Anexa nr. 1

# STRATEGIA SECURITĂȚII INFORMAȚIONALE

# A REPUBLICII MOLDOVA PENTRU ANII 2019–2024

## I. INTRODUCERE

**1.** Tehnologiile informaţionale, resursele de informare şi sistemele de comunicare electronică au devenit parte indispensabilă a tuturor domeniilor de activitate ale persoanei, societăţii şi statului. Prin dezvoltarea lor accelerată, tehnologiile informaţionale contribuie la transformări sociale de esenţă, fiind un generator pentru apariţia şi consolidarea societăţii informaţionale de nivel naţional, regional şi internaţional, depăşind cadrul juridic al frontierelor de stat sau al comunităţilor de state.

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

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

**4.** Potrivit raportului anual cu privire la monitorizarea evoluției societății informaționale la nivel mondial „Measuring the Information Society 2017”, lansat de 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 mondial[1]. Sînt implementate ori sînt în proces continuu de dezvoltare peste 21 de programe[2] şi proiecte on-line de infrastructură şi servicii publice digitale, sînt lansate strategii sectoriale în domeniul tehnologiei informației şi politici de modernizare tehnologică a guvernării.

**5.** Interacţiunea tehnologiilor informaţionale cu diversitatea conţinutului informaţional, pe de o parte, şi fuziunea reţelelor de comunicare publică şi socială cu sistemele electronice guvernamentale, pe de altă parte, contribuie la o extindere şi sinergie a spaţiului informaţional cu domeniile centrale de securitate şi apărare naţională, responsabile de asigurarea suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

**6.** Tehnologiile informaţionale generează modificări ale dimensiunii de informare şi comunicare, care se transformă în ritm accelerat într-o platformă multimedia, fiind dezvoltate noi

[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.

componente şi mijloace de comunicare on-line şi off-line, iar libera circulaţie a informaţiilor şi ideilor la nivel local, regional şi global devin un imperativ pentru crearea şi promovarea unei societăţi informate într-un stat democratic şi de drept.

**7.** Tendinţele de dezvoltare continuă a interacțiunii dintre dimensiunea tehnologică și dimensiunea de informare în toate formele de structură şi funcţionare, de natură individuală, publică, privată sau de stat, de factură naţională sau globală, conduc la apariţia unei noi configuraţii de comunicare şi schimb de date pe domeniile publice și private de care depind nivelul şi starea sectorială sau generală de securitate.

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

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

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

**11.** Campaniile de dezinformare sînt orientate spre accentuarea neîncrederii, a confuziei şi a destabilizării situaţiei sociopolitice a statului, spre influenţarea percepţiilor şi a preferinţelor existente în diferite comunităţi sociale. Acest fapt poate duce la controlul, de către diverşi actori, al comportamentului unei părţi a societăţii, precum şi la influenţarea politicilor interne şi externe ale statului.

**12.** Creşterea numărului de utilizatori ai Internetului şi evoluţiile tehnologiilor informaţionale conexe creează provocări substanţiale în ceea ce privește starea mediului de securitate, ordinea publică şi apărarea, prevenirea criminalităţii şi aplicarea legii în direcţia protecţiei drepturilor în spaţiul informațional.

**13.** Concepţia securităţii informaţionale a Republicii Moldova (în continuare – *Concepţie*), 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*) şi documentul de politici ce integrează domeniile centrale şi asociate spaţiului informaţional, ce oferă noţiuni, definește principiile de organizare la nivel de stat, societate şi persoană, precum şi detaliază metodele juridice, tehnico-organizatorice, economice şi contrainformative pentru asigurarea securităţii informaţionale a Republicii Moldova.

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

**15.** Prezenta Strategie descrie situația curentă în domeniul securității informaționale din perspectiva progreselor înregistrate și a tendinţelor de dezvoltare a societăţii informaţionale la nivel naţional, a problemelor existente și de perspectivă, care generează și creează riscuri şi ameninţări de securitate, inclusiv hibride. Complexul de acţiuni, conform scopului şi obiectivelor specificate, este compartimentat pe patru piloni:

1) Pilonul I. Asigurarea securității spațiului informațional-cibernetic 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 şi obiectivele prezentei Strategii se vor realiza în baza Planului de acţiuni pentru implementarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019–2024.

## II. DESCRIEREA SITUAȚIEI

**17.** Republica Moldova, 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 parte[3], sînt stabilite priorități de încurajare și promovare a punerii în aplicare a instrumentelor tehnologiilor informaţiei şi comunicaţiilor (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

[3] Art. 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.

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 securității informaționale este esențială pentru a întări discernămîntul 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.** Interacţiunea în spaţiul cibernetic este facilitată de diverşi actori: persoane fizice şi juridice, autorităţi de stat şi structuri neguvernamentale, grupuri formale şi informale, utilizatori personalizaţi şi anonimi. Unii îi conectează pe utilizatori, permit prelucrarea informaţiilor, găzduiesc servicii web, inclusiv conţinutul generat de utilizatori, alţii cumulează informaţii şi permit căutări, oferind acces la conţinut, gazdă, indicatori şi servicii create sau operate de către persoane terţe. O altă categorie de actori ai spaţiului cibernetic facilitează vînzarea de bunuri şi servicii, inclusiv servicii audiovizuale, de asemenea permit alte tranzacţii comerciale, de publicitate şi plăţi.

**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, începînd din momentul conceperii acestora, și pe cel al protecției implicite a datelor, în corespundere cu legislația privind protecția datelor cu caracter personal.

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

**24.** Dată fiind importanța promovării sectorului TIC pentru dezvoltarea unei societăţi informaţionale avansate în Republica Moldova, pentru crearea și dezvoltarea unei infrastructuri infocomunicaţionale integrate şi eficiente, orientate spre creşterea competitivităţii economiei naţionale şi asigurarea accesului tuturor cetăţenilor la serviciile societăţii informaţionale, au fost ajustate, completate 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 şi accesarea în siguranță a datelor, inclusiv a celor de interes public;
2) securitatea şi integritatea rețelelor şi a serviciilor de comunicații electronice;
3) dezvoltarea capacităților de prevenire şi de reacție urgentă la nivel național (crearea rețelei CERT naționale);
4) prevenirea şi combaterea criminalității informatice;
5) consolidarea capacităților de apărare cibernetică;
6) educația, formarea şi informarea continuă în domeniul securității cibernetice;
7) cooperarea şi 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 şi/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 restrînsă și/sau scopul reglementării este diferit.

**29.** În aceste condiţii, Legea nr. 299/2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova poate fi considerată un punct de pornire pentru consolidarea protejării intereselor persoanelor, ale societății și ale statului în domeniul informaţional, pentru prevenirea şi contracararea ameninţărilor complexe și persistente la adresa securităţii informaţionale, 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 importanţa şi necesitatea unei strategii care să cuprindă reglementări comprehensive ale tuturor vectorilor securităţii informaţionale.

**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 implicaţi. Mediul virtual facilitează comiterea infracțiunilor, pune la dispoziţia conduitei criminale atît un nou obiect (informaţia conţinută şi procesată de sistemele informatice), cît şi un nou instrument. Acest mediu oferă un repertoriu vast de tehnici şi strategii de săvîrşire a infracţiunilor, 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 implicaţi, mai ales la nivel instituţional, unde se concentrează responsabilitatea elaborării şi aplicării de politici coerente în domeniu.

**34.** Adoptarea prezentei Strategii este determinată de necesitatea protecţiei intereselor persoanelor, societăţii şi ale statului în spaţiul informaţional, de gravitatea şi multitudinea ameninţărilor la adresa securităţii informaţionale în societatea modernă, de necesitatea menţinerii unui echilibru între interesele persoanelor, ale societăţii şi ale statului pentru asigurarea securităţii informaţionale. Totodată, natura globală a sistemelor informaţionale şi a reţelelor de comunicaţii electronice necesită o coordonare strînsă între toate instituţiile responsabile atît la nivelul naţional, cît şi la nivel global.

## III. DEFINIREA PROBLEMELOR

### *3.1. Componenta de securitate cibernetică și investigarea criminalității informatice.*

**35.** În prezent, accesarea neautorizată a reţelelor şi serviciilor de comunicaţii electronice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice, restricţionarea ilegală a accesului la aceste date şi spionajul cibernetic sînt nişte probleme de nivel global. Rapoartele anuale ale agenţiilor internaţionale de specialitate constată creşterea costului global al criminalităţii cibernetice, prejudiciile economice fiind estimate la ordinul sutelor de miliarde de dolari SUA.

**36.** Ameninţările şi riscurile, atacurile şi incidentele cibernetice, precum şi alte evenimente survenite în spaţiul cibernetic se materializează prin exploatarea vulnerabilităților de natură umană, tehnică şi procedurală. Pe aceste căi, în ultimii ani în Republica Moldova s-au constatat creşteri ale indicatorilor privind numărul de infracţiuni şi contravenţii 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 naţional nu au fost efectuate procese de audit complexe de securitate cibernetică, nici nu există studii sau rapoarte[4] care ar reflecta în detaliu situaţia privind criminalitatea informatică (riscurile şi ameninţările cibernetice, atacurile şi incidentele cibernetice, alte evenimente survenite în spaţiul cibernetic), precum şi numărul victimelor şi valoarea prejudiciilor economice ale acesteia.

[4] Singurele surse oficiale de date statistice privind criminalitatea informatică sînt Registrul de evidenţă a infracţiunilor, a cauzelor penale, a persoanelor care au săvîrşit infracţiuni şi a materialelor cu privire la infracţiuni, deţinut de Ministerul Afacerilor Interne şi Sistemul informaţional automatizat ,,Urmărirea penală: E-dosar", gestionat de Procuratura Generală.

**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 securităţii cibernetice în cadrul căruia să se efectueze coordonat planificarea şi utilizarea resurselor disponibile, identificarea vulnerabilităţilor şi a riscurilor în urma auditului de securitate cibernetică, precum și a intervenţiilor necesare pentru diminuarea impactului dăunător al criminalităţii, al atacurilor şi al incidentelor cibernetice asupra dezvoltării sigure a societăţii informaţionale.

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

**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) insuficienţa de specialişti calificaţi în domeniul tehnologiilor informaționale şi 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, specialiştilor şi experţilor 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) finanţarea redusă pentru participarea specialiştilor 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 algoritmelor complexe asimetrice de criptare a informației critice la estorcarea mijloacelor financiare prin intermediul tehnologiilor informaţionale;

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

4) rețelele de schimb direct de date dintre utilizatori, ceea ce nu lasă anumite urme ale activităţii în conţinutul istoricului înregistrat în sistemul informatic sau în logurile deţinute 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 constrîngeri în gestionarea, dezvoltarea și asigurarea securității acestora.

**44.** Resursele disponibile ale instituţiilor de stat sînt insuficiente pentru pregătirea şi instruirea unor specialişti calificaţi, precum şi pentru stimularea acestora, fapt care determină migrarea specialiştilor în sectorul privat, cu repercusiuni asupra modului de implementare a securităţii 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 standarde. Prin urmare, acestea sînt, de asemenea, expuse unor riscuri de atacuri cibernetice prin exploatarea unor vulnerabilități.

**46.** La etapa actuală a progresului tehnologic şi a procesului de informatizare a vieţii economice, politice, sociale etc., funcţionarea mecanismelor principale ale statului se realizează prin utilizarea produselor program şi 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 L 345/75 din 23 decembrie 2008.

### *3.2. Componenta de securitate a spaţiului mediatic*

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

**48.** Conform prevederilor pct. 4.7 din Strategia securităţii naţionale a Republicii Moldova, aprobată prin Hotărîrea Parlamentului nr. 153/2011, securitatea informaţională a statului ţine şi de provocările cu caracter mediatic îndreptate împotriva Republicii Moldova sub formă de dezinformare şi/sau de informare 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 funcţie de anumite evoluții interne/externe, se mizează pe crearea unei stări de nemulțumire socială.

**51.** Necesitatea stringentă de a proteja securitatea spaţiului informaţional naţional este conștientizată și la nivelul autorităților administraţiei publice, dar și reprezintă un deziderat al societății civile.

**52.** Îngrijorarea privind intensificarea atacurilor din exterior la adresa securităţii informaţionale a fost enunţată inclusiv în Declaraţia Parlamentului Republicii Moldova privind condamnarea atacurilor provenite din Federaţia Rusă asupra securităţii informaţionale naţionale şi amestecul abuziv în activitatea politică din Republica Moldova, aprobată prin Hotărîrea Parlamentului nr. 12/2018, care stipulează că atacurile media din exterior vizează denigrarea Republicii Moldova, a unor instituţii şi a unor oficiali, dar cel mai grav este că vizează denigrarea cetăţenilor ţării.

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

**54.** Concomitent, subiectul este unul de actualitate atît la nivel internațional, cît și regional. În acest sens, prin Rezoluţia sa din 23 noiembrie 2016 referitoare la comunicarea strategică a Uniunii Europene pentru a contracara propaganda părţilor terţe împotriva sa (2016/2030 (INI)), Parlamentul European statuează că „UE, statele sale membre și cetățenii săi suportă o presiune crescîndă 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, difuzînd 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, independenţa şi integritatea teritorială, context în care statele membre ale UE şi partenerii acestora sînt încurajaţi să realizeze „evaluări critice ale modului în care ar trebui abordate sursele mass-media cu un trecut demonstrat de implicare repetată într-o strategie de 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 depăşesc cu mult capabilităţile de răspuns şi de combatere a fenomenului respectiv ale Republicii Moldova.

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

### *3.3. Componenta contrainformativă şi de securitate*

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

**60.** Potrivit Rezoluţiei Parlamentului European din 23 noiembrie 2016 referitoare la comunicarea strategică a Uniunii Europene pentru a contracara propaganda părţilor terţe 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 şi 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 şi agresiune mediatică, precum şi influența informațional-psihologică cu scopul de a destabiliza situația social-politică, a submina suveranitatea şi 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 şi grupuri separate de cetățeni finanțați de către centre subversive şi 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 şi 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 eficace de prevenire şi/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 şi nonstatali exploatează lipsa unui cadru juridic internațional în domenii 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 Convenţia Consiliului Europei privind criminalitatea informatică prin Legea nr. 6/2009. Totodată, a fost adoptată Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice și au fost operate modificări la Codul penal al Republicii Moldova nr. 985/2002 în corespundere cu prevederile Convenţiei ratificate. Cu toate acestea, nu au fost implementate integral multiple prevederi de ordin material și procesual, inclusiv cele ce ţin de dezvoltarea punctului de contact al reţelei 24/7.

**68.** Complementar, este de remarcat că, pînă în prezent, nu există un cadru legal privind delimitarea şi armonizarea competenţelor şi responsabilităţilor instituţiilor statului şi ale celor private în domeniul securităţii cibernetice, nu se aplică mecanismul obligatoriu de audit al securităţii cibernetice în cadrul instituţiilor publice şi private, prin care pot fi identificate vulnerabilităţile, riscurile şi ameninţările cibernetice în scopul prevenirii sau diminuării, prin măsuri speciale, a impactului atacurilor, incidentelor şi a altor evenimente survenite în spaţiul 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 corespondenţei”, nu prevede răspunderea penală pentru faptele comise în privința corespondenței (mesageriei) electronice, întrucît noțiunea „trimiteri poștale”, conform Legii comunicațiilor poștale nr. 36/2016, prevede numai bunurile fizice expediate și recepționate;

b) articolul $208^1$ din cod, „Pornografia infantilă”, nu incriminează obţinerea accesului cu bună ştiinţă, prin intermediul tehnologiilor informaţionale şi a comunicaţiilor, la pornografia infantilă, deși acest lucru este prevăzut în Convenția Consiliului Europei 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, „Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor”, au componență 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 Europei 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 restricţionarea accesului la paginile web, inclusiv cele găzduite de furnizorul respectiv, ce conţin informații care periclitează viața, sănătatea și dezvoltarea normală a copiilor, informaţii ce fac propagandă războiului sau terorismului, îndeamnă la ură sau discriminare naţională, rasială ori religioasă, la ostilitate sau violenţă.

**70.** De asemenea, se constată lipsa unui cadru normativ care ar reglementa infrastructura critică națională, precum și lipsa unei clasificări clare a sistemelor informaționale în funcţie de tipul datelor pe care acestea le conțin, de tipul de acces la acestea și de destinația acestora, lipsa unei definiri 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 definirii 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. Definirea problemelor de conştientizare a maselor*

**71.** La acest capitol se evidenţiază importanța sensibilizării publicului privind siguranța on-line, a educației și a competenței mediatice 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 acţiuni de consolidare a cunoștințelor la toate nivelurile sistemului educațional, cît şi impulsionarea/încurajarea persoanelor să devină cetățeni activi și să se conștientizeze în calitatea lor de consumatori de mass-media.

**74.** Un alt element de conştientizat 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 ştirilor false, pe parcursul anului 2017, a constituit obiectul şedinţelor Comisiei Europene, care a decis crearea unui Grup de lucru la nivel înalt care să elaboreze şi să prezinte o strategie de combatere a ştirilor false în 2018, cu un an înaintea alegerilor europene. Evaluările sale relevă că „contracararea propagandei prin propagandă este contraproductivă", statele membre UE fiind îndemnate să o combată doar prin demontarea campaniilor de dezinformare și prin utilizarea mesajelor și a informațiilor pozitive. În acest sens, experţii recomandă „dezvoltarea unei strategii eficace care să nu fie adaptată în funcție de natura actorilor care disemineză propaganda"[5].

## IV. VIZIUNE ȘI OBIECTIVE ALE STRATEGIEI

[5] Conform pct. 46 din Rezoluţia Parlamentului European din 23 noiembrie 2016 referitoare la comunicarea strategică a Uniunii Europene pentru a contracara propaganda părţilor terţe împotriva sa (2016/2030 (INI)).

**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-cibernetic și investigarea criminalității informatice

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

Obiectivul menţionat urmează a fi realizat prin următoarele 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 autorităţile publice competente şi persoanele fizice şi juridice;

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 naţional 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 cibernetice, sistematizarea datelor statistice la capitolul securității cibernetice, analiza și evaluarea acestora;

4) elaborarea mecanismelor de creare şi consolidare a centrelor departamentale de reacţie la incidente de securitate cibernetică și informațională, atît de drept public, cît și de drept privat;

5) elaborarea cadrului normativ pentru asigurarea unui nivel înalt de securitate a rețelelor și a sistemelor informatice la nivel național în baza bunelor practici 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 menţionat urmează a fi realizat prin următoarele acțiuni:

1) identificarea și eliminarea surselor de amenințare la adresa securităţii persoanei, a societăţii şi a statului în spaţiul cibernetic:

a) efectuarea auditului de securitate cibernetică a infrastructurilor de tehnologie a informației de interes naţional și a Sistemului de telecomunicații al autorităților administrației publice, precum și a altor infrastructuri cibernetice 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 direcţiilor de activitate prioritare pentru prevenirea şi suprimarea ameninţărilor respective;

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

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

5) coordonarea cu Centrul Naţional pentru Protecţia 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.

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

Obiectivul menţionat urmează a fi realizat prin următoarele acțiuni:

1) delimitarea şi atribuirea rolurilor şi a responsabilităţilor 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. Protecţia reţelelor de comunicaţii speciale ale Republicii Moldova şi a informaţiei cu accesibilitate limitată pentru menţinerea funcţiilor 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 şi utilizării mijloacelor de protecţie a informaţiei***

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

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

2) dezvoltarea sistemelor de monitorizare a importului mijloacelor de 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 menţionat 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 (atragerea 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 menţionat 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 şi 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 instituţiilor 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 menţionat 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 criminalităţii informatice;

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

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

**87.** ***Obiectivul nr. 10. Efectuarea unor cercetări ştiinţifice aplicative în domeniul securităţii informaţionale***

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 capacităţilor de rezilienţă cibernetică și ridicarea nivelului de cultură în domeniul TIC***

Obiectivul menţionat 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 cibernetice;

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 exerciţii și antrenamente comune de consolidare a capacităţilor 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 conţinuturi 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 informaţională;

2) dezvoltarea unor politici de comunicare strategică pe plan intern și racordarea la platformele de comunicare strategică externe ale structurilor sistemului de securitate, apărare şi 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 informaţională;

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

c) tentativele și acțiunile de dezinformare și/sau de informare manipulatorii ce afectează securitatea informaţională şi 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 organizaţiilor neguvernamentale şi a mass-mediei în domeniul securităţii informaționale, prin:

a) desemnarea unui consiliu existent sau crearea unui organ colectiv din rîndul societăţii civile cu atribuţii de evaluare a experților, a organizaţiilor neguvernamentale şi a mass-mediei din perspectiva implicării în materie de asigurare a securităţii informaţionale și naționale – Consiliul societăţii civile;

b) certificarea de către Consiliul societăţii civile a experţilor şi a reprezentanţilor societăţii civile şi ai mass-mediei ce se vor preocupa de monitorizarea nivelului de asigurare a securităţii informaţionale la nivel naţional;

2) implicarea reprezentanţilor societăţii civile certificaţi de către Consiliul societăţii civile în activitatea Consiliului coordonator pentru asigurarea securităţii informaţionale;

3) îmbunătăţirea sau crearea mecanismelor de implicare a societăţii civile în procesele de definire, de elaborare, de monitorizare şi de evaluare a politicilor de asigurare a securității informaționale realizate de către autoritățile abilitate în asigurarea securităţii informaţionale;

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 publicaţiilor periodice, al agenţiilor 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 implicaţi în producerea şi diseminarea conţinutului media on-line şi a altor intermediari şi serviciilor auxiliare ce au impact pentru securitatea informaţională;

2) elaborarea și ajustarea cadrului legal funcțional în scopul reglementării juridice a raporturilor dintre reprezentanții mass-media care colectează şi difuzează informaţii în Internet, societate și autoritățile cu atribuţii de asigurare a securităţii informaționale, în conformitate cu recomandările Comisiei Europene și bunele practici europene;

3) implementarea cadrului normativ care prevede acţiuni comune de intervenție și de gestionare a spațiului media on-line şi off-line.

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

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

1) elaborarea, sub egida Consiliului coordonator pentru asigurarea securităţii informaţionale, a criteriilor de calificare a informației ca produs de dezinformare, de manipulare sau de propagandă, orientat spre subminarea securităţii 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 priveşte analiza riscurilor și a amenințărilor din domeniul mass-mediei, cu scopul de a monitoriza evoluţia ameninţărilor depistate, de a investiga activitatea subversivă sau penală în spaţiul informaţional şi 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 publicaţiilor periodice, al agenţiilor de presă și al altor entități care activează în spațiul media din Internet | 2. Lege de modificare a 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 şi de răspuns la nivel naţional pentru asigurarea securităţii informaţionale***

Obiectivul menționat urmează a fi realizat prin următoarele acțiuni:

1) crearea, la nivel național, a entității cu competenţe de promovare şi coordonare a politicilor de securitate informaţională într-o societate democratică în funcţie de dezvoltarea tehnologiei, raporturile juridice şi de altă natură din sectorul informațional, atît la nivel național cît şi internaţional (Consiliul coordonator pentru asigurarea securităţii informaţionale):

a) identificarea și integrarea componentelor existente cu funcții și atribuții în domeniul cibernetic și mediatic, a autorităţilor administraţiei 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 securităţii informaţionale în funcţie de atribuțiile și funcțiile deţinute din perspectiva asigurării securităţii informaţionale;

c) elaborarea şi adoptarea cadrului normativ de interacţiune pentru realizarea sarcinilor de depistare, prevenire şi contracarare a riscurilor şi a ameninţărilor la adresa securităţii informaţionale;

2) elaborarea, promovarea şi coordonarea politicilor de securitate informaţională în conformitate cu Concepţia, cu prezenta Strategie şi cu alte documente de politici de nivel naţional şi internaţional ce se referă la societatea informaţională;

3) informarea publicului privind modalitățile de prevenire și contracarare a riscurilor și a ameninţărilor la adresa componentelor sistemice ale securităţii 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 operaţionale de interacţiune între autorităţile responsabile şi factorii de decizie în cazul unor ameninţări hibride de securitate;

4) consolidarea gradului de cunoaştere şi înţelegere a concepţiei ameninţărilor hibride de securitate la nivelul organelor abilitate cu asigurarea securităţii informaţionale şi 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 Hibride și Centrul de Excelenţă pentru Comunicare Strategică al NATO.

**95.** ***Obiectivul nr. 3. Dezvoltarea competențelor operaţionale de apărare cibernetică***

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) crearea în cadrul Forțelor Armate a entităţii 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 şi contracararea factorilor de risc cu potenţial informativ-subversiv la adresa apărării cibernetice a Republicii Moldova prin implementarea unui management integrat al spaţiului virtual și dezvoltarea unui sistem de avertizare timpurie cu privire la elementele de risc la adresa obiectivelor de infrastructură.

**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 răspîndirii 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 instituţiilor statului cu competenţe în domeniu către Serviciul de Informaţii şi Securitate a informaţiilor 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 securităţii informaţionale***

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

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

2) identificarea categoriilor de beneficiari care urmează să fie incluşi cu prioritate în programele noi de instruire a resurselor umane în domeniul securităţii informaţionale;

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

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

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

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

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

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

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

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

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

1) evaluarea nivelului actual al cooperării dintre Republica Moldova și organizaţiile internaţionale ce îşi desfăşoară activitatea în domeniul asigurării securităţii informaţionale şi elaborarea unor acţiuni privind intensificarea cooperării respective;

2) stabilirea cooperării dintre Republica Moldova și statele partenere, în special cele din cadrul Uniunii Europene, privind schimbul de informaţii, experienţe şi analize în scopul prevenirii, depistării şi contracarării ameninţărilor hibride la adresa securității în spaţiul informaţional;

3) promovarea pe plan internaţional, inclusiv în cadru bilateral, a necesităţii de a încheia acorduri ce ar unifica conceptul de „armă informaţională”, interzicînd elaborarea, răspîndirea şi aplicarea acesteia în relaţiile dintre state;

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

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

Obiectivul în cauză urmează a fi realizat prin următoarele acțiuni:

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

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

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

**103.** ***Obiectivul nr. 5. Consolidarea cooperării internaţionale 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 şi confiscării produselor şi a instrumentelor provenite din infracţiunile 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 internaționale în domeniul apărării cibernetice | 2. Cadrul legal de cooperare negociat și încheiat |
| 3. Stabilirea mecanismelor de cooperare internațională între autoritățile statului cu atribuții în combaterea criminalității informatice și organismele internaționale pe segmentul asigurării securității informaționale | 3. Runde de consultări; acorduri bilaterale/multilaterale semnate și încheiate |

## V. ESTIMAREA IMPACTULUI ŞI 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 cetăţenilor la prelucrarea datelor acestora;

2) protejarea şi promovarea democraţiei participative şi pluraliste;

3) dezvoltarea societății informaționale naţionale, sub toate aspectele structurale şi funcţionale, 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 orînduirii constituționale;

7) dezvoltarea mecanismelor de combatere colectivă a ameninţărilor hibride de securitate ce periclitează securitatea informaţională şi 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 şi a platformelor de informare on-line şi 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 situaţia 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/subiecţilor din spaţiul informaţional al Internetului.

**106.** În scopul obținerii rezultatelor trasate la pct. 105, este necesar, întîi 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 acţiuni pentru implementarea prezentei Strategii generează riscul divulgării unor date clasificate, fapt ce impune definitivarea, în mod individual, la nivelul autorităţilor/instituțiilor, a sumelor necesare pentru fiecare an bugetar şi reglementarea acestora prin actele normative care urmează a fi elaborate în contextul Strategiei.

## VI. REZULTATELE SCONTATE ȘI 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 soluţii tehnice speciale de sporire a fiabilităţii reţelelor comunicaţionale în cazuri critice;

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

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

4) vor fi dezvoltate capacităţile naţionale necesare efectuării unui schimb securizat şi stocării informaţiilor, transmiterii prompte şi eficiente a fluxului de informaţii, inclusiv a celor clasificate, pe plan intern şi extern, în cazul unor crize ori situaţii excepţionale;

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

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

7) vor fi stabilite garanții specifice pentru a proteja cît 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 atribuţii consultative şi operaţionale, ce va fi responsabil și va asigura integrarea sistemică a componentelor spațiului informațional şi susţinerea unui nivel înalt de securitate informaţională.

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

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

b) *Palierul mediatic,* care va fi constituit din reprezentanţi ai spaţiului mediatic naţional, în special din reprezentanţi ai mass-mediei tradiţionale (posturi radio, posturi TV şi presa scrisă), dar şi ai media din Internet, incluși în funcţie de caracterul politicilor editoriale ce vor avea drept preocupări procesele ce ţin de asigurarea securităţii spaţiului mediatic;

c) *Palierul operaţional*, care va fi format în special din reprezentanţi ai autorităţilor publice cu atribuţii şi competenţe în materie de apărare, informații, contrainformații, investigații şi procesuală, conform prerogativelor acestora de asigurare a securităţii spaţiului informaţional;

d) *Palierul civic-privat*, care va fi constituit din reprezentanţi ai societăţii civile, potrivit recomandărilor Consiliului societăţii civile, ai asociaţiilor ce reprezintă sectorul IT naţional, ai companiilor de drept privat din domeniul IT, precum şi din experţi internaţionali din rîndul partenerilor strategici actuali şi de perspectivă ai Republicii Moldova, specializaţi în consolidarea dimensiunii de securitate cibernetică şi informaţională la nivel regional, european şi internaţional.

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

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

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

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

6) Serviciul de Informaţii şi Securitate va avea calitatea de coordonator al activităţii Consiliului coordonator pentru asigurarea securității informaționale, fiind responsabil de recepţionarea sesizărilor de incidente de securitate informaţională şi prezentarea 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 însoţit de monitorizarea permanentă a realizării acţiunilor propuse şi a rezultatelor obţinute, fiind operate, în caz de necesitate, modificările de rigoare în politicile publice promovate de Guvern în contextul prezentei Strategii.

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

**116.** Ministerele, instituţiile şi alte autorităţi administrative centrale vor asigura întreprinderea măsurilor necesare în vederea realizării integrale, în termenele stabilite și conform competenţelor ce le sînt atribuite, a acţiunilor incluse în Planul de acţiuni pentru implementarea prezentei Strategii.