnice și tehnico-organizatorice întreprinse pentru asigurarea securității cibernetice	Serviciul de Informații și Securitate	Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Numărul de controale efectuate
		3) Actualizarea cadrului normativ în domeniul sistemelor speciale de comunicații electronice	Serviciul de Informații și Securitate	Ministerul Afacerilor Interne (Serviciul Tehnologia Informației)	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2023	Cadrul normativ modificat
		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	Serviciul de Informații și Securitate		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2023–2024	Sistemul de atestare a obiectelor de informatizare, elaborat și implementat

1	2	3	4	5	6	7	8
		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	Centrul Național pentru Protecția Datelor cu Caracter Personal	Ministerul Afacerilor Interne; Serviciul de Informații și Securitate; Procuratura Generală; Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Cadrul normativ modificat
		6) Promovarea cadrului normativ privind instituirea subdiviziunilor responsabile de protecția datelor cu caracter personal în cadrul persoanelor juridice de drept public și de drept privat	Centrul Național pentru Protecția Datelor cu Caracter Personal	Autoritățile administrației publice	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020	Cadrul normativ promovat
5	Asigurarea controlului asupra importului, certificării și utilizării	1) Certificarea mijloacelor de protecție tehnică și criptografică a informației	Serviciul de Informații și Securitate	Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limita alocațiilor aprobate	Permanent	Numărul de mijloace certificate
		2) Dezvoltarea sistemelor	Serviciul	Ministerul	Bugetul	2020–2023	Sistemul elaborat și

1	2	3	4	5	6	7	8
	mijloacelor de protecție a informației	de monitorizare a importului mijloacelor de protecție a informației	Vamal; Serviciul de Informații și Securitate	Economiei și Infrastructurii	instituțiilor, în limita alocațiilor aprobate		implementat
		3) Alinierea cadrului normativ în domeniul protecției criptografice a informației la cadrul normativ european	Serviciul de Informații și Securitate	Ministerul Justiției; Ministerul Afacerilor Externe și Integrării Europene; Ministerul Economiei și Infrastructurii	În limita bugetului instituțiilor	2021	Cadrul normativ modificat
		4) Crearea unei baze de date privind mijloacele de protecție tehnică și criptografică a informației	Serviciul de Informații și Securitate	Serviciul Tehnologia Informației și Securitate Cibernetică; Agenția de Guvernare Electronică; Ministerul Economiei și Infrastructurii	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2022	Baza de date creată și completată
		5) Exercițarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice	Serviciul de Informații și Securitate		Bugetul instituțiilor, în limita alocațiilor aprobate	Permanent	Registrul completat
6	Combaterea criminalității informatice (investigarea infracțiunilor informatice)	1) Eficientizarea capacităților (mecanismului) de combatere a criminalității informatice	Ministerul Afacerilor Interne (Inspectoratul General al Poliției);		Bugetul instituțiilor, în limita alocațiilor aprobate	Permanent	Numărul de persoane instruite

1	2	3	4	5	6	7	8
			Procuratura Generală				
		2) Acordarea ajutorului metodico-practic subdiviziunilor teritoriale privind investigarea infracțiunilor informatice	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală		Bugetul instituțiilor, în limita alocațiilor aprobate	Permanent	Numărul de persoane din cadrul subdiviziunilor teritoriale, instruite
		3) Implementarea de noi mecanisme la nivelul instituțiilor implicate în combaterea criminalității informatice (atragera companiilor private și a experților independenți, dezvoltarea laboratoarelor)	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Serviciul de Informații și Securitate	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Mecanisme funcționale implementate
		4) Perfecționarea cadrului legal ce reglementează salarizarea efectivului specializat în combaterea criminalității informatice și investigarea infracțiunilor informatice	Ministerul Finanțelor; Ministerul Afacerilor Interne	Ministerul Sănătății, Muncii și Protecției Sociale	Bugetul instituțiilor, în limita alocațiilor aprobate	2020	Cadrul legal privind majorarea cu 30% a salariului în raport cu salariul net, aprobat
7	Protecția copiilor față de orice formă de abuz în spațiul on-line	1) Combaterea fenomenului de pornografie infantilă pe Internet	Ministerul Afacerilor Interne (Inspectoratul	Ministerul Sănătății, Muncii și Protecției Sociale; Ministerul Educației,	Bugetul instituțiilor, în limita alocațiilor aprobate;	Permanent	Numărul de măsuri realizate/cazuri investigate

1	2	3	4	5	6	7	8
			General al Poliției); Procuratura Generală	Culturii și Cercetării; organizațiile neguvernamentale; societatea civilă; mass-media	asistență externă		
		2) Combaterea fenomenelor de ademenire (grooming) și hărțuire sexuală a copiilor prin intermediul Internetului	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Ministerul Educației, Culturii și Cercetării; organizațiile neguvernamentale; societatea civilă; Ministerul Sănătății, Muncii și Protecției Sociale; furnizorii de servicii de comunicații electronice	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Numărul de măsuri realizate/cazuri investigate
		3) Promovarea unui Internet mai sigur pentru copii prin intermediul consilierilor on-line și încurajarea raportărilor prin proiecte informaționale specializate	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Ministerul Educației, Culturii și Cercetării; organizațiile neguvernamentale; societatea civilă; Ministerul Sănătății, Muncii și Protecției Sociale	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Numărul de campanii de informare
8	Combaterea fraudelor prin utilizarea mijloacelor de plată electronice	1) Schimbul de informații între Centrul pentru combaterea crimelor informatice din cadrul MAI și departamentele de securitate ale instituțiilor	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura	Banca Națională a Moldovei; instituțiile financiare	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Acord privind schimbul de informații

1	2	3	4	5	6	7	8
		financiare	Generală				
		2) Promovarea unor măsuri de securitate sporită în privința bancomatelor (ATM-urilor) la nivel de hardware și software	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Banca Națională a Moldovei; instituțiile financiare	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Numărul de măsuri de securitate implementate
		3) Identificarea mecanismelor comune de combatere a fraudelor în tranzacțiile cu card și fără card (card-present și card not-present)	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Banca Națională a Moldovei; instituțiile financiare	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Mecanismul identificat și implementat
9	Dezvoltarea capacităților instituționale în combaterea criminalității informatice	1) Dezvoltarea unor subdiviziuni specializate în cadrul Inspectoratului General al Poliției al Ministerului Afacerilor Interne, al Procuraturii Generale și al Serviciului de Informații și Securitate în scopul depistării și contracarării tentativelor infracționale în domeniu	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală; Serviciul de Informații și Securitate		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Numărul de subdiviziuni create/specializate
		2) Crearea unei baze de date naționale privind	Procuratura Generală;	Centrul Național Anticorupție; Serviciu	Bugetul instituțiilor, în	2022	Baza de date creată

1	2	3	4	5	6	7	8
		evoluția fenomenului criminalității informatice	Serviciul de Informații și Securitate; Ministerul Afacerilor Interne	I Vamal; Centrul Național pentru Protecția Datelor cu Caracter Personal	limita alocațiilor aprobate; asistență externă		
		3) Ajustarea activității desfășurate în domeniul criminalității informatice în banca centrală de date a Sistemului informațional automatizat „Registrul informațiilor criminalistice și criminologice”	Ministerul Afacerilor Interne (Serviciul Tehnologia Informației)	Procuratura Generală; Serviciul de Informații și Securitate; Serviciul Vamal; Centrul Național Anticorupție; Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Mecanismele ajustate/ implementate
		4) Elaborarea cadrului normativ care să reglementeze instituirea Sistemului informațional automatizat „E-dosar” în cadrul organelor implicate în efectuarea urmăririi penale și judecarea cauzelor, precum și implementarea, dezvoltarea și interconectarea acestuia	Procuratura Generală	Ministerul Afacerilor Interne; Serviciul de Informații și Securitate; Centrul Național Anticorupție; Serviciu I Vamal; Centrul Național pentru Protecția Datelor cu Caracter Personal	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2019–2021	Cadrul normativ elaborat
10	Efectuarea unor cercetări științifice	1) Planificarea și dezvoltarea activității de	Ministerul Educației,		Bugetul instituțiilor, în	2019–2021	Planul de acțiuni elaborat și aprobat

1	2	3	4	5	6	7	8
	aplicative în domeniul securității informaționale	cercetare științifică în domeniul tehnologiei informaționale și comunicaționale	Culturii și Cercetării; Academia de Științe a Moldovei; Agenția Națională pentru Cercetare și Dezvoltare		limita alocațiilor aprobate; asistență externă		
		2) Crearea/consolidarea laboratoarelor de securitate cibernetică din cadrul instituțiilor de învățământ superior și al instituțiilor de cercetare științifică	Academia de Științe a Moldovei	Serviciul Tehnologia Informației și Securitate Cibernetică; reprezentanți ai sectorului privat	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2022–2024	Numărul de laboratoare de securitate cibernetică create și consolidate
11	Dezvoltarea capacităților de reziliență cibernetică și ridicarea nivelului de cultură în domeniul TIC	1) Desfășurarea unor acțiuni de sensibilizare și informare a societății privind amenințările, vulnerabilitățile și riscurile la adresa securității cibernetică	Serviciul Tehnologia Informației și Securitate Cibernetică	Agenția de Guvernare Electronică; Serviciul de Informații și Securitate; Ministerul Educației, Culturii și Cercetării; Ministerul Economiei și Infrastructurii	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de campanii de informare realizate
		2) Realizarea de către Centrul național de reacție la incidente de securitate cibernetică a	Serviciul Tehnologia Informației și Securitate	Serviciul de Informații și Securitate; Agenția de	Bugetul instituțiilor, în limita alocațiilor aprobate;	2021–2024	Raportul privind incidentele de securitate cibernetică,

1	2	3	4	5	6	7	8
		analizei strategice privind incidentele de securitate cibernetică și coordonarea acțiunilor de răspuns la astfel de incidente, inclusiv prin organizarea unor cursuri specializate de către experți calificați	Cibernetică	Guvernare Electronică; Centrul Național pentru Protecția Datelor cu Caracter Personal	asistență externă		elaborat
		3) Desfășurarea unor exerciții și antrenamente comune de consolidare a capacităților de reacție la atacuri ciberneticе, inclusiv de blocare a atacurilor ciberneticе 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 limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de exerciții și antrenamente realizate
		4) Organizarea și desfășurarea atelierelor de lucru în domeniul securității ciberneticе pentru personalul din sectorul public și privat deținători 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;	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de ateliere de lucru organizate

1	2	3	4	5	6	7	8
				Procuratura Generală; Centrul Național pentru Protecția Datelor cu Caracter Personal; reprezentanți ai sectorului privat; societatea civilă			
		5) Certificarea specialiștilor în domeniul securității cibernetice de către organizații /companii specializate pornind de la standardele aplicate și cerințele minime obligatorii de securitate cibernetică	Agenția de Guvernare Electronică	Ministerul Economiei și Infrastructurii; Serviciul Tehnologia Informației și Securitate Cibernetică; autoritățile administrației publice	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de specialiști certificați
		6) Organizarea unor campanii de sensibilizare și informare privind pericolele din 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; reprezentanți ai sectorului privat	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2022	Campanii de sensibilizare organizate
		7) Introducerea și promovarea unor conținuturi curriculare privind securitatea	Ministerul Educației, Culturii și Cercetării	Serviciul Tehnologia Informației și Securitate Cibernetică;	Bugetul instituțiilor, în limita alocațiilor aprobate;	2020–2021	Numărul de instituții de învățământ în care au fost introduse

1	2	3	4	5	6	7	8
		informațională în programele naționale de studii		Agencia de Guvernare Electronică; Serviciul de Informații și Securitate; Ministerul Afacerilor Interne; Procuratura Generală; Centrul Național pentru Protecția Datelor cu Caracter Personal; societatea civilă	asistență externă		conținuturile curriculare
		8) Organizarea, inclusiv împreună cu partenerii străini, a cursurilor de instruire tematică în domeniul securității cibernetice pentru angajații instituțiilor publice	Agencia de Guvernare Electronică	Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Numărul de cursuri de instruire realizate
PILONUL II: Asigurarea securității spațiului informațional-mediatic							
12	Dezvoltarea mecanismelor de comunicare strategică pentru realizarea intereselor naționale ale	1) Evaluarea sectoarelor vulnerabile la componenta mediatică din cadrul sistemului de securitate informațională	Autoritățile administrației publice		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Raportul de evaluare a sectoarelor vulnerabile sub aspectul comunicării strategice

1	2	3	4	5	6	7	8
	Republicii Moldova	2) Dezvoltarea unor politici 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 Audiovizualului	Autoritățile administrației publice; societatea civilă; mass-media	Bugetul instituțiilor, în limita 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) ghidurile de comunicare strategică pe subiecte de interes național; c) tentativele și acțiunile de dezinformare și/sau de informare manipulatorii ce afectează securitatea informațională și starea	Serviciul de Informații și Securitate	Societatea civilă; mass-media	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Resursa/platforma informațională creată și prezentată

1	2	3	4	5	6	7	8
		generală de securitate					
13	Controlul civic și consolidarea cooperării societății civile cu autoritățile publice cu atribuții de asigurare a securității informaționale	<p>1) Crearea unui mecanism de implicare a experților din rîndul societății civile, a organizațiilor neguvernamentale și a mass-mediei în domeniul securității informaționale, prin:</p> <p>a) desemnarea unui consiliu existent sau crearea unui organ colectiv din rîndul societății civile cu atribuții de evaluare a experților, a organizațiilor neguvernamentale și a mass-mediei din perspectiva implicării în materie de asigurare a securității informaționale și naționale – Consiliul societății civile;</p> <p>b) certificarea de către Consiliul societății civile a experților și a reprezentanților societății civile și ai mass-mediei ce se vor ocupa de</p>	Societatea civilă; mass-media	Autoritățile statului din cadrul sistemului de securitate și apărare	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	

1	2	3	4	5	6	7	8
		monitorizarea nivelului de asigurare a securității informaționale la nivel național					
		2) Implicarea reprezentanților societății civile certificați de către Consiliul societății civile în activitatea Consiliului coordonator pentru asigurarea securității informaționale	Societatea civilă; mass-media	Autoritățile statului din cadrul sistemului de securitate și apărare	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	
		3) Îmbunătățirea sau crearea mecanismelor de implicare a societății civile în procesele de definire, de elaborare, de monitorizare și de evaluare a politicilor de asigurare a securității informaționale realizate de către autoritățile abilitate în asigurarea securității informaționale	Societatea civilă; mass-media	Autoritățile statului din cadrul sistemului de securitate și apărare	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	
		4) Elaborarea și organizarea unor cursuri de instruire tematică pentru radiodifuzori, distribuitorii de servicii,	Societatea civilă; mass-media	Autoritățile statului ale sistemului de securitate și apărare	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	

1	2	3	4	5	6	7	8
		formatorii de opinie publică, jurnaliști și ONG-urile de profil cu privire la tehnicile de dezinformare și/sau de informare manipulatorie utilizate pentru prejudicierea securității informaționale a statului					
14	Determinarea statutului juridic al publicațiilor periodice, al agențiilor de presă și al altor subiecți care activează în spațiul media din Internet	1) Evaluarea spațiului Internet din perspectiva identificării entităților/subiecților implicați în producerea și diseminarea conținutului media online și a altor intermediari și servicii auxiliare ce au impact pentru securitatea informațională	Serviciul de Informații și Securitate; Ministerul Afacerilor Interne; Serviciul Tehnologia Informației și Securitate Cibernetică; autoritățile administrației publice	Societatea civilă; mass-media	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Raportul/studiul realizat
		2) Elaborarea și ajustarea cadrului legal funcțional în scopul reglementării juridice a raporturilor dintre reprezentanții mass-mediei care colectează și difuzează informații în Internet,	Serviciul de Informații și Securitate; Ministerul Justiției; Consiliul Audiovizualului;	Societatea civilă; mass-media	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Cadrul normativ elaborat și aprobat

1	2	3	4	5	6	7	8
		societate și autoritățile cu atribuții de asigurare a securității informaționale, în conformitate cu recomandările Comisiei Europene și bunele practici europene	autoritățile administrației publice				
		3) Implementarea cadrului normativ care prevede acțiuni comune de intervenție și de gestionare a spațiului media on-line și off-line	Autoritățile administrației publice; societatea civilă	Reprezentanți ai sectorului privat	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Raportul privind gradul de implementare a cadrului normativ, aprobat
15	Asigurarea transparenței financiare în activitatea autorităților administrației 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, de manipulare sau de propagandă, orientat spre subminarea securității informaționale, în scopul identificării comanditarilor, a surselor de finanțare și a executorilor	Serviciul de Informații și Securitate; Ministerul Justiției; Centrul Național Anticorupție; Consiliul Audiovizualului	Societatea civilă; mass-media	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Criteriile de calificare elaborate
		2) Ajustarea cadrului legal în vederea eficientizării colectării de	Serviciul de Informații și Securitate;	Societatea civilă; mass-media	Bugetul instituțiilor, în limita alocațiilor	2019–2024	Cadrul normativ elaborat și aprobat

1	2	3	4	5	6	7	8
		date pentru identificarea provenienței mijloacelor financiare și a proprietății ale subiecților implicați în activități de dezinformare, manipulare și propagandă ce subminează securitatea informațională	Ministerul Justiției; Centrul Național Anticorupție; Consiliul Audiovizualului		aprobate; asistență externă		
		3) Interacțiunea cu instituțiile de drept în ceea ce privește analiza riscurilor și a 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	Serviciul de Informații și Securitate	Serviciul de Informații și Securitate; Procuratura Generală; Ministerul Afacerilor Interne; Centrul Național Anticorupție	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Mecanismul de cooperare implementat; cadrul normativ elaborat și aprobat
Pilonul III. Consolidarea capacităților operaționale							
16	Dezvoltarea mecanismelor de prevenire, de depistare, de atenuare și de răspuns la nivel național pentru	1) Crearea, la nivel național, a entității cu competențe de promovare și coordonare a politicilor de securitate informațională într-o societate democratică în	Serviciul de Informații și Securitate	Serviciul Tehnologia Informației și Securitate Cibernetică; autoritățile administrației publice; societatea civilă;	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2019	Actul normativ privind crearea entității, elaborat și aprobat

1	2	3	4	5	6	7	8
	asigurarea securității informaționale	<p>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):</p> <p>a) identificarea și integrarea componentelor existente cu funcții și atribuții în domeniul cibernetic și mediatic, a autorităților administrației publice locale, precum și a componentelor care vor fi create pe parcurs;</p> <p>b) determinarea liniei de activitate pentru fiecare componentă inclusă în cadrul Consiliului coordonator pentru asigurarea securității informaționale, în funcție de atribuțiile și funcțiile deținute din perspectiva asigurării securității informaționale;</p> <p>c) elaborarea și adoptarea cadrului normativ de</p>		mass-media; reprezentanți ai sectorului privat			

1	2	3	4	5	6	7	8
		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 în conformitate cu Concepția, cu prezenta Strategie și cu alte 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; mass-media; reprezentanți ai sectorului privat	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Mecanisme clare de interacțiune interinstituțională, elaborate și aprobate
		3) Informarea publicului privind modalitățile de prevenire și contracarare a riscurilor și amenințărilor la adresa componentelor sistemice ale securității informaționale, inclusiv privind fenomenele nou-apărute la nivel național	Serviciul de Informații și Securitate	Autoritățile administrației publice; societatea civilă; mass-media	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de campanii de informare
17	Dezvoltarea capacităților de reacție în cazul	1) Crearea unei componente analitico-informaționale,	Serviciul de Informații și Securitate	Ministerul Afacerilor Externe și Integrării Europene;	Bugetul instituțiilor, în limita alocațiilor	2019	Actul privind crearea componentei

1	2	3	4	5	6	7	8
	unor amenințări hibride de securitate	specializată pe amenințările hibride de securitate în cadrul Serviciului de Informații și Securitate		Ministerul Afacerilor Interne; Procuratura Generală; Ministerul Apărării	aprobate; asistență externă		analitico-informaționale, elaborat și aprobat
		2) Crearea rețelei naționale a autorităților responsabile de combaterea amenințărilor hibride de securitate	Serviciul de Informații și Securitate		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020	Acord privind crearea unei rețele naționale
		3) Elaborarea unor protocoale operaționale de interacțiune între autoritățile responsabile și factorii de decizie în cazul unor amenințări hibride de securitate	Serviciul de Informații și Securitate	Autoritățile administrației publice; societatea civilă; mass-media; reprezentanți ai sectorului privat	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Numărul de protocoale elaborate și semnate
		4) Consolidarea gradului de cunoaștere și înțelegere a concepției amenințărilor hibride de securitate la nivelul organelor abilitate cu asigurarea securității informaționale și consolidarea mediului general de securitate	Serviciul de Informații și Securitate	Autoritățile administrației publice; societatea civilă; mass-media; reprezentanți ai sectorului privat	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Numărul de protocoale interinstituționale încheiate
		5) Efectuarea exercițiilor pentru dezvoltarea capacităților autorităților	Serviciul de Informații și Securitate	Autoritățile administrației publice;	Bugetul instituțiilor, în limita alocațiilor	2020–2024	Numărul de exerciții de cercetare și

1	2	3	4	5	6	7	8
		specializate în combaterea amenințărilor hibride de securitate		societatea civilă; mass-media	aprobate; asistență externă		expertizare
		6) Asocierea Republicii Moldova la Centrul European de Excelență pentru Combaterea Amenințărilor Hibride și la Centrul de Excelență pentru Comunicare Strategică al NATO	Serviciul de Informații și Securitate	Autoritățile administrației publice; societatea civilă; mass-media; reprezentanți ai sectorului privat	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2022–2024	Actul normativ elaborat și acordul încheiat
18	Dezvoltarea competențelor operaționale de apărare cibernetică	1) Crearea în cadrul Forțelor Armate a entității responsabile de apărarea cibernetică la nivel național	Ministerul Apărării	Serviciul Tehnologia Informației și Securitate Cibernetică; Serviciul de Informații și Securitate; Ministerul Afacerilor Interne	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2019–2020	Entitate creată
		2) Consolidarea capacităților de instruire și formare cibernetică prin participarea la exerciții interstatale și internaționale de apărare cibernetică	Ministerul Apărării; Serviciul de Informații și Securitate	Ministerul Afacerilor Externe și Integrării Europene; Ministerul Afacerilor Interne (Serviciul tehnologii informaționale)	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2019–2024	Numărul de persoane instruite, de exerciții desfășurate
		3) Identificarea, prevenirea și contracararea factorilor de risc cu potențial informativ-subversiv în	Serviciul de Informații și Securitate	Ministerul Apărării; Serviciul Tehnologia Informației și Securitate Cibernetică; Minister	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Raport privind riscurile identificate și/sau prevenite

1	2	3	4	5	6	7	8
		adresa apărării cibernetice a Republicii Moldova prin implementarea unui management integrat al spațiului virtual și dezvoltarea unui sistem de avertizare timpurie cu privire la elementele de risc la adresa obiectivelor de infrastructură		ul Economiei și Infrastructurii			
19	Monitorizarea spațiului informațional și depistarea acțiunilor de dezinformare și /sau de informare manipulatorii din exteriorul și din interiorul țării	1) Revizuirea cadrului legal existent în sensul definirii și uniformizării noțiunilor cu privire la dezinformare, știrile false și/sau informarea manipulatorie, precum și în vederea prevenirii răspândirii acestora prin platformele media. Determinarea sectoarelor din cadrul securității naționale a căror afectare (prin dezinformare) ar crea riscuri majore pentru funcționalitatea statului	Ministerul Justiției; Consiliul Audiovizualului	Serviciul de Informații și Securitate	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Cadrul normativ revizuit; comunicate privind sectoarele de risc ale securității naționale
		2) Stabilirea atribuțiilor organelor competente privind depistarea și contracararea mesajelor manipulatorii și de	Serviciul de Informații și Securitate	Academia de Științe a Moldovei; organizațiile societății civile; mass-media	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Cadrul legal modificat

1	2	3	4	5	6	7	8
		dezinformare din rețeaua globală Internet					
		3) Stabilirea unor filtre de depistare și/sau de blocare a unor produse informaționale și/sau resurse informaționale, ce conțin elemente de risc la adresa securității naționale, precum și elaborarea și adoptarea cadrului normativ aferent	Serviciul de Informații și Securitate	Academia de Științe a Moldovei; organizațiile societății civile; mass-media	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Cadrul normativ elaborat și adoptat
20	Sporirea capacităților de protecție a infrastructurilor critice naționale	1) Elaborarea și aprobarea cadrului legal privind identificarea și desemnarea infrastructurilor critice naționale, inclusiv a celor ce țin de sistemele informaționale de importanță vitală	Serviciul de Informații și Securitate	Autoritățile administrației publice	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2019–2021	Cadrul legal elaborat și aprobat
		2) Evaluarea și raportarea privind starea și nivelul de securitate ale obiectivelor de infrastructură critică din perspectiva securității informaționale	Serviciul de Informații și Securitate	Autoritățile administrației publice	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Mecanismul de evaluare și raportare realizat

1	2	3	4	5	6	7	8
21	Dezvoltarea capacităților de prevenire, de depistare și de contracarare a acțiunilor extremiste, teroriste și de altă natură ce periclitează securitatea informațională	1) Sincronizarea și repartizarea rațională a forțelor instituțiilor naționale spre depistarea preventivă a acțiunilor derulate din exteriorul și/sau interiorul țării, concepute ca diversiuni complexe la adresa securității informaționale	Serviciul de Informații și Securitate	Ministerul Afacerilor Interne; Procuratura Generală; Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2022	Mecanisme de interacțiune inter-instituțională elaborate; schimb sistematic de informații implementat
		2) Raportarea din partea instituțiilor statului cu competențe în domeniu către Serviciul de Informații și Securitate a informațiilor privind starea de risc la adresa securității informaționale	Autoritățile administrației publice	Serviciul de Informații și Securitate	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Numărul de rapoarte transmise/recepționate
Pilonul IV.Eficientizarea proceselor de coordonare internă și de cooperare internațională în domeniul securității informaționale							
22	Dezvoltarea sistemului de pregătire a resurselor umane în domeniul securității informaționale	1) Evaluarea nivelului actual de pregătire a resurselor umane în domeniul securității informaționale, pe fiecare compartiment în parte: mass-media, tehnologia informațională, apărare, ordine publică și contrainformații	Autoritățile administrației publice; Consiliul Audiovizualului; Ministerul Economiei și Infrastructurii; Ministerul Apărării; Ministerul	Ministerul Educației, Culturii și Cercetării	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Studiu efectuat

1	2	3	4	5	6	7	8
			Afacerilor Interne;Procuratura Generală;Serviciul de Informații și Securitate; organizațiile neguvernamentale				
		2) Identificarea categoriilor de beneficiari care urmează să fie incluși cu prioritate în programele noi de instruire a resurselor umane în domeniul vizat	Autoritățile administrației publice	Consiliul Audiovizualului;Ministerul Economiei și Infrastructurii; Ministerul Apărării; Ministerul Afacerilor Interne; Procuratura Generală; Serviciul de Informații și Securitate; organizațiile neguvernamentale din domeniul media	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021	Numărul de beneficiari identificați și instruiți
		3) Elaborarea unor programe noi de pregătire a resurselor umane în domeniul vizat	Ministerul Educației, Culturii și Cercetării;Academia de Științe a	Consiliul Audiovizualului;Ministerul Economiei și Infrastructurii; Ministerul Apărării; Ministerul Afacerilor	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021	Numărul de programe elaborate

1	2	3	4	5	6	7	8
			Moldovei	Interne; Procuratura Generală; Serviciul de Informații și Securitate; Centrul Național pentru Protecția Datelor cu Caracter Personal; organizațiile neguvernamentale din domeniul media			
		4) Dezvoltarea și implementarea unor programe de instruire adresate angajaților cu atribuții de investigare și urmărire penală, procurorilor, judecătorilor,	Academia de Științe a Moldovei; Institutul Național al Justiției; Ministerul Afacerilor Interne	Ministerul Educației, Culturii și Cercetării; Consiliul Audiovizualului; Ministerul Economiei și Infrastructurii; Ministerul Apărării; Procuratura	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2021–2024	Numărul de programe elaborate
		specialiștilor și experților judiciari în domeniu din cadrul structurilor de aplicare a legii, precum și celor adresate personalului tehnic din cadrul instituțiilor publice	(Academia „Ștefan cel Mare”)	Generală; Serviciul de Informații și Securitate; Centrul Național pentru Protecția Datelor cu Caracter Personal; organizațiile neguvernamentale			

1	2	3	4	5	6	7	8
				din domeniul media			
23	Coordonarea activității autorităților administrației publice, a instituțiilor publice și private în exercitarea atribuțiilor privind asigurarea securității informaționale	1) Identificarea cadrului normativ relevant ce reglementează atribuțiile autorităților administrației publice, ale instituțiilor publice și private privind asigurarea securității informaționale și modificarea acestuia excluzând lacunele și dublările de competențe	Autoritățile menționate în Concepție, în limita competențelor lor		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020	Cadrul normativ revizuit
		2) Reglementarea expresă în legislație a atribuției de coordonare a activității autorităților administrației publice, a instituțiilor publice și private în exercitarea atribuțiilor privind asigurarea securității informaționale, precum și a mecanismului de realizare a acestei activități de către autoritatea publică desemnată	Autoritățile menționate în Concepție, în limita competențelor lor		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020	Cadrul normativ revizuit, activitatea instituției responsabile, reglementată

1	2	3	4	5	6	7	8
		3) Elaborarea și încheierea unor acorduri de cooperare interinstituțională multilaterală, care ar specifica modul de coordonare a activității în exercitarea atribuțiilor privind asigurarea securității informaționale	Autoritățile menționate în Concepție, în limita competențelor lor		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Numărul de acorduri de colaborare încheiate
24	Asigurarea cooperării internaționale în domeniul securității informaționale	1) Evaluarea nivelului actual al cooperării dintre Republica Moldova și organizațiile internaționale ce își desfășoară activitatea în domeniul asigurării securității informaționale și elaborarea unor acțiuni privind intensificarea cooperării respective	Autoritățile administrației publice		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2021	Studiul de evaluare elaborat
		2) Stabilirea cooperării dintre Republica Moldova și statele partenere, în special cele din cadrul Uniunii Europene, privind schimbul de informații, experiențe și analize în scopul prevenirii, depistării și contracarării	Autoritățile administrației publice	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de runde de consultări organizate

1	2	3	4	5	6	7	8
		amenințărilor hibride de securitate în spațiul informațional					
		3) Promovarea pe plan internațional, inclusiv în cadru bilateral, a necesității de a încheia acorduri ce ar unifica conceptul de „armă informațională”, interzicând elaborarea, răspîndirea și aplicarea acestora în relațiile dintre state	Autoritățile administrației publice	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de acorduri internaționale negociate/semnate
		4) Alinierea la și implementarea instrumentelor internaționale existente ce ar asigura prevenirea, depistarea și contracararea accesului neautorizat la informațiile cu accesibilitate limitată din rețelele de comunicații electronice bancare și din sistemele de comerț electronic, precum și la informațiile organelor internaționale de ocrotire a normelor de drept	Autoritățile administrației publice	Ministerul Justiției; Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Cadrul normativ modificat

1	2	3	4	5	6	7	8
25	Dezvoltarea cooperării naționale și internaționale în domeniul apărării cibernetice	1) Crearea/implementarea cadrului de cooperare interinstituțională pe domeniul apărării cibernetice	Ministerul Apărării; Serviciul de Informații și Securitate; Ministerul Economiei și Infrastructurii; Serviciul Tehnologia Informației și Securitate Cibernetică; Procuratura Generală; Ministerul Afacerilor Interne	Autoritățile administrației publice	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de runde de consultări organizate
		2) Intensificarea cooperării cu partenerii de dezvoltare externi privind schimbul de informații și de experiență în domeniul apărării cibernetice	Ministerul Apărării	Ministerul Afacerilor Externe și Integrării Europene; Serviciul de Informații și Securitate; Ministerul Economiei și Infrastructurii; Serviciul Tehnologia Informației și Securitate Cibernetică	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	2020–2024	Numărul de acorduri negociate/semnate
		3) Semnarea unor	Ministerul	Centrul național de	Bugetul	2020–2024	Numărul de

1	2	3	4	5	6	7	8
		acorduri de colaborare (asistență mutuală) în domeniul apărării cibernetice	Apărării; Serviciul de Informații și Securitate	reacție la incidente de securitate cibernetică; Ministerul Afacerilor Externe și Integrării Europene	instituțiilor, în limita alocațiilor aprobate; asistență externă		acorduri negociate/semnate
26	Consolidarea cooperării internaționale în domeniul prevenirii și combaterii criminalității informatice	1) Consolidarea mecanismelor de cooperare internațională între autoritățile statului cu atribuții în combaterea criminalității informatice și organismul internațional specializat EMAS (Europol Malware Analysis Solution) al EUROPOL	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Mecanismele instituite/ consolidate
		2) Utilizarea, la nivel național, a instrumentelor și metodelor de identificare a victimelor, inclusiv prin utilizarea Sistemului informațional automatizat „Protecția Copiilor” și a Bazei de date privind exploatarea sexuală a copiilor (ICSE) a OIPC INTERPOL	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Instrumentele și metodele identificate și utilizate
		3) Cooperarea în cadrul punctelor naționale de contact 24/7 în baza	Ministerul Afacerilor Interne	Ministerul Afacerilor Externe și Integrării Europene	Bugetul instituțiilor, în limita alocațiilor	Permanent	Actul de cooperare stabilit

1	2	3	4	5	6	7	8
		Convenției Consiliului Europei privind criminalitatea informatică (Budapesta, 2001) și G7 24/7	(Inspectoratul General al Poliției); Procuratura Generală		aprobate; asistență externă		
		4) Dezvoltarea parteneriatelor existente cu 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 limita alocațiilor aprobate; asistență externă	În funcție de necesitate	Numărul de acorduri și parteneriate stabilite
		5) Dezvoltarea unor parteneriate în scopul identificării, blocării, sechestrării și confiscării produselor și 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 limita alocațiilor aprobate; asistență externă	2021	Mecanismul 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		Bugetul instituțiilor, în limita alocațiilor aprobate; asistență externă	Permanent	Numărul de evenimente frecventate; numărul de experți instruiți

1	2	3	4	5	6	7	8
			Poliției); Procuratura Generală; Servi ciul de Informații și Securitate				