GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din 2025

Chișinău

Cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026-2030

În temeiul art. 6 alin. (3) din Legea nr. 48/2023 privind securitatea cibernetică (Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225), Guvernul HOTĂRĂŞTE:

1. Se aprobă Programul național de securitate cibernetică pentru anii 2026-2030 (se anexează).

2. Autoritățile și instituțiile publice responsabile:

2.1. vor realiza acțiunile prevăzute în Planul de acțiuni privind implementarea Programului național de securitate cibernetică pentru anii 2026-2030;

2.2. vor prezenta Ministerului Dezvoltării Economice și Digitalizării semestrial, până la data de 20 ianuarie și, respectiv, până la 20 iulie, precum și la solicitare rapoarte privind gradul de realizare a acțiunilor incluse în Planul de acțiuni nominalizat.

3. Ministerul Dezvoltării Economice și Digitalizării va prezenta Guvernului semestrial, până la data de 1 martie, raportul de progres privind implementarea Programului național de securitate cibernetică pentru anii 2026-2030, prin intermediul Sistemului informațional „e-Monitorizare”.

4. Finanțarea acțiunilor prevăzute în Programul național de securitate cibernetică pentru anii 2026-2030 se va efectua din contul și în limitele alocațiilor aprobate în acest scop în bugetele autorităților/instituțiilor implicate, precum și din alte surse, conform legislației.

5. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Dezvoltării Economice și Digitalizării.

6. Prezenta hotărâre intră în vigoare la data de 1 ianuarie 2026.

Prim-ministru **ALEXANDRU MUNTEANU**

Contrasemnează:

Viceprim-ministru,
ministrul dezvoltării
economice și digitalizării Eugeniu OSMOCHESCU

Aprobat
prin Hotărârea Guvernului nr. /2025

PROGRAM NAȚIONAL
de securitate cibernetică pentru anii 2026-2030

Capitolul I
INTRODUCERE

1. Programul național de securitate cibernetică pentru anii 2026-2030 (în continuare – *Program*) este un document de politici publice care stabilește un set de obiective și acțiuni pe termen mediu menite să asigure dezvoltarea, implementarea și aplicarea unor măsuri digitale sigure, securizate și reziliente, printr-o abordare multilaterală. Programul stabilește obiective și priorități menite să consolideze întregul ecosistem digital național. El promovează o abordare integrată a securității cibernetice, și nu una limitată la sectoare sau riscuri izolate. În cadrul acestui ecosistem, mediul academic are un rol esențial în formare, cercetare aplicată și transfer de cunoaștere.

2. Prezentul Program este elaborat în conformitate cu Obiectivele de Dezvoltare Durabilă (în continuare – *ODD*) ale Organizației Națiunilor Unite și contribuie indirect la realizarea acestora. În mod particular, Programul susține următoarele ODD și țintele lor naționale, reflectate în Hotărârea Guvernului nr. 953/2022 cu privire la aprobarea cadrului național de monitorizare a implementării Agendei de Dezvoltare Durabilă 2030:

2.1. ODD 9 – Construirea unor infrastructuri reziliente, promovarea industrializării durabile și încurajarea inovației:

2.1.1. Ținta 9.c – Creșterea semnificativă a accesului la tehnologia informației și comunicațiilor (TIC) și promovarea accesului universal la internet până în 2030;

2.2. ODD 4 – Asigurarea unei educații de calitate și promovarea oportunităților de învățare de-a lungul vieții pentru toți:

2.2.1. Ținta 4.b – Extinderea semnificativă, până în 2030, a numărului de burse pentru învățământul superior, inclusiv în domeniul TIC, inginerie și științe;

2.3. ODD 17 – Consolidarea mijloacelor de implementare și revitalizarea parteneriatului global pentru dezvoltare durabilă:

2.3.1. Ținta 17.8 – Operaționalizarea completă a băncii de tehnologii și a mecanismului de consolidare a capacităților în domeniile științei, tehnologiei și inovației, inclusiv prin sporirea utilizării TIC.

3. Prezentul Program va contribui nu doar la protejarea infrastructurii digitale a Republicii Moldova, ci și la dezvoltarea durabilă, prin consolidarea

economiei digitale, protecția drepturilor cetățenilor și promovarea cooperării internaționale, în concordanță cu Agenda 2030.

4. Totodată, prezentul Program răspunde priorității privind consolidarea securității cibernetice și a infrastructurii IT critice, stabilită în Programul de activitate al Guvernului „UE, pace, dezvoltare”, aprobat prin Hotărârea Parlamentului nr. 269/2025.

5. Prezentul Program este aliniat cu 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, care prevede priorități privind prevenirea și combaterea criminalității, inclusiv a criminalității informatice.

6. De asemenea, prezentul Program contribuie la implementarea direcției prioritare din Strategia națională de dezvoltare „Moldova Europeană 2030”, aprobată prin Legea nr. 315/2022:

6.1. transformarea electronică a guvernării, societății și economiei:

6.1.1. consolidarea infrastructurii de securitate cibernetică și a infrastructurii critice de date, asigurarea confidențialității datelor personale;

6.1.2. consolidarea și adaptarea programelor de studii avansate în domeniul securității cibernetice și al investigării infracțiunilor cibernetice.

7. În ceea ce privește corelarea cu documentele de politici și de planificare în vigoare, prezentul Program se aliniază cu următoarele:

7.1. *Strategia securității naționale a Republicii Moldova*, aprobată prin Hotărârea Parlamentului nr. 391/2023, direcția: Securitatea și reziliența cibernetică, care include:

7.1.1. cooperarea public-privată în domeniul securității cibernetice;

7.1.2. modernizarea sistemelor IT și introducerea standardelor europene în verificarea biometrică;

7.1.3. dezvoltarea planurilor de securitate și apărare cibernetică a infrastructurii și entităților critice naționale;

7.1.4. educație în igiena cibernetică;

7.1.5. exerciții naționale de securitate cibernetică;

7.1.6. consolidarea dialogului și a cooperării în domeniul cibernetic cu Uniunea Europeană;

7.1.7. alinierea la normele Uniunii Europene privind tehnologiile transformative;

7.2. *Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030*, aprobată prin Hotărârea Guvernului nr. 650/2023, obiectivul general 5 – Crearea unui mediu digital accesibil, sigur și incluziv:

7.2.1. instituirea unei autorități naționale competente în domeniul securității cibernetice;

7.2.2. măsuri de raportare obligatorie a incidentelor și consolidarea infrastructurii digitale critice;

7.2.3. aplicarea standardelor de securitate în achiziții IT;

7.2.4. dezvoltarea competențelor resurselor umane;

7.3. *Strategia națională de apărare a Republicii Moldova pentru anii 2024-2034*, aprobată prin Hotărârea Parlamentului nr. 319/2024, direcția 29.7 – Consolidarea protecției spațiului cibernetic:

7.3.1. asigurarea rezilienței entităților critice;

7.3.2. consolidarea capacităților Forțelor Armate în securitatea cibernetică;

7.3.3. cooperarea națională și internațională;

7.4. *Strategia de dezvoltare „Educația 2030”* și *Programul de implementare a acesteia pentru anii 2023-2025,* aprobate prin Hotărârea Guvernului nr. 114/2023:

7.4.1. asigurarea creșterii nivelului de alfabetizare digitală și integrare socială a cetățenilor;

7.5. *Strategia de dezvoltare a domeniului afacerilor interne pentru anii 2022-2030*, aprobată prin Hotărârea Guvernului nr. 658/2022:

7.5.1. consolidarea serviciilor TIC și a securității informaționale;

7.5.2. creșterea gradului de conștientizare a riscurilor cibernetice în rândul populației;

7.6. *Programul național de prevenire și de combatere a criminalității pentru anii 2026-2030*, aprobat prin Hotărârea Guvernului nr. 654/2025:

7.6.1. dezvoltarea capacităților instituționale de combatere a criminalității informatice prin utilizarea tehnologiilor digitale prin ajustarea cadrului legal, implementarea unor mecanisme și sisteme moderne de investigare;

7.6.2. colectarea eficientă a datelor privind incidentele de securitate cibernetică;

7.6.3. campanii de sensibilizare a populației, inclusiv a copiilor;

7.7. *Programul național pentru digitalizare și inovare în sănătate pe anii 2025-2030*, aprobat prin Hotărârea Guvernului nr. 556/2025:

7.7.1. asigurarea securității cibernetice pentru Dosarul Electronic de Sănătate (DES) și pentru sistemele informaționale/registrele medicale naționale;

7.7.2. crearea unui mecanism de protecție a datelor medicale și de gestionare a consimțământului informat, în conformitate cu Regulamentul (UE) 2025/327 privind Spațiul European al Datelor de Sănătate (EHDS);

7.7.3. consolidarea rezilienței instituțiilor medicale în fața atacurilor cibernetice și instruirea personalului medical în domeniul securității digitale;

7.8. *Programul de transformare digitală a domeniului energetic al Republicii Moldova pentru anii 2026-2030*, aprobat prin Hotărârea Guvernului nr. 652/2025:

7.8.1. fortificarea capacităților de securitate cibernetică în domeniul energetic până în anul 2030;

7.8.2. asigurarea monitorizării 24/7 a infrastructurii critice energetice prin consolidarea capacităților de securitate cibernetică ale operatorilor de infrastructură energetică, inclusiv prin implementarea de mecanisme moderne de detectare și răspuns rapid, în conformitate cu cerințele naționale și directivele Uniunii Europene (inclusiv Directiva NIS2);

7.8.3. asigurarea certificării tuturor operatorilor de infrastructură critică energetică conform standardelor ISO/IEC 27001 și cerințelor Directivei NIS2;

7.8.4. asigurarea reducerii timpului de recuperare după incidente cibernetice cu impact semnificativ la maximum patru ore pentru serviciile critice;

7.9. *Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029*, aprobat prin Hotărârea Guvernului nr. 306/2025:

7.9.1. subcapitolul 10.5. Servicii de încredere și securitate cibernetică;

7.9.2. subcapitolul 24.1.5. Prevenirea și combaterea criminalității informatice;

7.10. *Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale*.

8. De asemenea, prezentul Program răspunde acțiunilor stabilite în Planul național de reglementări pentru anul 2025, aprobat prin Hotărârea Guvernului nr. 841/2024, care prevede elaborarea și aprobarea până în noiembrie 2025 a unui document strategic în domeniul securității cibernetice. Toate acestea sunt corelate cu Legea nr. 48/2023 privind securitatea cibernetică, care prevede obligativitatea aprobării unui document de politici în domeniul securității cibernetice.

9. Suplimentar, la elaborarea proiectului prezentului Program și, implicit, a Planului de acțiuni privind implementarea acestuia, s-au luat în considerare prevederile Comunicării Comune către Parlamentul European și Consiliu „Strategia de securitate cibernetică a UE pentru deceniul digital”.

10. Totodată, pe fondul intensificării amenințărilor cibernetice la nivel global și european, Republica Moldova se confruntă cu o nevoie acută de consolidare a capacităților naționale de securitate cibernetică. Datele din perioada 2018-2024 demonstrează o creștere constantă a numărului de incidente cibernetice semnificative raportate în Uniunea Europeană, din care aproape o treime au fost acțiuni rău-intenționate, cu un impact major asupra sectoarelor critice precum comunicațiile, sănătatea, energia și transporturile. În acest context, Republica Moldova, în pofida eforturilor recente de aliniere la standardele europene, rămâne vulnerabilă la atacuri cibernetice, care pot afecta stabilitatea națională, infrastructurile critice naționale și încrederea populației în serviciile digitale.

11. Transformarea digitală accelerată a economiei Republicii Moldova, cu un sector IT care contribuie semnificativ la produsul intern brut (în continuare – *PIB*) și la exporturi, implică nu doar oportunități, ci și expuneri crescute la riscuri cibernetice. Estimările privind pierderile economice cauzate de criminalitatea cibernetică arată că prejudiciul anual pentru Republica Moldova este de circa 49 de milioane de dolari SUA, o cifră semnificativă raportată la dimensiunea economiei naționale. În plus, Indicele global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor evidențiază deficiențe semnificative în măsurile tehnice și în dezvoltarea capacităților, iar lipsa unui mecanism funcțional de gestionare a crizelor cibernetice expune țara la riscuri suplimentare în cazul unui atac de amploare.

12. Toate aceste aspecte relevă necesitatea stringentă de a elabora și de a aproba prezentul Program. Programul definește obiectivele strategice, măsurile de politică şi cele de reglementare, cu scopul atingerii și menținerii unui nivel înalt de securitate a rețelelor și sistemelor informatice, și va permite consolidarea capacității naționale de prevenire, detectare, reacție și recuperare în fața incidentelor cibernetice. Programul urmărește, de asemenea, asigurarea implementării legislației armonizate cu acquis-ul Uniunii Europene, dezvoltarea și punerea în aplicare a unui mecanism eficient de gestionare a crizelor cibernetice, stimularea cooperării internaționale și încurajarea participării sectorului privat și a societății civile în asigurarea unui spațiu digital sigur și rezilient.

13. În ceea ce privește apărarea cibernetică, care ține de competența Ministerului Apărării și a entităților subordonate acestuia, prezentul Program nu intervine direct asupra acestui segment, ci urmărește doar corelarea obiectivelor și a acțiunilor propuse cu obiectivele Strategiei naționale de apărare a Republicii Moldova pentru anii 2024-2034.

14. Prin prezentul Program, Republica Moldova își va consolida poziția în procesul de integrare europeană, va proteja mai eficient interesele cetățenilor, va asigura funcționarea neîntreruptă a serviciilor esențiale și va susține dezvoltarea economică bazată pe digitalizare și inovație.

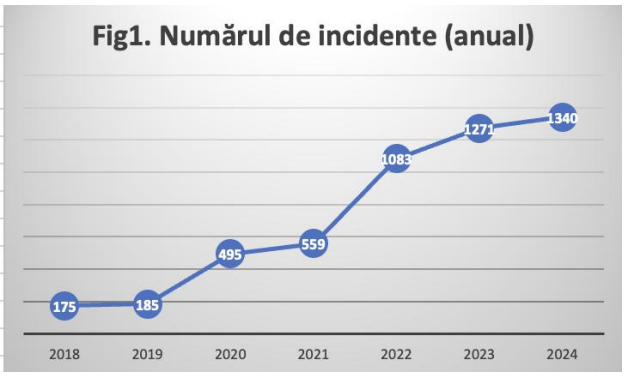
15. În ceea ce privește elaborarea prezentului Program, autoritățile și instituțiile publice indicate la capitolul VII au contribuit, în limitele competențelor, la procesul de elaborare și consultare inițiat de Ministerul Dezvoltării Economice și Digitalizării. Aceste autorități au furnizat perspective sectoriale esențiale pentru consolidarea rezilienței cibernetice, în special în sectoarele care gestionează infrastructura critică națională.

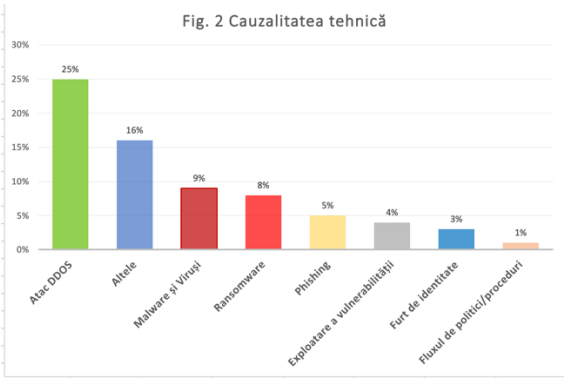
Capitolul II
ANALIZA SITUAȚIEI

16. Digitalizarea a fost motorul dezvoltării economice în ultimele decenii, asigurând o interconectare globală tot mai mare și reducând barierele în relațiile dintre țări. În perioade de turbulențe geopolitice, această interdependență digitală poate duce la provocări majore. În plus, digitalizarea exponențială a generat oportunități mai mari pentru actorii răuvoitori și a crescut suprafața totală de atac, iar această amenințare nu va face decât să crească în viitor, pe măsură ce tehnologiile digitale vor continua să se dezvolte. În fiecare zi, securitatea națională, întreprinderile și mediul online sigur pentru persoane fizice sunt amenințate de actori statali și criminali.

17. Între 2018 și 2024, statele membre ale Uniunii Europene au raportat un total de 3 251 de incidente cibernetice cu impact semnificativ, conform criteriilor stabilite de Directiva NIS1, Codul european al comunicațiilor electronice și Regulamentul eIDAS, din care 29 % au fost considerate acțiuni rău-intenționate. Cel mai afectat sector a fost sectorul privat, în special următoarele domenii: comunicațiile, bancar, sănătate, servicii de încredere, transporturi și energie.

18. Datele indică o tendință generală de creștere a numărului de incidente cu impact semnificativ (figura 1). Din cele 1 402 incidente rău-intenționate raportate, majoritatea au fost clasificate ca infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în figura 2.





Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică

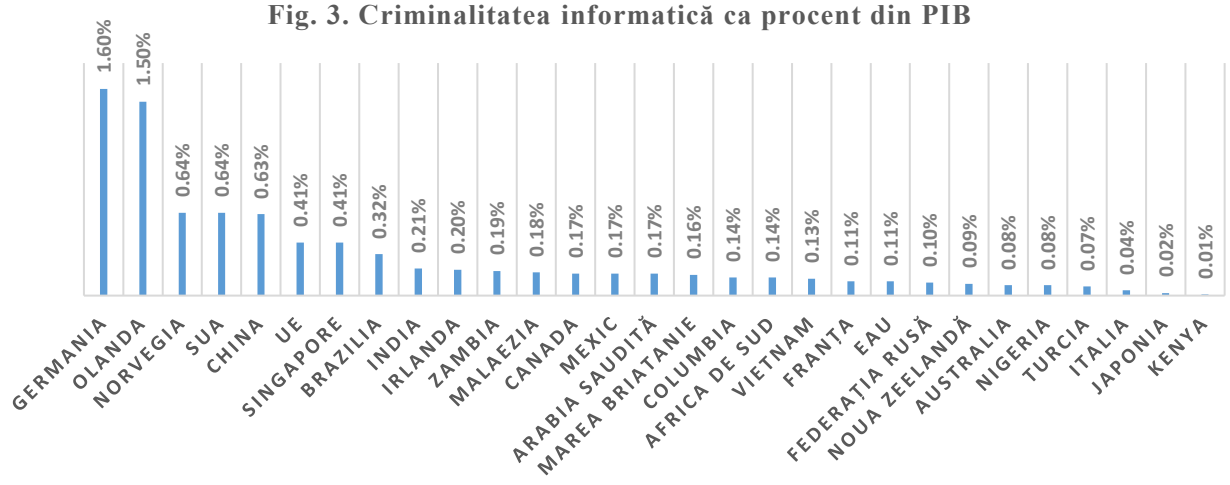
19. În absența unei intervenții guvernamentale coordonate și a consolidării capacităților instituționale în domeniul securității cibernetice, se anticipează o creștere constantă a numărului de incidente cibernetice. Datele istorice indică o tendință ascendentă semnificativă, de la 173 de cazuri raportate în 2018 la peste 1 340 în anul 2024. Conform proiecțiilor bazate pe evoluțiile recente, până în anul 2030 numărul anual de incidente ar putea depăși pragul de 2 000, reflectând o dublare a volumului actual al atacurilor. Această evoluție ar amplifica

vulnerabilitățile infrastructurilor critice naționale, ar afecta continuitatea serviciilor publice digitale și ar reduce încrederea cetățenilor și a mediului de afaceri în utilizarea serviciilor electronice. Tendința confirmă necesitatea intervenției statului prin politici și măsuri coordonate, orientate spre creșterea rezilienței cibernetice naționale.

20. Conform raportului actualizat al International Business Machines privind costul unei încălcări a securității datelor în 2024, impactul financiar al încălcărilor securității datelor este și mai mare pentru entitățile critice. Raportul indică faptul că în 2024 costul mediu global al unei încălcări a securității datelor a atins un nivel record de 4,88 milioane de dolari SUA, înregistrând o creștere de 10 % față de 2023.

21. Studiul global realizat de compania McAfee, care a evaluat pierderile economice cauzate de criminalitatea informatică, intitulat „Pierderi nete: estimarea costului global al criminalității informatice", oferă o estimare a impactului economic al criminalității informatice pentru diferite țări, exprimat ca procent din PIB. Graficul prezentat în figura 3 evidențiază țările cel mai grav afectate în funcție de proporția daunelor monetizate în raport cu PIB-ul lor. În medie, pierderile cauzate de criminalitatea cibernetică reprezintă aproximativ 0,3 % din PIB. Extrapolând aceste date pentru Republica Moldova, având în vedere că PIB-ul țării a fost de aproximativ 16,5 miliarde de dolari SUA în 2023, se poate estima un prejudiciu anual potențial de aproximativ 49 de milioane de dolari, pe baza mediei de 0,3 % din PIB.

Fig. 3. Criminalitatea informatică ca procent din PIB



Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică

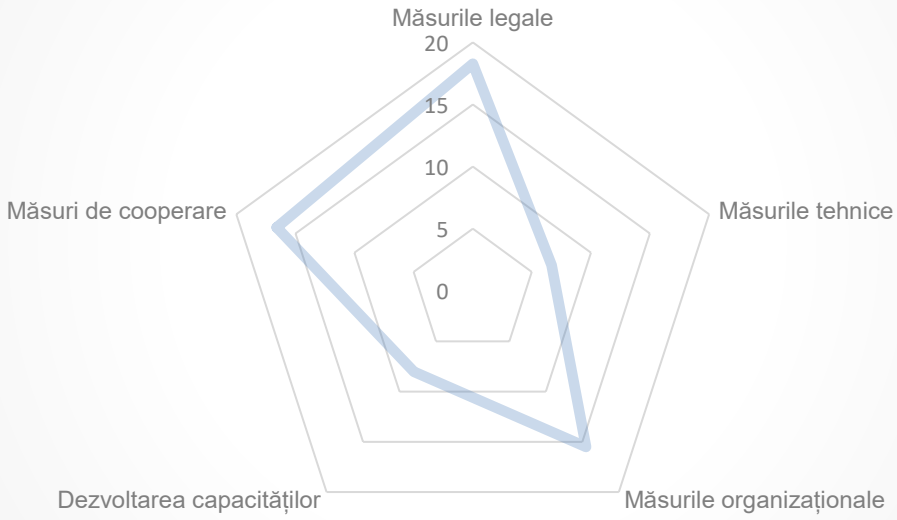
22. În Republica Moldova, fenomenul criminalității organizate a evoluat semnificativ în ultima perioadă, reflectând o tendință de adaptare și diversificare a activităților infracționale. Numărul infracțiunilor comise de grupuri criminale a crescut de peste patru ori, de la 201 cazuri în 2022 la 205 cazuri în 2023 și până la 889 în 2024, ceea ce indică o escaladare alarmantă a criminalității organizate

online. În ceea ce privește criminalitatea informatică, în 2024 au fost inițiate 135 de dosare penale pentru comiterea de infracțiuni informatice și infracțiuni în domeniul comunicațiilor electronice, comparativ cu 167 de dosare inițiate în 2023. Cele mai frecvente infracțiuni comise în mediul online sunt infracțiunile care vizează activele financiare ale cetățenilor.

23. În 2024, Academia de e-Guvernare (Estonia) și Magenta Consulting au realizat un sondaj de opinie online privind conștientizarea siguranței online în Republica Moldova. Șaptezeci și șapte de procente dintre respondenții acestui sondaj consideră că oricine poate deveni victimă a fraudei online, a atacurilor cibernetice sau a criminalității cibernetice. „Furtul de identitate” este termenul cel mai cunoscut, 53 % dintre respondenți fiind familiarizați cu acesta, ceea ce indică o înțelegere largă a acestei forme de criminalitate cibernetică. Cu toate acestea, „cyberbullying” are un nivel de recunoaștere mai scăzut, doar 27 % dintre respondenți fiind familiarizați cu acest termen. „Phishing” este cunoscut de 19 % dintre respondenți, ceea ce sugerează că acest termen poate fi mai puțin înțeles în comparație cu altele. În cele din urmă, „ransomware” are cel mai scăzut nivel de familiarizare, unul din zece respondenți recunoscând termenul (10 %).

24. Conform Indicelui global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor pentru 2024, Republica Moldova are un scor general de 65,09, iar performanța țării este descrisă ca fiind de nivelul 3 (nivelul 3 reprezintă țările care au obținut un scor general de cel puțin 55/100), demonstrând un angajament de bază în materie de securitate cibernetică, care include evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate, pe un număr moderat de piloni sau indicatori. Conform raportului Uniunii Internaționale a Telecomunicațiilor privind echipa națională de răspuns la incidente de securitate cibernetică, performanța Republicii Moldova pentru 2024, comparativ cu 2020, a înregistrat o creștere în ceea ce privește măsurile legale, organizaționale și de cooperare și o scădere notabilă în ceea ce privește măsurile tehnice și de dezvoltare a capacităților, dar acest lucru poate fi atribuit parțial ajustărilor metodologice și ponderilor Indicelui global al securității cibernetice, precum și modificărilor aduse întrebărilor. Graficul de mai jos (figura 4) evidențiază performanța Republicii Moldova în Indicele global al securității cibernetice pentru 2024, subliniind că măsurile tehnice și consolidarea capacităților sunt punctele slabe ale țării în acest domeniu. Cu toate acestea, indicele în cauză poate fi îmbunătățit prin implementarea corespunzătoare a legislației naționale armonizate cu legislația Uniunii Europene.

Fig. 4. Performanța Republicii Moldova în Indicele golbal al securității cibernetice pentru 2024



Sursa: Uniunea Internațională a Telecomunicațiilor

25. Industria tehnologiei informației în Republica Moldova se dezvoltă rapid. În 2023, industria tehnologiei informației a atins o pondere de peste 5,3 % din PIB, depășind 15 miliarde de lei în vânzări, ponderea sectorului TIC este de peste 8,3 % din PIB, cu peste 25 de miliarde de lei în vânzări în 2023, realizate de aproximativ 3 200 de companii cu peste 35 000 de angajați.

26. În același timp, Strategia securității naționale a Republicii Moldova evidențiază riscurile cibernetice la care este expusă Republica Moldova, subliniind în principal atacurile cinetice sau cibernetice lansate de actori statali externi asupra infrastructurii critice naționale și regionale, atacurile cibernetice lansate asupra instituțiilor publice sau private de către structuri specializate în criminalitatea cibernetică, precum și riscurile asociate evoluțiilor din domeniul tehnologiilor precum blockchain și criptomonede, inteligența artificială, învățarea automată, internetul obiectelor, tehnologia 5G, big data, tehnologiile cuantice, internetul ascuns.

27. Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 acordă prioritate punerii în aplicare a Legii nr. 48/2023 privind securitatea cibernetică, în special identificării furnizorilor de servicii critice și punerii în aplicare a cerințelor de securitate pentru rețele și sisteme informatice, precum și operaționalizării complete a Agenției pentru Securitate Cibernetică. În acest sens, recent a fost aprobată Hotărârea Guvernului nr. 562/2025 cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în sectoarele critice, care include în obiectul său de reglementare și cerințele de securitate pentru rețele și sisteme

informatice. Este necesară consolidarea capacităților furnizorilor de servicii din sectoarele critice pentru a aplica corect cerințele de securitate cibernetică. Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 prevede transpunerea Actului privind reziliența cibernetică, care impune producătorilor și comercianților cu amănuntul, începând cu sfârșitul anului 2027, să asigure securitatea cibernetică pe tot parcursul ciclului de viață al produselor lor. Procesul de certificare a securității cibernetice în Uniunea Europeană este încă în curs de elaborare și se află în faza de pilotare, prin urmare nu reprezintă o prioritate pentru această perioadă de programare. Cu toate acestea, Agenția pentru Securitate Cibernetică joacă un rol important în orientarea și sprijinirea tuturor proceselor menționate în Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, ceea ce impune suplimentar necesitatea consolidării capacității operaționale a Agenției. În prezent, Agenția pentru Securitate Cibernetică se află în proces de angajare de personal (20 de persoane angajate din 45 planificate).

28. Implementarea setului de instrumente al Uniunii Europene pentru securitatea 5G acoperă diverse aspecte, precum evaluarea riscurilor, cerințele de securitate, securitatea lanțului de aprovizionare, implementarea sigură și răspunsul la incidente.

29. Modelul organizațional actual de securitate cibernetică în Republica Moldova este reprezentat de autorități și instituții publice aflate în structura administrativă a Guvernului sau în afara acesteia, cu un spectru divers de responsabilități cu incidență pe întregul eșichier de realizare a politicii de stat în domeniul securității cibernetice.

30. Consiliul Național de Securitate, în conformitate cu Legea nr. 249/2025 privind securitatea națională a Republicii Moldova, este un organ de coordonare între autoritățile și instituțiile publice, având drept scop analizarea amenințărilor, riscurilor, pericolelor și vulnerabilităților la adresa securității statului, apărării naționale și ordinii și securității publice, formularea de propuneri și adoptarea de decizii pentru identificarea, prevenirea, gestionarea și contracararea acestora, precum și consultarea Președintelui Republicii Moldova în domeniile vizate de politica de securitate națională.

31. Consiliul coordonator în domeniul securității cibernetice a fost înființat prin Hotărârea Guvernului nr. 333/2024 cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice. Acest organism acționează ca un mecanism strategic de coordonare în domeniul securității cibernetice. El examinează și formulează opinii asupra politicilor publice pentru a asigura coerența, complementaritatea și alinierea acestora la obiectivele strategice, propune îmbunătățiri legislative și coordonează procesul de

elaborare și actualizare a planului național de răspuns la incidente și crize cibernetice, sprijinind autoritatea competentă și facilitând cooperarea între părțile implicate. Totodată, contribuie la consolidarea coordonării interinstituționale și oferă recomandări privind subiectele emergente din domeniu, sprijinind reacția eficientă a autorităților la provocările actuale și viitoare.

32. Ministerul Dezvoltării Economice și Digitalizării este autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul tehnologiei informației, societății informaționale, economiei digitale, securității cibernetice și guvernanței internetului. De asemenea, este autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul comunicațiilor electronice, inclusiv de elaborarea, coordonarea și monitorizarea politicilor privind gestionarea domeniului de nivel superior .md, precum și de asigurarea evaluării conformității echipamentelor de comunicații electronice.

33. Agenția pentru Securitate Cibernetică este autoritatea publică în subordinea Ministerului Dezvoltării Economice și Digitalizării care are rolul de a identifica și de a ține evidența furnizorilor de servicii din sectoarele și subsectoarele critice, de a supraveghea și de a controla respectarea cadrului normativ de către aceștia, precum și de a emite acte obligatorii, recomandări și îndrumări metodologice pentru asigurarea conformității. Agenția exercită funcția de punct unic de contact la nivel național și de echipă națională de răspuns la incidente cibernetice, monitorizând amenințările, vulnerabilitățile și incidentele, gestionând crizele și acordând asistență tehnică furnizorilor de servicii. Ea facilitează cooperarea și schimbul de informații la nivel național și internațional, coordonează procesul de divulgare coordonată a vulnerabilităților, elaborează planuri, orientări metodologice, promovează bunele practici, sprijină cercetarea și dezvoltarea în domeniu și asigură protecția informațiilor sensibile.

34. Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică, în care Cancelaria de Stat exercită funcția de fondator, administrează, întreține și dezvoltă infrastructura informatică, sistemul de telecomunicații al autorităților administrației publice ca parte a rețelei speciale de comunicații și sistemele informaționale de stat, gestionează infrastructura cheilor publice a Guvernului, precum și administrează centrele de date din sectorul public. Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică exercită funcție de CERT-Gov, echipă de răspuns la incidente cibernetice în sectorul public, adică echipă responsabilă numai pentru rețele și sisteme informatice de stat.

35. Instituția Publică Agenția de Guvernare Electronică, în care Cancelaria de Stat exercită calitatea de fondator, este responsabilă pentru implementarea politicilor în domeniile de modernizare a serviciilor guvernamentale și

transformare digitală a guvernării, gestionează platforme și servicii electronice guvernamentale (MConnect, MPass, MSign, MPay etc). De asemenea, are responsabilități ce țin de asigurarea securității informației în autoritățile și instituțiile din sectorul public în procesul de e-Transformare a guvernării. Împreună cu partenerii săi, Instituția Publică Agenția de Guvernare Electronică ia măsuri juridice, organizatorice și tehnice complexe de garantare a securității informațiilor. Conform regulamentului său de activitate, principalele responsabilități ale Agenției în domeniul securității cibernetice sunt auditul securității cibernetice în sectorul public, inclusiv monitorizarea implementării rezultatelor auditului securității cibernetice, cercetarea securității cibernetice, precum și supravegherea instituțiilor publice în ceea ce privește implementarea cerințelor minime de securitate.

36. Instituția Publică Centrul de Tehnologii Informaționale în Finanțe, în care Ministerul Finanțelor exercită calitatea de fondator, are rolul de dezvoltator și administrator al sistemelor informaționale pentru autorități publice în domeniile: finanțe publice, achiziții publice, fiscal și vamal.

37. Serviciul de Informații și Securitate al Republicii Moldova are un rol important în protejarea infrastructurii critice naționale și a sistemelor speciale de telecomunicații. În calitate de serviciu de inteligență, Serviciul de Informații și Securitate este responsabil pentru asigurarea securității naționale atât per general, cât și în domeniul securității cibernetice în special. În acest context, se realizează acțiuni de prevenire, identificare, investigare și contracarare a activităților de spionaj cibernetic, sabotaj cibernetic, precum și a activităților malițioase ale actorilor cibernetici statali. De asemenea, Serviciul de Informații și Securitate este responsabil de autorizarea sistemelor informatice care prelucrează informația atribuită la secret de stat. Serviciul de Informații și Securitate informează autoritățile naționale privind amenințările cibernetice din spațiul cibernetic național și regional.

38. Centrul pentru combaterea crimelor cibernetice al Inspectoratului Național de Investigații al Inspectoratului General al Poliției al Ministerului Afacerilor Interne este unitatea principală de investigare și prevenire a infracțiunilor informatice și a celor conexe, precum și a infracțiunilor grave, deosebit de grave și excepțional de grave cu rezonanță socială sporită, comise prin intermediul sistemelor informatice, prin organizarea activității speciale de investigații. Centrul acordă suport și asistență subdiviziunilor teritoriale ale poliției în materie de criminalitate cibernetică și dovezi electronice. Centrul are un acord bilateral cu CERT-GOV pentru schimbul de informații privind incidentele cibernetice. De asemenea, Centrul cooperează cu Serviciul de Informații și Securitate și îi oferă, la solicitare, informații despre situația din spațiul cibernetic național.

39. Procuratura Generală, în cadrul căreia este instituită și funcționează Secția combatere crime cibernetice, contribuie la implementarea politicii naționale şi internaționale a statului în domeniul investigării criminalităţii informatice, coordonează, conduce şi exercită urmărirea penală, reprezintă învinuirea în instanţele de judecată şi asigură cooperarea juridică internaţională în conformitate cu standardele stabilite de Convenţia Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, precum şi de alte acte internaţionale la care Republica Moldova este parte.

40. Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației este autoritatea publică centrală care reglementează activitatea în comunicațiile electronice, tehnologia informației și comunicațiile poștale, asigură implementarea strategiilor de dezvoltare în aceste sectoare și supraveghează conformitatea furnizorilor de comunicații electronice și de servicii poștale cu legislația care reglementează aceste sectoare. Modul de organizare și funcționare a Agenției Naționale pentru Reglementare în Comunicații Electronice și Tehnologia Informației este stabilit de Guvern. Cu toate acestea, Agenția este autonomă față de Guvern în activitatea sa de reglementare.

41. Ministerul Apărării și Armata Națională a Republicii Moldova au propriile capacități defensive și echipă de răspuns la incidente cibernetice (CERT militar) pentru a-și proteja propriile rețele.

42. Ministerul Energiei este autoritatea cu responsabilități sectoriale în domeniul securității cibernetice pentru infrastructura critică energetică.

43. Instituţia Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”) este responsabilă de formarea profesională continuă a personalului din sectorul public și privat prin programe specializate în domeniul securității cibernetice, precum și de dezvoltarea proiectelor de cercetare și a soluțiilor inovatoare pentru protecția infrastructurilor critice naționale și a datelor personale. Totodată, elaborează ghiduri și bune practici în domeniu, stabilește parteneriate cu mediul academic, sectorul privat și organizații internaționale, pentru implementarea accelerată a standardelor de securitate cibernetică.

44. Centrul Național de Management al Crizelor este autoritatea administrativă centrală din subordinea Guvernului care coordonează, la nivel național, ansamblul activităților de management al crizelor în domeniile de prevenire, pregătire, răspuns și recuperare după crize și crize majore.

45. Republica Moldova nu dispune în prezent de un cadru clar pentru gestionarea crizelor în domeniul securității cibernetice. Pe măsură ce amenințările evoluează, gestionarea incidentelor cibernetice la scară largă și a crizelor cibernetice este abordată din ce în ce mai mult de Uniunea Europeană. Astfel cum este definit în Directiva (UE) 2022/2555 (Directiva NIS 2), un incident de securitate cibernetică la scară largă este un incident care provoacă un nivel de perturbare care depășește capacitatea unui stat membru de a răspunde la acesta sau care are un impact semnificativ asupra a cel puțin două state membre. Un astfel de incident, în funcție de cauza și impactul său, poate escalada și se poate transforma într-o criză de proporții care afectează buna funcționare a pieței interne sau prezintă riscuri grave pentru securitatea publică și siguranța entităților sau a cetățenilor din mai multe state membre sau din Uniunea Europeană în ansamblu. În acest sens, Comisia Europeană a aprobat Recomandarea 2017/1584 din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare.

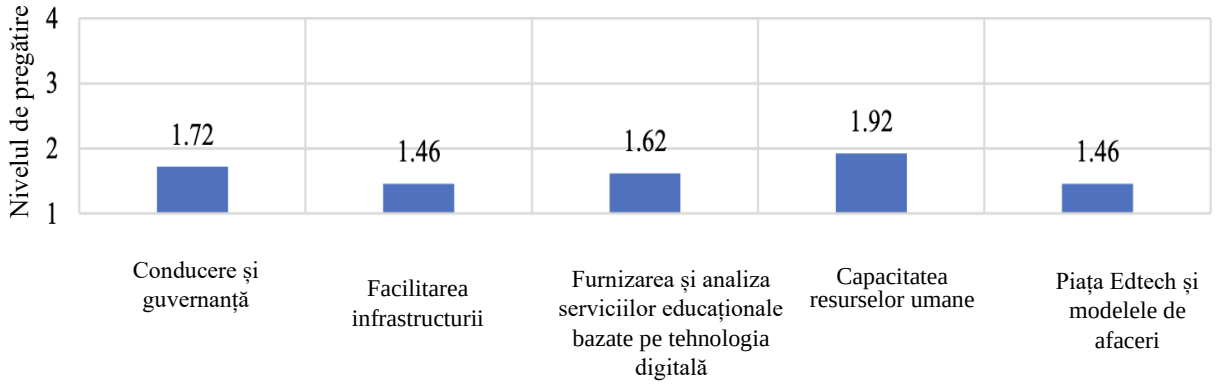
46. Crearea unui cadru de gestionare a crizelor de securitate cibernetică este o sarcină complexă pentru state. În lumea de astăzi, un atac cibernetic la scară largă poate amplifica o criză de securitate deja existentă, precum și poate provoca întreruperea pe termen lung a serviciilor esențiale, distrugerea datelor importante sau alte consecințe grave, ceea ce duce la pagube mari și pune în pericol securitatea statului și a societății. Din cauza escaladării rapide și a complexității crizelor cibernetice, rezolvarea acestora necesită un mecanism bine pregătit și fiabil, care să fie bine integrat cu resursele generale de gestionare a crizelor ale statului și să aibă, de asemenea, o capacitate foarte bună de cooperare internațională.

47. Consolidarea rezilienței digitale este strâns legată de investițiile în cercetare, inovare și capital uman. Acestea joacă un rol esențial în generarea unei creșteri economice inteligente și durabile și în crearea de locuri de muncă. Conform Strategiei de dezvoltare „Educația 2030” și Programului de implementare a acesteia pentru anii 2023-2025, finanțarea activităților de cercetare și inovare în Republica Moldova pe cap de locuitor se ridică la aproximativ 6,6 euro, fiind de 80 de ori mai mică decât media europeană. Legătura slabă dintre comunitatea științifică și mediul de afaceri împiedică implementarea rezultatelor cercetării, aplicarea noilor tehnologii de către mediul de afaceri, stimularea dezvoltării economice și crearea de locuri de muncă.

48. Dezvoltarea competențelor digitale reprezintă, de asemenea, o prioritate în cadrul Strategiei de dezvoltare „Educația 2030” și al Programului de implementare a acesteia pentru anii 2023-2025. În 2022, Banca Mondială a evaluat cinci domenii ale pregătirii digitale a sistemului de învățământ din Republica Moldova, concluzionând că aceasta se află la nivel „emergent” – investițiile fundamentale au progresat, dar multe probleme rămân nerezolvate (figura 5). În

prezent, o parte integrantă a competențelor digitale o constituie cunoștințele în domeniul securității cibernetice. Strategia abordează lipsa generală de profesori și manageri calificați, bine pregătiți și motivați, dar și alte provocări, precum progresul lent în promovarea noilor mijloace de comunicare, a resurselor deschise și a tehnologiilor în educație, inclusiv aplicarea ineficientă a TIC în educație. Investițiile limitate în formarea profesorilor și, în continuare, în dezvoltarea specialiștilor IT, împreună cu emigrarea lucrătorilor calificați, creează o lipsă permanentă pe piața muncii din domeniul IT și reduce posibilitățile de lansare a unor noi întreprinderi avansate din punct de vedere digital. De asemenea, este abordată dezvoltarea oportunităților de învățare pe tot parcursul vieții pentru toți cetățenii.

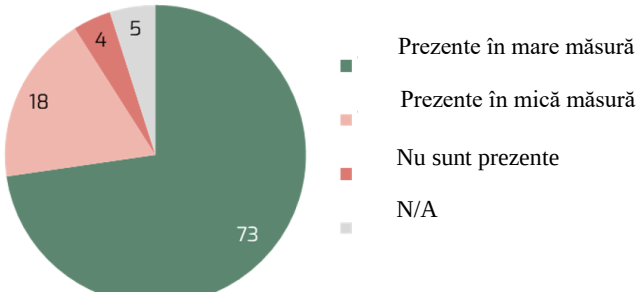
Fig. 5. Evaluarea pregătirii pentru educația digitală 2021-2022 în Republica Moldova



Sursa: Banca Mondială

49. Conform sondajului privind conștientizarea siguranței online în Republica Moldova, realizat în 2023, se evidențiază importanța abordării problemelor de securitate online, întrucât smartphone-urile sunt cele mai răspândite dispozitive personale în gospodării. Aproape jumătate dintre respondenți utilizează smartphone-urile pentru sarcini legate de muncă. Jumătate dintre cei chestionați păstrează confidențialitatea telefoanelor lor mobile, în timp ce o treime au menționat că și alte persoane ar putea avea acces la informațiile lor. O mai bună conștientizare a amenințărilor hibride actuale este esențială pentru cetățeni, întrucât 73 % dintre respondenții sondajului consideră că manipularea, propaganda și dezinformarea sunt prezente în mare măsură în conținutul postat pe rețelele de socializare (figura 6).

Fig. 6. Răspunsuri la întrebarea „În ce măsură credeți că manipularea, propaganda și dezinformarea sunt prezente în conținutul postat pe rețelele de socializare?”



Sursa: Academia de e-Guvernare (Estonia) și Magenta Consulting

50. În concluzie, Republica Moldova se confruntă cu multiple provocări în domeniul securității cibernetice, dintre care se evidențiază următoarele:

50.1. creșterea numărului de atacuri cibernetice – atacurile asupra entităților publice și private s-au intensificat, punând în pericol infrastructurile critice naționale și datele cetățenilor;

50.2. creșterea criminalității cibernetice – criminalitatea cibernetică, inclusiv frauda online, atacurile ransomware și furtul de identitate s-au intensificat. Grupurile infracționale folosesc metode din ce în ce mai sofisticate pentru a exploata vulnerabilitățile digitale, afectând atât instituțiile, cât și cetățenii;

50.3. provocări geopolitice și riscuri hibride – Republica Moldova este expusă la campanii de dezinformare, atacuri asupra infrastructurilor IT și alte acțiuni care vizează destabilizarea securității naționale;

50.4. capacitate instituțională limitată – autoritățile publice cu responsabilități în domeniul securității cibernetice nu dispun de expertiză și resurse suficiente pentru a face față amenințărilor emergente;

50.5. lipsa de conștientizare și educație în materie de securitate cibernetică – atât sectorul public, cât și cel privat, precum și populația în general au nevoie de o mai mare instruire și conștientizare a riscurilor și a măsurilor de protecție;

50.6. lipsa unui ecosistem public-privat de colaborare – sectorul privat nu este pe deplin integrat în mecanismele naționale de securitate cibernetică, iar cooperarea dintre instituțiile guvernamentale și companiile de tehnologie este insuficientă;

50.7. securitatea cibernetică a infrastructurilor critice naționale – sistemele energetice, financiare, de sănătate și de transport necesită măsuri urgente de protecție împotriva amenințărilor cibernetice sofisticate;

50.8. cooperare internațională insuficientă – deși Republica Moldova a început procesul de integrare în inițiativele internaționale de securitate cibernetică, nivelul de colaborare cu partenerii externi trebuie să fie extins și consolidat. Schimbul de informații, alinierea la standardele internaționale și participarea activă la platformele de securitate cibernetică sunt esențiale pentru creșterea capacității naționale de protecție;

50.9. fragmentare și soluții digitale învechite – soluțiile digitale existente se află la niveluri diferite de maturitate tehnică și securitate, au interoperabilitate limitată și sunt dependente de tehnologii legacy.

51. Ca răspuns la aceste provocări, prezentul Program prevede patru domenii principale de intervenție (figura 7):

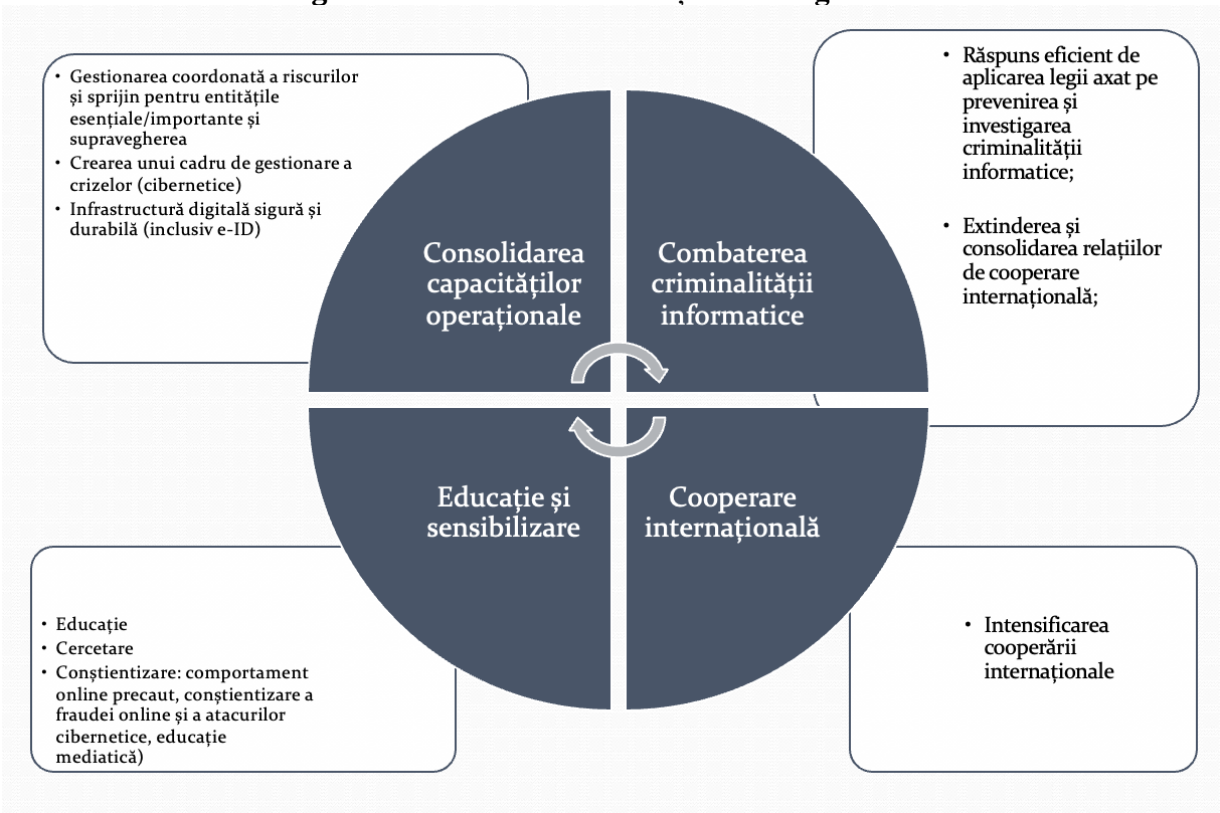
51.1.consolidarea capacităților operaționale;

51.2.combaterea criminalității informatice;

51.3.educație și sensibilizare;

51.4.cooperare internațională.

Fig. 7. Domeniile de intervenție ale Programului



Domeniul de intervenție I – consolidarea capacităților operaționale

52. În ultimii ani, Republica Moldova a dezvoltat un cadru strategic, normativ și organizațional pentru protecția spațiului său cibernetic și asigurarea securității rețelelor și a sistemelor informatice, în vederea creșterii nivelului de reziliență cibernetică. Următorul pas este consolidarea capacităților operaționale ale țării pentru implementarea cadrului creat. Prezentul Program se concentrează pe stabilirea unor acțiuni practice pentru prevenirea și soluționarea incidentelor cibernetice, pe minimizarea impactului, prin reducerea consecințelor și asigurarea recuperării rapide și restabilirea continuității serviciilor esențiale, precum și pe reducerea riscurilor asociate utilizării rețelelor și sistemelor informatice la furnizarea serviciilor esențiale.

53. Este necesară sprijinirea autorităților și a instituțiilor publice responsabile de securitatea cibernetică în înțelegerea amenințărilor, monitorizarea și evaluarea acestora. Practica de a învăța din incidentele din spațiul cibernetic este încă în dezvoltare, de aceea capacitățile acestor organizații de a răspunde, de a recupera și de a învăța rapid și eficient din incidente și crize cibernetice necesită suport. Guvernul va investi în resurse umane și sisteme care să ofere o imagine clară asupra originii amenințărilor și a țintelor acestora.

54. Procedurile de raportare și gestionare a incidentelor sunt încă la un stadiu incipient. Este necesară instituirea unui cadru interinstituțional mai bine structurat și funcțional, care să includă toți actorii relevanți, pentru a asigura un răspuns eficient și coordonat la atacurile cibernetice. În anul 2022 a fost aprobat Conceptul Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică” (Hotărârea Guvernului nr. 388/2022), iar Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică trebuie să acționeze ca punct unic de contact pentru autoritățile și instituțiile publice în raportarea incidentelor cibernetice. În primăvara anului 2025, un sondaj realizat de Ministerul Dezvoltării Economice și Digitalizării printre autoritățile publice a arătat că raportarea incidentelor nu este o practică comună. Totodată, Registrul de stat al incidentelor de securitate cibernetică nu este încă unul funcțional. Astfel, lipsește o imagine bazată pe date reale privind situația din spațiul cibernetic al Republicii Moldova, în special în sectorul public, ceea ce îngreunează planificarea protecției. Un obiectiv strategic al prezentului Program este ca organizațiile guvernamentale, care au echipe de răspuns la incidentele cibernetice, și autoritățile de supraveghere să inițieze un schimb de informații eficient atât despre incidentele înregistrate, cât și despre amenințări și vulnerabilități, asumându-și pe deplin responsabilitatea de a sprijini entitățile care intră în domeniul lor de competență în detectarea și răspunsul la incidente cibernetice.

55. Managementul coordonat și integrat al riscurilor la nivel organizațional, sectorial și național este încă la început. Riscurile cibernetice nu au încă un loc bine definit în cadrul general de management al riscurilor. Abordarea bazată pe risc, prevăzută în Legea nr. 48/2023 privind securitatea cibernetică, trebuie să joace un rol esențial în determinarea și atingerea nivelului dorit de reziliență. Autoritățile publice cu funcții de supraveghere din Republica Moldova trebuie să furnizeze materiale metodologice pentru a sprijini furnizorii de servicii în sectoarele critice să înțeleagă și să implementeze corect cadrul normativ și măsurile de securitate. Sprijinirea acestor entități în implementarea cerințelor legii este un obiectiv principal al prezentului Program.

56. Lipsa unui mecanism integrat de gestionare a crizelor în domeniul securității cibernetice și dezvoltarea unui mecanism național integrat de gestionare

a crizelor, în conformitate cu Strategia securității naționale a Republicii Moldova, oferă oportunitatea de a crea un mecanism robust și eficient de gestionare a crizelor cibernetice. Pe data de 10 iulie 2025, Parlamentul a adoptat Legea nr. 248/2025 privind managementul situațiilor de criză, care stabilește cadrul juridic, organizatoric (funcțional și instituțional), operațional și de coordonare a gestionării crizelor în Republica Moldova. În acest context, un obiectiv pentru perioada următoare este instituirea unui proces de gestionare a crizelor cibernetice, integrat în sistemul național de gestionare a crizelor și pregătit pentru integrarea în cadrul Uniunii Europene. Comunicarea în timpul crizelor este esențială pentru răspunsul eficient la incidente cibernetice. Furnizarea de informații veridice și la timp menține încrederea publicului și reduce posibilele prejudicii de reputație. Exercițiile naționale periodice de gestionare a crizelor cibernetice și participarea activă la exerciții internaționale reprezintă instrumente importante pentru creșterea gradului de pregătire.

57. Republica Moldova, care și-a stabilit transformarea digitală ca prioritate strategică, își propune un efort coordonat al sectorului public și privat pentru a oferi infrastructuri digitale sigure și durabile. Identitatea digitală este unul dintre elementele fundamentale. Fără posibilitatea de identificare și de interacționare online în siguranță, transformarea digitală nu poate fi completă. În anul 2024, serviciul electronic guvernamental de autentificare și control al accesului (MPass) a fost utilizat de peste 20 de milioane de ori de către aproximativ 200 000 de utilizatori, iar serviciul electronic guvernamental integrat de semnătură electronică (MSign) a fost folosit pentru peste 53 de milioane de semnături electronice de către peste 180 000 de utilizatori. Printre realizările recente se numără lansarea aplicației mobile integrate EVO și introducerea noii cărți electronice de identitate (eID). Prin asigurarea interoperabilității și a recunoașterii legale a identificării electronice și a serviciilor de încredere în întreaga Uniune Europeană, armonizarea cu Regulamentul eIDAS trebuie să fie o prioritate.

58. Obținerea unei imagini precise a situației securității cibernetice, inclusiv în ceea ce privește amenințările, incidentele și impactul acestora, este esențială. În acest scop, trebuie să fie dezvoltate capacitatea de identificare și analiză a amenințărilor cibernetice, precum și capacitatea centralizată de raportare și gestionare a incidentelor la nivel național.

59. Printre problemele-cheie în acest domeniu se numără următoarele:

59.1. lipsa unei capacități consolidate de cooperare internațională și participarea insuficientă la formate internaționale pentru schimbul de informații privind securitatea cibernetică limitează accesul Republicii Moldova la informații esențiale despre riscuri și amenințări;

59.2. deficiențele în colectarea, raportarea, înregistrarea și analiza centralizată a incidentelor cibernetice împiedică obținerea unei imagini clare

asupra situației naționale, atât la nivel operațional, cât și la nivel strategic. Lipsa unei evidențe complete a incidentelor de criminalitate informatică afectează dezvoltarea de măsuri preventive eficiente și întârzie investigarea, urmărirea penală și soluționarea acestora.

Domeniul de intervenție II – combaterea criminalității informatice

60. Criminalitatea informatică (cibernetică) a apărut ca una dintre principalele probleme ale societăților de astăzi, provocând pierderi economice directe și indirecte semnificative și subminând încrederea în funcționarea întregului ecosistem digital, a guvernului, a economiei și a societății. Combinată cu operațiunile de criminalitate cibernetică sponsorizate de stat, este o amenințare în creștere, care necesită o intervenție din ce în ce mai decisivă și la scară largă a statului și cooperare internațională în majoritatea țărilor. Criminalitatea cibernetică, inițiată atât de grupurile de crimă organizată, cât și de actorii criminali sponsorizați de stat, poate reprezenta o amenințare iminentă nu numai pentru sentimentul de securitate al societății și al cetățenilor, ci și pentru securitatea națională. Odată rezervate actorilor statului-națiune, tacticile cibernetice avansate și persistente sunt acum comune în rândul infractorilor cibernetici, făcându-le la fel de devastatoare în contextul amenințărilor de astăzi.

61. Strategia securității naționale a Republicii Moldova recunoaște atacurile cibernetice lansate de actori statali străini asupra infrastructurii critice naționale și regionale și atacurile cibernetice lansate asupra entităților publice sau private de către structurile specializate în criminalitate informatică ca o amenințare la adresa securității Republicii Moldova. Pentru a îmbunătăți lupta împotriva criminalității informatice, Republica Moldova trebuie să stabilească un răspuns mai eficient de aplicare a legii, axat pe detectarea și trasabilitatea datelor privind criminalitatea informatică și urmărirea penală a infractorilor cibernetici.

62. În 2025, Republica Moldova se confruntă cu mai multe provocări semnificative în combaterea criminalității cibernetice, influențată de tensiunile geopolitice, limitările infrastructurale și evoluția amenințărilor digitale.

63. Conform studiului „World Cybercrime Index”, publicat în aprilie 2024, Republica Moldova se situează pe locul 15 la nivel mondial (din 97 de țări analizate) în clasamentul percepției experților internaționali privind sursele de activitate infracțională cibernetică. Această poziționare, îngrijorătoare prin asocierea cu statele implicate în generarea sau facilitarea atacurilor informatice, evidențiază atât utilizarea teritoriului național ca bază operațională pentru grupări infracționale transnaționale, cât și vulnerabilități structurale în sistemele de prevenire, investigare și combatere a criminalității cibernetice.

64. Principalele amenințări legate de criminalitatea cibernetică pentru Republica Moldova sunt:

64.1. amenințări cibernetice sponsorizate de stat și atacuri hibride – Republica Moldova a fost supusă unor atacuri cibernetice asociate cu actori străini, în special din Federația Rusă. Aceste atacuri urmăresc să perturbe operațiunile guvernamentale și să erodeze încrederea publică, mai ales în timpul evenimentelor critice precum alegerile. În 2024, serverele de e-mail ale Parlamentului Republicii Moldova au fost compromise înaintea alegerilor prezidențiale și a referendumului de aderare la Uniunea Europeană, evidențiind vulnerabilitățile operațiunilor cibernetice motivate politic;

64.2. ransomware și fraudă online – Republica Moldova a înregistrat o creștere a incidentelor ransomware și a fraudei online care vizează atât entitățile publice, cât și întreprinderile private. Un caz recent semnificativ a implicat arestarea unui suspect care ar avea legătură cu atac ransomware de 4,5 milioane de euro asupra Organizației Olandeze pentru Cercetare Științifică, demonstrând rolul Republicii Moldova în investigațiile internaționale privind criminalitatea cibernetică;

64.3. atacuri cibernetice asupra infrastructurii critice naționale – infrastructura critică națională, inclusiv sistemele de sănătate și de salarizare guvernamentale, a fost ținta unor atacuri cibernetice menite să submineze încrederea publicului în serviciile publice furnizate de organizațiile de stat. Aceste atacuri au determinat Guvernul să îmbunătățească măsurile de securitate cibernetică pentru a proteja interesele naționale. Crima organizată destabilizează progresiv societatea, deoarece apare din ce în ce mai mult online și este puternic accelerată de inteligența artificială și alte tehnologii noi;

64.4. insuficiența personalului calificat în securitatea cibernetică pe întregul ciclu de prevenire, investigare, urmărire și judecare a faptelor ilegale comise în spațiul cibernetic – Republica Moldova se confruntă cu un deficit semnificativ de expertiză în securitate cibernetică în domeniul criminalității cibernetice, exacerbat de fenomenul „exodului de creiere”, profesioniștii calificați căutând oportunități în străinătate. Acest deficit împiedică dezvoltarea și implementarea unor strategii eficiente de apărare cibernetică;

64.5. provocări în materie de securitate cibernetică pentru întreprinderile mici și mijlocii – întreprinderile mici și mijlocii, care constituie peste 97 % din companiile Republicii Moldova, sunt deosebit de vulnerabile la amenințările cibernetice. Conștientizarea redusă și resursele limitate fac dificilă implementarea unor măsuri adecvate de securitate cibernetică, prezentând riscuri pentru ecosistemul economic mai larg.

65. Dezvoltarea și promovarea cooperării internaționale pentru combaterea criminalității informatice a fost una dintre prioritățile operaționale ale țării. Republica Moldova este parte la Convenția de la Budapesta și a fost activă în mai multe parteneriate internaționale, precum:

65.1. colaborarea cu Consiliul Europei: Republica Moldova se implică activ în inițiativele Consiliului Europei precum CyberEast și GLACY+, concentrându-se pe consolidarea capacităților și alinierea legislativă la Convenția de la Budapesta;

65.2. sprijinul Uniunii Europene: Proiectul „EU4Security Moldova” își propune să sporească capacitățile de aplicare a legii în domeniul securității cibernetice. Printre evoluțiile recente se numără inaugurarea unui laborator cibernetic la Chișinău pentru a sprijini investigațiile digitale;

65.3. cooperare bilaterală: în ianuarie 2025, Republica Moldova și Țările de Jos au desfășurat primul lor dialog cibernetic bilateral, concentrându-se pe amenințările hibride, securitatea cibernetică și criminalitatea cibernetică. Dialogul a pus accentul pe consultări între agenții și schimbul de cunoștințe.

66. De asemenea, autoritățile naționale au fost active în colaborarea internațională în domeniul aplicării legii, prin formatele Interpol, precum și în operațiuni comune cu agențiile internaționale de aplicare a legii. Prin aceste eforturi concertate, Republica Moldova și-a consolidat poziția în lupta globală împotriva criminalității informatice, promovând reziliența și aliniindu-se la cele mai bune practici internaționale.

67. Programul de prevenire și combatere a criminalității pentru anii 2022-2025 a abordat o serie de probleme de criminalitate informatică, concentrându-se pe crearea și facilitarea accesului la instrumente și mecanisme adecvate în combaterea și prevenirea criminalității informatice. Programul recunoaște lupta împotriva crimei organizate prin aprofundarea cooperării cu statele membre ale Uniunii Europene și instituțiile relevante. Aceste probleme continuă a fi abordate și în Programul național de prevenire și de combatere a criminalității pentru anii 2026-2030, care conține o serie de măsuri pentru soluționarea acestora.

Domeniul de intervenție III – educație și sensibilizare

68. Acest domeniu de intervenție se concentrează pe oamenii din spatele tehnologiei și pe reziliența cibernetică a publicului. Abordarea la nivelul întregii societăți va fi utilizată la dezvoltarea competențelor digitale, de la cunoștințe și competențe de bază la expertiză la nivel înalt și competențe specializate în securitate cibernetică. Conștientizarea sectorului public și privat, a societății civile și a publicului larg pentru a se putea proteja împotriva amenințărilor cibernetice este în continuare limitată în Republica Moldova. În mod similar, există încă prea puține cunoștințe aprofundate de securitate cibernetică. Prin urmare, accentul trebuie să fie pus pe consolidarea capacităților și proiectarea viitoarelor programe de educație și formare pentru a aborda deficitul de personal specializat în securitate cibernetică.

69. Scopul Strategiei naționale de dezvoltare „Moldova Europeană 2030” în domeniul educației este de a oferi oportunități tuturor de a-și dezvolta abilitățile și competențele necesare de-a lungul vieții de la o vârstă fragedă. Aceasta urmărește să îmbunătățească educația, să promoveze învățarea pe tot parcursul vieții și să coreleze competențele dobândite în instituțiile de învățământ formal cu cele dezvoltate în contexte nonformale și informale. Competențele digitale, inclusiv securitatea cibernetică, sunt vitale în toate sectoarele economiei moderne. Acestea oferă un acces mai bun la locuri de muncă bine plătite și ajută la gestionarea informațiilor și la luarea deciziilor în cunoștință de cauză. În ultimii ani au fost implementate numeroase inițiative și modificări legislative în educație, cu scopul de a asigura o educație de calitate, echitabilă și incluzivă și de a oferi oportunități de învățare pe tot parcursul vieții pentru toți.

70. Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030 acordă prioritate dezvoltării competențelor digitale. În timp ce în anii trecuți proporția instituțiilor cu acces la internet și computere în scopuri pedagogice a ajuns la 100 %, îmbunătățirea calității educației și dezvoltarea competențelor digitale ale elevilor este încă o provocare. Eforturile continue de dezvoltare și promovare a educației în securitate cibernetică sunt importante pentru a răspunde cerințelor și oportunităților din sectorul tehnologic și pentru a pregăti specialiști competenți și calificați în acest domeniu în Republica Moldova. Asigurarea resurselor adecvate și a unor programe de învățământ actualizate în domeniul securității cibernetice, precum și sprijinirea formării inițiale și continue a specialiștilor pot contribui la îmbunătățirea calității educației în acest domeniu.

71. Activitățile de igienă cibernetică și siguranță online au mai mult succes dacă sunt gestionate strategic pe termen lung de o gamă largă de parteneri și părți interesate. Asigurarea igienei cibernetice într-o țară nu este responsabilitatea unui minister sau a unei agenții, ci este o problemă pe care părțile interesate din sectorul public și privat, organizațiile societății civile și mediul academic trebuie să o abordeze și să contribuie la activități preventive atunci când reacționează la atacuri cibernetice sau escrocherii. Prin urmare, promovarea colaborării intersectoriale și regionale în schimbul de cunoștințe și experiențe este esențială, în acest sens fiind încă necesar un punct de contact comun în sectorul public, prin care să poată fi organizate dezvoltarea și diseminarea de campanii universale de înaltă calitate și materiale de sensibilizare. Intervențiile de comunicare sunt cele mai eficiente atunci când se bazează pe datele din incidente și situații din spațiul cibernetic național. Prin urmare, Agenția pentru Securitate Cibernetică și Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică sunt cele mai indicate să creeze mecanisme și platforme de comunicare pentru a asigura realizarea acestor imperative.

72. Din 2023, campania „Siguranța Digitală” este implementată de Academia de e-Guvernare (Estonia) în cooperare cu parteneri locali. Campania face parte dintr-o misiune mai amplă de creștere a gradului de conștientizare cu privire la siguranța online și de oferire a abilităților printr-un curs online. Cu toate acestea, inițiativele în cauză au fost la scară mică și, în scopul exercitării responsabilităților, Agenția pentru Securitate Cibernetică trebuie să își consolideze rolul central de proiectare și coordonare a activităților de consolidare a capacităților, de sensibilizare și de formare în domeniul securității cibernetice, în comun cu furnizorii de servicii în sectoarele critice, mediul academic, societatea civilă și alte părți interesate. În plus, cunoștințele privind siguranța online vor fi îmbunătățite semnificativ dacă un număr mare de părți interesate, atât din sectorul public, cât și din cel privat, precum și din societatea civilă, sporesc și se implică activ în comunicarea periodică online privind siguranța cu clienții și părțile interesate, precum și în oricare campanii de conștientizare.

73. Schimbarea gradului de conștientizare a subiectelor legate de siguranța online și securitatea cibernetică ar trebui evaluată în mod sistematic, inclusiv pentru a determina impactul activităților de comunicare la scară largă, cum ar fi campaniile. Prin urmare, este necesar să se inițieze evaluări periodice, în dinamică și structurate în acest domeniu.

74. Unul dintre domeniile cel mai afectate care are mult de câștigat din cooperarea oportună și anticipată între părțile interesate din sectorul public și privat îl constituie alegerile. Pe de o parte, rezultatele alegerilor depind de conștientizarea de către alegători a recunoașterii dezinformării. Potrivit sondajului privind conștientizarea siguranței online în Republica Moldova realizat în 2023, 73 % dintre respondenți consideră că manipularea, propaganda și dezinformarea sunt prezente în mare măsură în conținutul postat pe rețelele de socializare. Pe de altă parte, rolul jurnaliștilor și al organizațiilor neguvernamentale este la fel de important. Aceștia ar trebui să fie instruiți să detecteze și să gestioneze manipulările, campaniile de dezinformare țintite în timpul perioadei electorale și ar trebui să diminueze impactul acestor manipulări, în loc să-l amplifice.

75. Securitatea cibernetică și protecția datelor se află într-o strânsă corelare și reprezintă două elemente de bază în protecția persoanelor și a drepturilor acestora. Tehnologiile de îmbunătățire a confidențialității sunt un bun exemplu în acest sens. Prin urmare, consolidarea cooperării și a colaborării între agențiile de protecție a datelor și de securitate cibernetică permite o mai bună abordare a provocărilor în materie de securitate cibernetică și confidențialitate într-o manieră holistică și ajută alte organizații, atât publice, cât și private, să își îmbunătățească pregătirea.

Domeniul de intervenție IV – cooperare internațională

76. Unul dintre principalele mijloace de asigurare a securității cibernetice îl constituie intensificarea și îmbunătățirea cantitativă și calitativă a cooperării internaționale și a activităților mai active în cadrul organizațiilor și inițiativelor internaționale.

77. Republica Moldova se află într-un proces intens de consolidare a posturii sale în domeniul securității cibernetice. Pe plan normativ, a fost modernizat cadrul normativ și au fost instituite mecanisme clare de răspuns la incidente. Din punct de vedere tehnic, țara dispune de o anumită capacitate operațională, echipa de răspuns la incidentele cibernetice la nivel național aflându-se într-o continuă dezvoltare. La nivel internațional, este tot mai bine conectată la programele și inițiativele UE și NATO, participă la schimburi de formare și este integrată în rețele multilaterale de reziliență. Pe plan operațional, Republica Moldova este pregătită să facă față amenințărilor hibride, beneficiind de acces la Rezerva de securitate cibernetică a Uniunii Europene și la canalele internaționale de răspuns la incidente.

78. Deși s-au înregistrat progrese notabile în guvernanța internă a securității cibernetice și cooperarea regională, diplomația cibernetică rămâne o dimensiune subdezvoltată, dar esențială a securității naționale și a politicii externe a țării. Nu există un reprezentant special dedicat domeniului cibernetic, o unitate sau un mecanism interinstituțional însărcinat cu reprezentarea Republicii Moldova în dezbaterile privind normele cibernetice globale, gestionarea diplomației incidentelor transfrontaliere sau negocierea acordurilor internaționale privind securitatea digitală. Ministerul Afacerilor Externe nu a dezvoltat încă o unitate de diplomație cibernetică. Acest lucru limitează vizibilitatea și influența țării pe platformele internaționale de securitate cibernetică și capacitatea sa de a-și susține interesele în procese multilaterale, cum ar fi OEWG (*Open-ended Working Group*) al Organizației Națiunilor Unite sau dialogurile Organizației pentru Securitate și Cooperare în Europa de consolidare a încrederii cibernetice. Totuși, Ministerul Afacerilor Externe depune efort în acest sens. Astfel, în ultimii doi ani, acesta a întreprins un șir de acțiuni îndreptate spre instituirea unei subdiviziuni noi în cadrul ministerului, care ar fi responsabilă de diplomația cibernetică. Ministerul Afacerilor Externe a elaborat proiectul noului Regulament de organizare și funcționare a ministerului, inclusiv noua structură a aparatului central, care prevede instituirea Serviciului diplomație cibernetică în cadrul Direcției cooperare multilaterală. Proiectul hotărârii Guvernului pentru aprobarea Regulamentului menționat se află la etapa de consultare publică.

79. Una dintre principalele provocări o constituie armonizarea legislației naționale cu reglementările Uniunii Europene și integrarea în formatele și

organizațiile de cooperare ale Uniunii Europene, urmând prioritățile naționale și liniile de acțiune pentru integrarea în Uniunea Europeană.

80. Al doilea factor foarte important în abordarea și alocarea resurselor pentru cooperarea internațională este natura globală a provocărilor în materie de securitate cibernetică. Majoritatea incidentelor cibernetice și a infracțiunilor cibernetice sunt de natură transnațională, autorii, facilitatorii și victimele fiind din diferite țări și jurisdicții, iar prevenirea unor astfel de incidente și infracțiuni necesită o cooperare internațională eficientă. De asemenea, trebuie remarcat faptul că amenințările tehnologice sunt în general de natură globală, cu aceleași tehnologii de securitate în rețea implementate de obicei în multe țări, iar atacurile cibernetice dintr-o țară sunt urmate imediat de atacuri împotriva acelorași tehnologii implementate în diverse țări. Datorită faptului că multe dintre grupările de crimă organizată operează dincolo de granițele lor naționale, activitățile lor au în mod evident consecințe internaționale. Pentru a preveni acest fenomen și a evita extinderea acestuia, sunt necesare măsuri preventive suplimentare prin aplicarea mecanismelor de cooperare internațională. Prin urmare, este extrem de important ca Republica Moldova să joace rolul unui partener de încredere și să aibă relații foarte bune și strânse și schimburi de informații cu autoritățile de securitate cibernetică și cu organizațiile internaționale din alte țări. Acest lucru necesită o comunicare internațională strânsă, reprezentare activă și participarea la forurile de cooperare internațională și contribuție la activitatea lor.

81. Pentru a utiliza cât mai eficient capacitățile cibernetice limitate, entitățile guvernamentale din Republica Moldova se confruntă cu necesitatea unei colaborări mai strânse și mai eficiente între ele. Provocarea majoră este implicarea nu doar a entităților guvernamentale, ci și a mediului de afaceri și a comunității de cercetare, astfel încât expertiza în domeniul securității cibernetice să fie valorificată la maximum pentru consolidarea rezilienței cibernetice a țării.

82. Conform Legii nr. 48/2023 privind securitatea cibernetică, Agenția pentru Securitate Cibernetică, în calitate de autoritate competentă în domeniul securității cibernetice, îndeplinește funcția de punct unic de contact național și trebuie să asigure interacțiunea autorităților și instituțiilor publice naționale cu autorități similare din alte state și/sau cu organizații ori entități internaționale înființate de acestea.

Capitolul III
OBIECTIVE GENERALE ȘI SPECIFICE

83. Prezentul Program își propune să contribuie la realizarea obiectivelor și a direcțiilor prioritare stabilite în documentele de politici publice de nivel superior, în special în Strategia securității naționale a Republicii Moldova și în Strategia de

transformare digitală a Republicii Moldova pentru anii 2023-2030, precum și în alte documente strategice și de planificare, cum ar fi Strategia de dezvoltare „Educația 2030” și Programul de implementare a acesteia pentru anii 2023-2025, Strategia de dezvoltare a domeniului afacerilor interne pentru anii 2022-2030, Strategia națională de apărare a Republicii Moldova pentru anii 2024-2034, Programul național de prevenire și de combatere a criminalității pentru anii 2026-2030 și Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029.

84. În urma analizei acestor documente strategice și a realizării unui inventar detaliat al situației în domeniul securității cibernetice, au fost formulate patru obiective generale, prezentate în tabelul 1.

85. Fiecare obiectiv general este detaliat în mai multe obiective specifice, care oferă o direcție mai clară cu privire la modul în care urmează a fi obținute rezultatele așteptate (tabelul 1).

Tabelul 1

Indicatori de rezultat pentru obiectivele specifice

Obiectiv general	Obiectiv specific	Indicator	Valoarea de referință (2025)	Țintă (2028)	Țintă (2030)
1	**2**	**3**	**4**	**5**	**6**
1. Consolidarea capacităților operaționale	1.1. Consolidarea capacităților de răspuns la incidentele cibernetice ale Agenției pentru Securitate Cibernetică	Creșterea scorului de țară la capitolul „dezvoltarea capacităților” *Sursa: Indicele global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor*	8,04 (2024)	12.5	17,5
	1.2. Consolidarea rezilienței furnizorilor de servicii în sectoarele critice împotriva amenințărilor cibernetice și a incidentelor cibernetice	Creșterea scorului de țară la capitolul „măsuri tehnice” *Sursa: Indicele global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor*	6,68 (2024)	10,5	15,5
	1.3. Îmbunătățirea răspunsului la crizele cibernetice prin asigurarea unei abordări coordonate și prin valorificarea structurilor existente pentru menținerea funcțiilor societale vitale	Creșterea scorului de țară la capitolul „măsuri tehnice” *Sursa: Indicele global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor*	6,68 (2024)	10,5	15,5

1	2	3	4	5	6
2.Consolidarea rezilienței țării împotriva criminalității informatice	2.1. Consolidarea competențelor și a abilităților autorităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice şi a infracţiunilor în domeniul comunicaţiilor electronice	Numărul instrumentelor inteligente de investigare dezvoltate *Sursa: Ministerul Afacerilor Interne*	8 instrumente (2024)	Minimum 9 instrumente	Minimum 10 instrumente
	2.2. Implementarea unor instrumente și soluții moderne în vederea prevenirii și a combaterii criminalității cibernetice	Dotarea cu instrumente și soluții inteligente de investigare *Sursa: Ministerul Afacerilor Interne*	8 instrumente (2024)	Minimum 9 instrumente	Minimum 10 instrumente
3. Dezvoltarea competențelor și a culturii de securitate cibernetică în societate	3.1. Dezvoltarea forței de muncă calificate în domeniul securității cibernetice prin extinderea oportunităților educaționale	Ponderea specialiștilor în TIC în rândul populației ocupate *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	2,7 % (2022)	3,3 %	4 %
		Ponderea absolvenților STEAM (știință, tehnologie, inginerie, artă și matematică) în rezerva totală de absolvenți de studii universitare *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	13,7 % (2022)	15 %	16 %
	3.2. Dezvoltarea unui mecanism național de monitorizare continuă și evaluare a dezvoltării societății digitale	Ponderea populației cu competențe digitale de bază *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	N/A	40 %	80 %
	3.3. Consolidarea cooperării interne între autoritățile și instituțiile publice,	Ponderea persoanelor care verifică veridicitatea	N/A	40 %	80 %

1	2	3	4	5	6
	precum și cu mass-media pentru a combate eficient manipulările electorale și atacurile cibernetice	informațiilor găsite pe internet *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*			
	3.4. Protejarea drepturilor și a libertăților persoanelor în procesul de prelucrare a datelor lor cu caracter personal	Ponderea utilizatorilor de internet care aplică măsuri active de gestionare a confidențialității și a datelor personale *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	N/A	40 %	80 %
4. Cooperarea internațională pentru a deveni un partener de încredere în comunitatea internațională de aplicare a legii și securitate cibernetică	4.1. Consolidarea cooperării internaționale prin integrarea Republicii Moldova în cadrele de cooperare în materie de aplicare a legii și securitate cibernetică la nivelul Uniunii Europene	Creșterea scorului de țară la capitolul „măsuri de cooperare” *Sursa: Indicele global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor*	15,51 (2024)	16,5	18,5
	4.2. Dezvoltarea platformelor de comunicare strategică externă pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova	Creșterea scorului de țară la capitolul „măsuri de cooperare” *Sursa: Indicele global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor*	15,51 (2024)	16,5	18,5
	4.3. Consolidarea capacității de diplomație cibernetică internațională	Creșterea scorului de țară la capitolul „măsuri de cooperare” *Sursa: Indicele global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor*	15,51 (2024)	16,5	18,5

Capitolul IV
IMPACT

86. Pe lângă contribuția la realizarea obiectivelor și a direcțiilor prioritare stabilite în documentele de politici publice de nivel superior, prezentul Program și Planul de acțiuni privind implementarea acestuia sprijină obiectivele Republicii

Moldova în ceea ce privește aderarea la Uniunea Europeană și armonizarea reglementărilor naționale cu legislația Uniunii Europene.

87. Implementarea prezentului Program va genera un impact semnificativ asupra securității cibernetice a Republicii Moldova. Dintre beneficiile așteptate trebuie relevate următoarele:

87.1. îmbunătățirea protecției infrastructurilor critice naționale – implementarea unor măsuri avansate de securitate va reduce vulnerabilitățile și riscul de atacuri cibernetice;

87.2. consolidarea capacității instituționale – vor fi create mecanisme eficiente de coordonare și vor crește resursele umane calificate în domeniul securității cibernetice;

87.3. creșterea rezilienței cibernetice a societății – prin educație și conștientizare, populația și mediul de afaceri vor fi mai bine pregătite pentru a preveni și a răspunde la incidentele cibernetice;

87.4. creșterea încrederii în serviciile digitale – un mediu cibernetic mai sigur va contribui la adoptarea pe scară mai largă a tehnologiei informației și a serviciilor digitale, sprijinind dezvoltarea economică și inovarea;

87.5. extinderea cooperării internaționale – colaborarea cu organizații internaționale și parteneri strategici va permite accesul la cele mai bune practici, instrumente și resurse în domeniul securității cibernetice;

87.6. combaterea criminalității informatice – va fi consolidată capacitatea de prevenire, detectare și investigare a criminalității informatice prin îmbunătățirea cooperării între autorități, cooperarea internațională și dezvoltarea unor mecanisme eficiente de sancționare a atacatorilor.

88. Trebuie remarcat faptul că digitalizarea accelerată a economiei Republicii Moldova a adus oportunități, dar și riscuri. Sectorul tehnologiei informației este unul dintre principalele motoare ale creșterii economice, atrăgând investiții și contribuind la exporturile de servicii digitale. În paralel, Guvernul promovează transformarea digitală a serviciilor publice pentru a îmbunătăți accesul cetățenilor la administrația publică.

89. Un nivel scăzut de securitate cibernetică poate descuraja investițiile străine și poate afecta încrederea publicului în serviciile digitale. În acest context, implementarea prezentului Program este esențială pentru asigurarea unui ecosistem digital sigur și rezilient, care să susțină dezvoltarea economică și modernizarea Republicii Moldova.

90. În vederea abordării eficiente a acestor provocări, este necesară dezvoltarea unor intervenții specifice pentru a stabili un ecosistem de securitate cibernetică care să fie atât rezilient la amenințările externe, cât și durabil pe termen lung.

91. Impactul implementării măsurilor propuse va fi reflectat prin îmbunătățirea poziției Republicii Moldova în Indicele global al securității cibernetice al Uniunii Internaționale a Telecomunicațiilor, prin avansarea de la locul 63 în anul 2024 la locul 55 în anul 2028 și locul 50 în anul 2030.

Capitolul V
COSTURI

92. Implementarea prezentului Program se va realiza din contul și în limitele alocațiilor aprobate în bugetele autorităților responsabile, prin intermediul asistenței financiare și tehnice acordate de organizațiile internaționale și partenerii de dezvoltare, precum și din alte surse conform legislației.

93. În urma evaluării costurilor, cheltuielile necesare pentru realizarea acțiunilor planificate sunt estimate la circa 73,1 milioane de lei. Dezagregarea pe obiective specifice și ani este prezentată în tabelul 2.

94. Deși o parte considerabilă din aceste cheltuieli nu dispune, în acest moment, de acoperire financiară din partea partenerilor de dezvoltare și urmează a fi reflectată în Cadrul bugetar pe termen mediu și bugetul de stat, autoritățile și instituțiile responsabile vor continua dialogul cu partenerii de dezvoltare și alți actori relevanți în vederea identificării și a mobilizării surselor externe de finanțare. Acest demers va contribui la diminuarea presiunii asupra bugetului național.

95. Implementarea prezentului Program se va realiza preponderent prin următoarele programe bugetare:

95.1. programul „03. Executivul și serviciile de suport”:

95.1.1. subprogramul „0303. e-Transformare a Guvernării”;

95.2. programul „15. Edificarea societății informaționale”:

95.2.1. subprogramul „1501. Politici și management în domeniul dezvoltării informaționale”;

95.2.2. subprogramul „1504. Tehnologii informaționale”;

95.3. programul „50. Servicii generale economice și comerciale”:

95.3.1. subprogramul „5001. Politici și management în domeniul macroeconomic și de dezvoltare a economiei”.

Tabelul 2

Costuri pentru punerea în aplicare a Programului

Obiectivul specific	Codul subprogramului bugetar	Costuri totale (mii lei)	Costuri pe ani (mii lei)				
			Anul 2026	Anul 2027	Anul 2028	Anul 2029	Anul 2030
1	2	3	4	5	6	7	8
Obiectivul specific 1.1		**9294,07**	**4569,4**	**1816,47**	**969,4**	**969,4**	**969,4**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)	1504	736	117,2	267,2	117,2	117,2	117,2
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		8558,07	4452,2	1549,27	852,2	852,2	852,2
Obiectivul specific 1.2		**41819,33**	**15013,97**	**15013,97**	**7000,1**	**66,8**	**66,8**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)	1504	1245,43	631,56	613,87	-	-	-
Costuri acoperite din asistența externă (mii lei)		8940	8940	-	-	-	-
Costuri neacoperite (mii lei)		31633,9	10100,1	14400,1	7000,1	66,8	66,8
Obiectivul specific 1.3		**4917,29**	**960**	**1077,29**	**960**	**960**	**960**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)	5001	117,29	-	-	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		4800	960	960	960	960	960
Obiectivul specific 2.1		**1467,29**	**350**	**117,29**	**1000**	**0**	**0**

1	2	3	4	5	6	7	8
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)	1504	117,29	-	117,29	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		1350	350	0	1000,00	0	0
Obiectivul specific 2.2		**189,0**	**-**	**189,0**	**-**	**-**	**-**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)		-	-	-	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		189	-	189	-	-	-
Obiectivul specific 3.1		**2420,64**	**466,9**	**643,04**	**436,9**	**436,9**	**436,9**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)		-	-	-	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		2420,64	466,9	643,04	436,9	436,9	436,9
Obiectivul specific 3.2		**2822,15**	**566,8**	**520**	**735,35**	**500**	**500**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)	1504	86,8	66,8	20	-	-	-

1	2	3	4	5	6	7	8
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		2735,35	500	500	735,35	500	500
Obiectivul specific 3.3		**1765,0**	**353,0**	**353,0**	**353,0**	**353,0**	**353,0**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)		-	-	-	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		1765,0	353,0	353,0	353,0	353,0	353,0
Obiectivul specific 3.4		**1024,08**	**356,08**	**167**	**167**	**167**	**167**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)		189,08	189,08	-	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		835	167	167	167	167	167
Obiectivul specific 4.1		**560,0**	**80,0**	**240**	**80,0**	**80,0**	**80,0**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)		-	-	-	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		560,0	80,0	240	80,0	80,0	80,0

1	2	3	4	5	6	7	8
Obiectivul specific 4.2		**4517,29**	**997,29**	**880**	**880**	**880**	**880**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)		117,29	117,29	-	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		880	880	880	880	880	880
Obiectivul specific 4.3		**2364,29**	**1898,85**	**166,46**	**99,66**	**99,66**	**99,66**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)		117,29	-	-	-	-	-
Costuri acoperite din asistența externă (mii lei)		-	-	-	-	-	-
Costuri neacoperite (mii lei)		2247	1781,56	166,46	99,66	99,66	99,66
TOTAL		**73160,43**	**30269,98**	**21183,52**	**12681,41**	**4512,76**	**4512,76**
Costuri acoperite în Cadrul bugetar pe termen mediu (mii lei)		**2726,47**	**1239,22**	**1135,65**	**117,2**	**117,2**	**117,2**
Costuri acoperite din asistența externă (mii lei)		**8940**	**8940**				
Costuri neacoperite (mii lei)		**61493,96**	**20090,76**	**20047,87**	**12564,21**	**4395,56**	**4395,56**

Capitolul VI
RISCURI DE IMPLEMENTARE

96. Riscurile identificate (tabelul 3) reflectă principalele constrângeri administrative, financiare, instituționale și tehnologice care pot influența implementarea prezentului Program. Evaluarea acestora s-a bazat pe o analiză integrată a rapoartelor Academiei de e-Guvernare din Estonia, Agenției Uniunii Europene pentru Securitate Cibernetică, Uniunii Internaționale a Telecomunicațiilor, precum și ale altor parteneri internaționali.

De asemenea, identificarea riscurilor s-a fundamentat pe analizele proprii, realizate în baza datelor statistice disponibile și a tendințelor reflectate în capitolul II. Această abordare combinată asigură corelarea între contextul național și tendințele globale, oferind o imagine realistă asupra vulnerabilităților actuale și emergente.

Tabelul 3

Descrierea riscurilor și a măsurilor de atenuare

Nr. crt.	Riscul	Impactul	Probabilitatea	Măsurile de diminuare a riscurilor
1	**2**	**3**	**4**	**5**
1.	Lipsa unei cooperări eficiente dintre autoritățile și instituțiile publice responsabile de implementarea Programului	Mare	Medie	• Stabilirea unor proceduri rigide de implementare, raportare și monitorizare; • stabilirea unui rol central al Ministerului Dezvoltării Economice și Digitalizării; • utilizarea mecanismului oferit de platforma Consiliului coordonator în domeniul securității cibernetice; • desemnarea unui secretariat permanent responsabil de monitorizarea progresului pe marginea implementării Programului
2.	Subfinanțarea măsurilor prevăzute în Program	Mare	Medie	• Asigurarea alinierii Programului la Cadrul bugetar pe termen mediu; • identificarea surselor de finanțare externe; • prioritizarea acțiunilor esențiale în Planul de acțiuni privind implementarea Programului; • includerea acțiunilor prioritare în Planul național de dezvoltare
3.	Capacitate administrativă limitată a autorităților și a	Mediu	Mare	• Instruirea personalului;

1	2	3	4	5
	instituțiilor publice responsabile			• alocarea de resurse pentru consolidarea echipelor responsabile; • implicarea experților din sectorul privat
4.	Nivel scăzut de conștientizare publică privind securitatea cibernetică	Mare	Mediu	• Campanii de informare naționale recurente; • revizuirea metodelor de instruire a tinerilor și a adulților în domeniul securității cibernetice; • desemnarea unei autorități responsabile de coordonarea aspectelor educaționale ale Programului
5.	Migrarea specialiștilor în domeniul securității cibernetice și lipsa forței de muncă calificate în domeniu	Mare	Mare	• Acordarea de stimulente salariale; • crearea unor instrumente de atragere și menținere a talentului în sectorul public; • sprijin pentru dezvoltarea ecosistemului de cercetare și inovare
6.	Lipsa de angajament și sprijin din partea factorilor de decizie și a funcționarilor publici în implementarea Programului, inclusiv schimbarea priorităților sau schimbările politice care pot afecta direcția și resursele alocate Programului	Mediu	Înaltă	• Includerea securității cibernetice în prioritățile asumate la nivel național; • asigurarea unui cadru legal stabil și predictibil; • elaborarea unui plan de comunicare detaliată referitor la realizarea Programului, inclusiv pentru a obține sprijinul și interesul publicului
7.	Dependența de furnizorii externi de soluții tehnologice	Mediu	Mediu	• Promovarea dezvoltării soluțiilor naționale; • diversificarea parteneriatelor tehnologice, în mod special a celor cu Uniunea Europeană

Capitolul VII
AUTORITĂȚI ȘI INSTITUȚII RESPONSABILE

97. De punerea în aplicare a prezentului Program sunt responsabile autoritățile și instituțiile publice cu competențe în realizarea politicii statului în domeniul securității cibernetice și combaterii criminalității cibernetice:

97.1. Ministerul Dezvoltării Economice și Digitalizării;

97.2. Ministerul Afacerilor Externe;

97.3. Ministerul Afacerilor Interne (Inspectoratul General al Poliției);

97.4. Ministerul Educației și Cercetării;

97.5. Procuratura Generală;

97.6. Agenția pentru Securitate Cibernetică;

97.7. Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică;

97.8. Instituţia Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”);

97.9. Comisia Electorală Centrală;

97.10. Centrul Național pentru Protecția Datelor cu Caracter Personal;

97.11. Ministerul Energiei;

97.12. Ministerul Infrastructurii și Dezvoltării Regionale;

97.13. Instituția Publică Centrul de Tehnologii Informaționale în Finanțe;

97.14. alte autorități și instituții relevante.

Capitolul VIII
PROCEDURI DE MONITORIZARE, EVALUARE ŞI RAPORTARE

98. Procesul de monitorizare și evaluare urmează să asigure realizarea tuturor acțiunilor planificate, ceea ce va duce la atingerea obiectivelor stabilite. Scopul monitorizării constă în urmărirea progresului înregistrat în realizarea Planului de acțiuni privind implementarea prezentului Program, în vederea determinării gradului de executare a acțiunilor și a conformității acestora cu cele planificate. Un alt aspect important îl constituie identificarea și evaluarea deficiențelor în realizarea acțiunilor și înaintarea propunerilor de remediere.

99. În procesul de implementare a prezentului Program vor fi realizate următoarele proceduri de monitorizare și evaluare:

99.1. monitorizarea semestrială – proces continuu, realizat la fiecare șase luni, care implică colectarea, analiza și interpretarea datelor referitoare la progresul activităților Programului, având scopul de a asigura conformitatea cu Planul de acțiuni privind implementarea Programului și de a identifica eventualele abateri și deficiențe de realizare. Secretariatul responsabil de monitorizarea Programului întocmește raportul semestrial privind implementarea Programului și a Planului de acțiuni în baza rapoartelor semestriale privind realizarea Planului de acțiuni prezentate de către entitățile publice implementatoare. Progresul privind realizarea Planului de acțiuni, în baza cărora se întocmește raportul de progres semestrial, se prezintă Secretariatului responsabil de monitorizarea Programului de către autoritățile și instituțiile publice implementatoare până la data de 20 a lunii următoare termenului scadent, prin intermediul sistemului informatic de monitorizare gestionat de Cancelaria de Stat. Raportul semestrial privind implementarea Programului și a Planului de acțiuni se prezintă spre validare Consiliului coordonator în domeniul securității cibernetice. Acesta va conține un rezumat tabelar al progresului realizat și al deficiențelor identificate, însoțit de propuneri de remediere, și va fi publicat pe site-ul web oficial al Ministerului Dezvoltării Economice și Digitalizării;

99.2. monitorizarea anuală – monitorizarea acțiunilor cu raportare anuală și la termen, finalizată cu un raport anual de progres privind implementarea Programului și a Planului de acțiuni. Raportul anual de progres are un caracter analitic și constituie un document de referință pentru planificarea următorului an de implementare, cu includerea datelor privind realizarea acțiunilor din Planul de acțiuni, cu raportare anuală și la termen, precum și a deficiențelor înregistrate în procesul de realizare a acțiunilor scadente. Raportul anual de progres privind implementarea Programului și a Planului de acțiuni se întocmește de către Secretariatul responsabil de monitorizarea Programului și se publică pe site-ul web oficial al Ministerului Dezvoltării Economice și Digitalizării. Rapoartele anuale privind realizarea Planului de acțiuni, în baza cărora se întocmește raportul anual de progres, se prezintă Secretariatului responsabil de monitorizarea Programului de către autoritățile și instituțiile publice implementatoare până la data de 20 a lunii următoare termenului scadent, prin intermediul sistemului informatic de monitorizare gestionat de Cancelaria de Stat. Informațiile prezentate în rapoartele autorităților și instituțiilor publice implementatoare trebuie să fie redate în mod obiectiv și detaliat pentru fiecare acțiune scadentă (inclusiv cu argumentele de rigoare privind deficiențele de realizare a acțiunii și măsurile întreprinse pentru remedierea sau eliminarea acestora). Raportul anual de progres privind implementarea Programului și a Planului de acțiuni se prezintă spre examinare și validare Consiliului coordonator în domeniul securității cibernetice. Acesta va conține un rezumat tabelar al progresului realizat și al deficiențelor identificate, însoțit de propuneri de remediere, și va fi publicat pe site-ul web oficial al Ministerului Dezvoltării Economice și Digitalizării;

99.3. evaluarea finală – se realizează în termen de șase luni de la terminarea perioadei de implementare a documentului de politici publice. Evaluarea finală se efectuează pentru a estima gradul de implementare a Programului și pentru a seta necesitățile și domeniile ce urmează a fi abordate în viitorul document de politici în domeniul securității cibernetice. Raportul final privind implementarea Programului se întocmește de către Secretariatul responsabil de monitorizarea Programului și se publică pe site-ul web oficial al Ministerului Dezvoltării Economice și Digitalizării.

100. Autoritățile și instituțiile publice implementatoare, specificate în Planul de acțiuni drept autorități/instituții responsabile, vor asigura reflectarea în propriile planuri operaționale anuale de activitate a obiectivelor și a acțiunilor incluse în Planul de acțiuni privind implementarea Programului, cu planificarea resurselor financiare pentru executarea acestora. În cadrul autorităților/instituțiilor menționate vor fi desemnate, prin ordin intern al conducătorilor, persoanele responsabile care vor asigura furnizarea tuturor informațiilor necesare și prezentarea rapoartelor privind gradul de implementare a Programului. Identificarea persoanelor responsabile va permite facilitarea comunicării autorităților/instituțiilor în cauză cu Secretariatul responsabil de monitorizarea

Programului. Secretariatul responsabil de monitorizarea Programului va întocmi și va actualiza anual lista persoanelor responsabile privind raportarea acțiunilor din Program. În caz de schimbare a persoanei responsabile, autoritățile și instituțiile publice implementatoare sunt obligate să informeze despre aceasta Secretariatul responsabil de monitorizarea Programului, cu indicarea noii persoane responsabile și a datelor de contact ale acesteia.

101. Ministerul Dezvoltării Economice și Digitalizării asigură activitatea Secretariatului responsabil de monitorizarea Programului prin desemnarea acestei sarcini Secției politici în domeniul securității cibernetice, subdiviziune din cadrul Ministerului Dezvoltării Economice și Digitalizării. Secretariatul responsabil de monitorizarea Programului coordonează procesul de colectare a informațiilor și a rapoartelor privind implementarea Programului de către autoritățile/instituțiile responsabile de realizarea acțiunilor, solicitând date, informații și analize relevante pentru monitorizarea și evaluarea gradului de implementare a Programului.

102. Autoritățile și instituțiile publice implementatoare prezintă, prin intermediul sistemului informatic de monitorizare gestionat de Cancelaria de Stat, Secretariatului responsabil de monitorizarea Programului informațiile necesare pentru monitorizarea și evaluarea progresului în realizarea acțiunilor planificate de care sunt responsabile, conform termenelor stabilite în Planul de acțiuni.

103. Raportul de evaluare se prezintă spre validare Consiliului coordonator în domeniul securității cibernetice și se publică pe site-ul web oficial al Ministerului Dezvoltării Economice și Digitalizării.

104. Elaborarea de către organizațiile societății civile a unor rapoarte alternative de evaluare privind implementarea Programului este încurajată. Rapoartele alternative pot oferi aprecieri calitative privind obiectivele atinse și măsurile realizate din Program, fiind susținute inclusiv prin sondajele de opinii privind creșterea nivelului de educație digitală.

Anexă
la Programul național de securitate cibernetică
pentru anii 2026-2030

PLAN DE ACȚIUNI
privind implementarea Programului național de securitate cibernetică pentru anii 2026-2030

Nr. crt.	Acțiuni unice identificabile	Indicatori de monitorizare	Costul total (mii lei)	Costuri totale repartizate pe surse de finanțare (mii lei)			Cod program/ subprogram bugetar, denumirea sursei de finanțare	Costuri repartizate pe ani (mii lei)					Termenul -limită (trimestru/ an)	Instituție responsabilă
				buget de stat	asistență externă	costuri neacoperite		2026	2027	2028	2029	2030		
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Obiectivul general 1. Consolidarea capacităților operaționale														
Obiectivul specific 1.1. Consolidarea capacităților de răspuns la incidentele cibernetice ale Agenției pentru Securitate Cibernetică														
1.1.1.	Dezvoltarea Registrului de stat al incidentelor cibernetice și a sistemului informatic care îl formează	Sistem centralizat de raportare și schimb de informații funcțional	3600			3600	1504	3600					Trimestrul IV al anului 2026	Agenția pentru Securitate Cibernetică
1.1.2.	Crearea unui mecanism centralizat pentru schimbul de informații cu furnizorii de servicii în sectoarele critice	Mecanism centralizat pentru schimbul de informații cu furnizorii de servicii funcțional	847,07	150.0		697,07	1504		847,07				Trimestrul II al anului 2027	Agenția pentru Securitate Cibernetică
1.1.3.	Instruirea furnizorilor de servicii în sectoarele critice privind mecanismele și instrumentele de raportare a incidentelor și a schimbului de informații	Cel puțin 100 de furnizori de servicii în sectoarele critice instruiți anual	261,1			261,1	1504	52,2	52,2	52,2	52,2	52,2	2026-2030	Agenția pentru Securitate Cibernetică; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1.1.4.	Organizarea de exerciții și simulări periodice de răspuns la incidente cibernetice pentru a consolida capacitățile operaționale în sectoarele critice	Cel puțin un exercițiu de răspuns la incidente cibernetice la nivel național și cel puțin un exercițiu la nivel sectorial/intersectorial organizate anual	4000			4000	1504	800	800	800	800	800	2026-2030	Agenția pentru Securitate Cibernetică; Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
1.1.5.	Publicarea evaluărilor periodice și a rapoartelor privind situația din spațiul cibernetic național	Raportul privind situația din spațiul cibernetic național publicat anual	586	586			1504	117,2	117,2	117,2	117,2	117,2	2026-2030	Agenția pentru Securitate Cibernetică; Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică; Ministerul Dezvoltării Economice și Digitalizării
Obiectivul specific 1.2. Consolidarea rezilienței furnizorilor de servicii în sectoarele critice împotriva amenințărilor cibernetice și a incidentelor cibernetice														
1.2.1.	Asigurarea implementării cadrului normativ cu privire la modul de realizare a obligațiilor de asigurare a securității cibernetice de către furnizorii de servicii în	Cadrul de reglementare privind acreditarea entităților ce vor avea dreptul de a efectua evaluarea conformității cu cerințele privind măsurile de securitate a	117,29	117,29			1504	117,29					Trimestrul IV al anului 2026	Agenția pentru Securitate Cibernetică

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	sectoarele critice și promovarea implementării standardelor naționale în domeniul securității informației și securității cibernetice de către furnizorii de servicii în sectoarele critice	rețelelor și a sistemelor informatice ale furnizorilor de servicii în sectoarele critice implementat												
		Standardele naționale în domeniul securității informației și securității cibernetice aprobate și actualizate anual	334			334		66,8	66,8	66,8	66,8	66,8	2026-2030	Institutul de Standardizare din Moldova
		Orientări și materiale metodice, inclusiv metodologie de evaluare a riscurilor și clasificare a informațiilor și a datelor, pentru publicul-țintă elaborate și publicate	150	150			1504		150				Trimestrul II al anului 2027	Agenția pentru Securitate Cibernetică
1.2.2.	Instruirea furnizorilor de servicii din sectoarele critice să utilizeze standardele naționale în domeniul securității informațiilor și al securității cibernetice în cadrul organizațiilor lor pentru a asigura conformitatea cu Legea nr. 48/2023 privind securitatea cibernetică	Necesitățile sectoriale de formare și dezvoltare profesională în domeniul securității cibernetice identificate în baza solicitărilor parvenite de la furnizorii de servicii în sectoarele critice; anul 2026 – 25 % de funcționari instruiți; anul 2027 – 40 % de funcționari instruiți	20800			20800	1504	6933,3	6933,3	6933,3			2026-2028	Agenția pentru Securitate Cibernetică; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”); Ministerul Dezvoltării Economice și Digitalizării; Institutul de Standardizare din Moldova
1.2.3.	Identificarea necesităților și promovarea certificării	Necesitățile sectoriale de formare/dezvoltare	66,8	66,8			1504		66,8				Trimestrul IV al	Agenția pentru

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	specialiștilor în securitatea cibernetică prin organizații specializate pentru a respecta standardele internaționale și programele de certificare profesională (Asociația de Audit și Control al Sistemelor Informatice (*Information Systems Audit and Control Association*), Administrator de Sistem, Audit, Rețea, Securitate (*SysAdmin, Audit, Network, Security*), Consiliul de Evaluare și Certificare Profesională (*Professional Evaluation and Certification Board*) etc.)	profesională în domeniul securității cibernetice identificate și sistematizate în baza solicitărilor											anului 2027	Securitate Cibernetică; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”); Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică; Ministerul Dezvoltării Economice și Digitalizării
		Cel puțin 20 de specialiști în securitate cibernetică certificați prin cursuri oferite în parteneriat cu organizații specializate	1000			1000	1504		1000				Trimestrul IV al anului 2027	Agenția pentru Securitate Cibernetică; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”); Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică;

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														Ministerul Dezvoltării Economice și Digitalizării; alte autorități și instituții relevante
1.2.4.	Consolidarea capacității instituționale a autorităților și a instituțiilor publice pentru alinierea acestora la cerințele de securitate stabilite de cadrul normativ în domeniul securității cibernetice	75 % din efectivul-limită al Agenției pentru Securitate Cibernetică angajat; cel puțin o persoană responsabilă de domeniul securității cibernetice desemnată în toate autoritățile publice centrale	400			400		400					Trimestrul IV al anului 2026	Agenția pentru Securitate Cibernetică
1.2.5.	Crearea cadrului normativ privind securitatea cibernetică a rețelelor 5G	Studiu de analiză a impactului și a riscurilor de implementare a setului de instrumente de securitate cibernetică 5G al Uniunii Europene elaborat	8940		8940		Acord de grant cu Swedfund (Ordinul ministrului dezvoltării regionale și digitalizării nr.32/2025)	8940					Trimestrul II al anului 2026	Ministerul Dezvoltării Economice și Digitalizării
		Cadru normativ privind securitatea cibernetică a rețelelor 5G adoptat	207,99	207,99			5001		207,99				Trimestrul I al anului 2027	Ministerul Dezvoltării Economice și Digitalizării
1.2.6.	Elaborarea proiectului de lege privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale	Legea privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale adoptată	207,99	207,99			5001	207,99					Trimestrul IV al anului 2026	Ministerul Dezvoltării Economice și Digitalizării
1.2.7.	Identificarea și desemnarea autorității sau a instituției publice care va exercita rolul de centru național de coordonare a competențelor în domeniul	Centru național de coordonare a competențelor în domeniul industrial, tehnologic și de cercetare în materie de	189,08	189,08			5001	189,08					Trimestrul IV al anului 2026	Ministerul Dezvoltării Economice și Digitalizării

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	industrial, tehnologic și de cercetare în materie de securitate cibernetică	securitate cibernetică desemnat												
1.2.8.	Elaborarea proiectului de hotărâre a Guvernului pentru aprobarea Regulamentului privind modul de semnare de către persoanele juridice de drept public a acordurilor de schimb de informații în materie de securitate cibernetică	Proiect de hotărâre a Guvernului adoptat	117,2	117,2			5001	117,2					Trimestrul II al anului 2026	Ministerul Dezvoltării Economice și Digitalizării
1.2.9.	Integrarea furnizorilor de servicii din sectoarele critice în cadrul platformei de monitorizare a evenimentelor de securitate cibernetică (SOC național) pentru asigurarea monitorizării și a răspunsului coordonat la incidentele cibernetice	Cel puțin 50 de furnizori de servicii integrați pe platforma de monitorizare a evenimentelor de securitate cibernetică (SOC național)	1000			1000	1504		1000				Trimestrul III al anului 2027	Agenția pentru Securitate Cibernetică
1.2.10.	Implementarea unei soluții de protecție DDOS și WAF pentru furnizorii de servicii din sectoarele critice	Cel puțin 50 de furnizori de servicii integrați pe platforma de monitorizare a evenimentelor de securitate cibernetică (SOC național)	5400			5400	1504		5400				Trimestrul I al anului 2027	Agenția pentru Securitate Cibernetică
1.2.11.	Implementarea unei soluții integrate de tip EDR pentru asigurarea protecției cibernetice a furnizorilor de servicii din sectoarele critice	Cel puțin 800 de dispozitive protejate	2700			2700	1504	2700					Trimestrul III al anului 2026	Agenția pentru Securitate Cibernetică
1.2.12.	Elaborarea și promovarea cadrului normativ secundar în vederea evaluării conformității mijloacelor de protecție	Cadru normativ aprobat	189,08	189,08					189,08				Trimestrul II al anului 2027	Serviciul de Informații și Securitate; Ministerul Dezvoltării

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	criptografică și a semnăturilor electronice și a certificării produselor criptografice în conformitate cu normele Uniunii Europene													Economice și Digitalizării
Obiectivul specific 1.3. Îmbunătățirea răspunsului la crizele cibernetice prin asigurarea unei abordări coordonate și valorificarea structurilor existente pentru menținerea funcțiilor societale vitale														
1.3.1.	Elaborarea cadrului normativ privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare	Cadru normativ aprobat	117,29	117,29			5001		117,29				Trimestrul IV al anului 2027	Ministerul Dezvoltării Economice și Digitalizării; Agenția pentru Securitate Cibernetică; Centrul Național de Management al Crizelor
1.3.2.	Îmbunătățirea capacităților de comunicare strategică în situații de criză cibernetică prin exerciții	Cel puțin trei exerciții comune de răspuns la crize cibernetice desfășurate anual cu părțile interesate transsectoriale	4000			4000		800	800	800	800	800	2026-2030	Centrul Național de Management al Crizelor; Centrul pentru Comunicare Strategică și Contracarare a Dezinformării; Agenția pentru Securitate Cibernetică; Ministerul Afacerilor Interne; Serviciul de Informații și Securitate; Ministerul Apărării; Ministerul Afacerilor Externe;

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														Ministerul Sănătății; alte autorități publice relevante
		Cel puțin două instruiri în comunicarea strategică pentru gestionarea crizelor cibernetice și/sau a atacurilor hibride – desfășurate	800			800		160	160	160	160	160	Anual	Centrul pentru Comunicare Strategică și Contracarare a Dezinformării; Centrul Național de Management al Crizelor; Agenția pentru Securitate Cibernetică; Ministerul Afacerilor Interne; Serviciul de Informații și Securitate; Ministerul Apărării; Ministerul Afacerilor Externe; Ministerul Sănătății; alte autorități publice relevante
Obiectivul general 2. Consolidarea rezilienței țării împotriva criminalității informatice														
Obiectivul specific 2.1. Consolidarea competențelor şi a abilităților entităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice şi a infracțiunilor în domeniul comunicațiilor electronice														
2.1.1.	Instituirea unui mecanism de coordonare și cooperare interinstituțională și stabilirea principalelor obiective strategice de funcționare a acestuia pentru combaterea	Acord de schimb de informații și de coordonare între autoritățile publice încheiat	117,29	117,29			1504	117,29					Trimestrul IV al anului 2026	Ministerul Afacerilor Interne (Inspectoratul General al Poliției);

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	criminalității informatice, cu implicarea autorităților publice responsabile de aplicarea legii și a celor responsabile de securitatea națională													Procuratura Generală; Agenția pentru Securitate Cibernetică; Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică
2.1.2.	Consolidarea continuă a capacităților de investigare a infracțiunilor informatice, inclusiv în domeniul criminalisticii digitale	Cel puțin 20 de profesioniști instruiți în prevenirea și combaterea criminalității informatice și/sau certificați în domeniul criminalisticii digitale	1000			1000				1000			Trimestrul IV al anului 2028	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Procuratura Generală
2.1.3.	Desfășurarea acțiunilor de informare a populației cu privire la măsurile preventive și la posibilitățile de raportare a faptelor ilegale în spațiul cibernetic către autoritățile de aplicare a legii	Cel puțin două acțiuni/campanii de informare a populației desfășurate	250			250		250					Trimestrul IV al anului 2026	Ministerul Afacerilor Interne (Inspectoratul General al Poliției)
2.1.4.	Informarea populației cu privire la operaționalizarea instrumentului/platformei online de raportare a infracțiunilor informatice	Cel puțin o campanie de informare realizată	100			100		100					Trimestrul IV al anului 2026	Ministerul Afacerilor Interne (Inspectoratul General al Poliției)
Obiectivul specific 2.2. Implementarea unor instrumente și soluții moderne în vederea prevenirii și a combaterii criminalității cibernetice														
2.2.1.	Reacreditarea Laboratorului de expertiză criminalistică în domeniul cibernetic	Laboratorul de expertiză criminalistică în domeniul cibernetic reacreditat	189			189			189				Trimestrul I al anului 2027	Ministerul Afacerilor Interne (Inspectoratul General al Poliției)
Obiectivul general 3. Dezvoltarea competențelor și a culturii de securitate cibernetică în societate														

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Obiectivul specific 3.1. Dezvoltarea forței de muncă calificate în domeniul securității cibernetice prin extinderea oportunităților educaționale														
3.1.1.	Promovarea educației în domeniul securității cibernetice pentru forța de muncă și facilitarea accesului la formare profesională în domeniul securității cibernetice pentru toate persoanele interesate, inclusiv pentru grupurile vulnerabile. Crearea de oportunități de formare pentru grupurile vulnerabile și concentrarea asupra fetelor și a femeilor pentru a încuraja participarea lor la industria digitală și la cursuri de formare	Programe de formare profesională elaborate și disponibile pentru diferite grupuri-țintă	20,0			20,0		20,0					Trimestrul IV al anului 2026	Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”); Ministerul Educației și Cercetării
		Minimum 100 de persoane instruite anual, din care cel puțin 45 de sex feminin	784,5			784,5		156,9	156,9	156,9	156,9	156,9	2026-2030	Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
3.1.2.	Diversificarea mecanismelor de finanțare a învățării și a educației adulților în domeniul securității cibernetice	Cel puțin două granturi acordate anual organizațiilor societății civile prin programul de sprijin specializat	200			200		40	40	40	40	40	Anual	Ministerul Educației și Cercetării; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
3.1.3.	Crearea mecanismului de acordare de burse pentru studenții calificați dedicați carierei în sectorul public la absolvire și furnizarea de programe de formare în domeniul securității cibernetice pentru	Cel puțin 10 burse și posibilități de granturi oferite diferitelor grupuri-țintă	1200			1200		240	240	240	240	240	Anual	Ministerul Educației și Cercetării; Instituția Publică Universitatea Tehnică a Moldovei

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	autoritățile responsabile de aplicarea legii (inclusiv sectorul vamal și judiciar)													(Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
3.1.4.	Promovarea integrării resurselor educaționale digitale și a tehnologiei în predarea disciplinelor STEAM legate de tehnologia informației și comunicațiilor și dezvoltarea de programe complexe de formare a profesorilor și oportunități de burse pentru îmbunătățirea și diversificarea abilităților de predare	Programe elaborate (inclusiv pentru formatori)	117,29			117,29			117,29				Trimestrul I al anului 2027	Ministerul Educației și Cercetării; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
		Program de formare a cadrelor didactice (inclusiv prin metode participative, instrumente digitale etc.) elaborat	20,0			20,0			20,0				Trimestrul I al anului 2027	Ministerul Educației și Cercetării
		Numărul formatorilor care au încheiat cursurile de formare a formatorilor și fac parte din grupul de formatori	48,85			48,85			48,85				Trimestrul III al anului 2027	Ministerul Educației și Cercetării
3.1.5.	Modernizarea curriculumului pentru a asigura conținut de învățare digitală pentru absolvenții de universitate, în special în domeniile științei, tehnologiei, ingineriei, artei și matematicii (STEAM)	Curriculumul universitar STEAM actualizat	10,0			10,0		10,0					Trimestrul III al anului 2026	Ministerul Educației și Cercetării; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
3.1.6.	Dezvoltarea pedagogiei digitale și a materialelor didactice relevante și	Materiale didactice inovatoare dezvoltate	20,0			20,0			20,0				Trimestrul II al	Ministerul Educației și Cercetării

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	inovatoare pentru a promova și a stimula dobândirea și practicarea competențelor STEAM												anului 2027	
Obiectivul specific 3.2. Dezvoltarea unui mecanism național de monitorizare continuă și evaluare a dezvoltării societății digitale														
3.2.1.	Dezvoltarea unui mecanism național de monitorizare continuă și evaluare a conștientizării riscurilor și implementarea măsurilor de securitate cibernetică	Sondaje efectuate anual	2500			2500		500	500	500	500	500	2026-2030	Agenția pentru Securitate Cibernetică; Ministerul Dezvoltării Economice și Digitalizării; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
3.2.2.	Dezvoltarea campaniilor de conștientizare și comunicare și a materialelor de formare și instruire pentru îmbunătățirea nivelului de siguranță online, în special dedicate grupurilor mai puțin calificate digital din societate	Nevoi sectoriale de formare definite și coordonate	66,8	66,8			1504	66,8					Trimestrul III al anului 2026	Agenția pentru Securitate Cibernetică; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
		Cursuri de formare elaborate	20,0	20,0			1504		20,0				Trimestrul I al anului 2027	Agenția pentru Securitate Cibernetică; Instituția Publică Universitatea Tehnică a Moldovei

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
														(Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”); alte autorități și instituții relevante
3.2.3.	Crearea unei rețele de experți, formatori și purtători de cuvânt în igiena cibernetică în diverse comunități prin utilizarea abordării de formare a formatorilor	Numărul formatorilor care au încheiat cursurile de formare a formatorilor și fac parte din grupul de formatori	235,35			235,35				235,35			Trimestrul II al anului 2028	Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
Obiectivul specific 3.3. Consolidarea cooperării interne între autoritățile și instituțiile publice, precum și mass-media, pentru a lupta eficient împotriva manipulărilor electorale și a atacurilor cibernetice														
3.3.1.	Elaborarea și organizarea de cursuri tematice de instruire pentru furnizori de servicii media, distribuitori de servicii media, formatori de opinie publică, jurnaliști și organizații neguvernamentale privind tehnicile de dezinformare și/sau manipulare a informațiilor și ingerințele străine utilizate pentru a afecta securitatea spațiului informațional al statului	Cel puțin trei instruiri desfășurate și ghiduri distribuite furnizorilor de servicii media, distribuitorilor de servicii media, formatori de opinie publică, jurnaliști și organizații neguvernamentale anual	1765			1765		353	353	353	353	353	2026-2030	Centrul pentru Comunicare Strategică și Contracarare a Dezinformării; Serviciul de Informații și Securitate
Obiectivul specific 3.4. Protejarea drepturilor și a libertăților persoanelor în procesul de prelucrare a datelor lor cu caracter personal														
3.4.1.	Stabilirea unei cooperări strategice între autoritățile și instituțiile publice cu competență în domeniul securității cibernetice și cele de protecție a datelor cu caracter personal și valorificarea reciprocă a punctelor forte pentru a proteja toate tipurile de date,	Semnarea unui memorandum de colaborare între autorități	189,08	189,08			1504	189,08					Trimestrul IV al anului 2026	Agenția pentru Securitate Cibernetică; Centrul Național pentru Protecția Datelor cu Caracter Personal

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	inclusiv datele cu caracter personal													
3.4.2.	Organizarea de campanii comune de promovare a conștientizării igienei cibernetice, a confidențialității și a protecției datelor cu caracter personal	Cel puțin o campanie comună de promovare a conștientizării igienei cibernetice, a confidențialității și a protecției datelor desfășurată anual	835			835		167	167	167	167	167	2026-2030	Agenția pentru Securitate Cibernetică; Centrul Național pentru Protecția Datelor cu Caracter Personal
Obiectivul general 4. Cooperarea internațională pentru a deveni un partener de încredere în comunitatea internațională de aplicare a legii și securitate cibernetică														
Obiectivul specific 4.1. Consolidarea cooperării internaționale prin integrarea Republicii Moldova în cadrele de cooperare în materie de aplicare a legii și securitate cibernetică la nivelul Uniunii Europene														
4.1.1.	Cooperarea cu Centrul european de combatere a criminalității informatice (EC3) al Agenției Uniunii Europene pentru Cooperare în Materie de Aplicare a Legii (Europol) și Agenția Uniunii Europene pentru Cooperare Judiciară în Materie Penală (Eurojust), Agenția Uniunii Europene pentru Securitate Cibernetică și cu autoritățile competente în domeniul securității cibernetice din țările învecinate și din țările din afara Uniunii Europene	Cel puțin două participări la grupuri operative comune și alte formate de cooperare anual	400			400		80	80	80	80	80	2026-2030	Ministerul Afacerilor Interne (Inspectoratul General al Poliției); Agenția pentru Securitate Cibernetică; Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică
4.1.2.	Integrarea cu rețeaua echipelor de răspuns la incidente cibernetice a Uniunii Europene, echipele de răspuns la situații de urgență cibernetică (CERT) și sistemele de alertă timpurie	Cel puțin două participări la grupuri operative comune și alte formate de cooperare	160			160			160				Trimestrul IV al anului 2027	Agenția pentru Securitate Cibernetică
Obiectivul specific 4.2. Dezvoltarea platformelor de comunicare strategică externă pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova														
4.2.1.	Elaborarea politicilor de comunicare strategică internă și conectarea la platformele de comunicare strategică externe ale structurilor sistemului de	Planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice aprobat	117,29	117,29			1504	117,29					Trimestrul IV al anului 2026	Agenția pentru Securitate Cibernetică

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	securitate, apărare și ordine publică pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova													
4.2.2.	Îmbunătățirea răspunsului la crizele cibernetice prin asigurarea unei abordări coordonate	Cel puțin două participări la exerciții regionale și internaționale de securitate cibernetică, de gestionare a crizelor și de gestionare a incidentelor cibernetice tehnice anual	400			400		80	80	80	80	80	2026-2030	Centrul Național de Management al Crizelor; Agenția pentru Securitate Cibernetică; Instituția Publică Serviciul Tehnologia Informației și Securitate Cibernetică
		Găzduirea a cel puțin unui exercițiu internațional de securitate cibernetică anual	4000			4000		800	800	800	800	800	2026-2030	Agenția pentru Securitate Cibernetică; Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
Obiectivul specific 4.3. Consolidarea capacității de diplomație cibernetică internațională														
4.3.1.	Crearea unei unități de diplomație cibernetică în cadrul Ministerului Afacerilor Externe	Unitate de diplomație cibernetică creată	117,29	117,29				117,29					Trimestrul II al anului 2026	Ministerul Afacerilor Externe
		Personalul unității de diplomație cibernetică angajat	1 681,9			1 681,9		1 681,9					Trimestrul IV al anului 2026	Ministerul Afacerilor Externe

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
4.3.2.	Oferirea de instruire specializată în diplomație cibernetică pentru personalul Ministerului Afacerilor Externe, al ambasadelor și al misiunilor permanente	Cel puțin o instruire a personalului relevant al Ministerului Afacerilor Externe, al ambasadelor și al misiunilor permanente organizată anual	231,1			231,1		46,22	46,22	46,22	46,22	46,22	2026-2030	Ministerul Afacerilor Externe
4.3.3.	Participarea la setul de instrumente pentru diplomație cibernetică al Uniunii Europene	Statutul de asociat sau observator în setul de instrumente pentru diplomație cibernetică al Uniunii Europene acordat Republicii Moldova	66,8			66,8			66,8				Trimestrul III al anului 2027	Ministerul Afacerilor Externe
4.3.4.	Negocierea acordurilor bilaterale sau regionale de cooperare cibernetică cu aliații strategici	Cel puțin un acord bilateral sau regional de cooperare cibernetică semnat anual	267,2			267,2		53,44	53,44	53,44	53,44	53,44	2026-2030	Agenția pentru Securitate Cibernetică; Ministerul Dezvoltării Economice și Digitalizării; Ministerul Afacerilor Externe

NOTA DE FUNDAMENTARE

la proiectul Hotărîrii Guvernului cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026-2030

1. Denumirea sau numele autorului și, după caz, a/al participanților la elaborarea proiectului actului normativ
Proiectul Hotărîrii Guvernului cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 a fost elaborat de către Ministerul Dezvoltării Economice și Digitalizării, în calitate de autoritate a administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice.
2. Condițiile ce au impus elaborarea proiectului actului normativ
2.1. Temeiul legal sau, după caz, sursa proiectului actului normativ Proiectul Hotărîrii Guvernului cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 este elaborat în conformitate cu prevederile art. 6 alin. (3) al Legii nr. 48/2023 privind securitatea cibernetică și Hotărârii Guvernului nr. 386/2020 cu privire la planificarea strategică. Totodată, Programul contribuie la implementarea unor obiective și direcții strategice ale următoarelor strategii: • Strategia securității naționale a Republicii Moldova, aprobată prin Hotărârea Parlamentului nr. 391/2023; • Strategia de transformare digitală a Republicii Moldova pentru anii 2023–2030, aprobată prin Hotărârea Guvernului nr. 650/2023; • Strategia națională de apărare a Republicii Moldova pentru anii 2024–2034, aprobată prin Hotărârea Parlamentului nr. 319/2024; • Strategia de dezvoltare "Educația 2030" și a Programului de implementare a acesteia pentru anii 2023–2025, aprobată prin Hotărârea Guvernului nr. 114/2023; • Strategia de dezvoltare a domeniului afacerilor interne pentru anii 2022–2030, aprobată prin Hotărârea Guvernului nr. 658/2022. Elaborarea proiectului de act normativ propus spre examinare este prevăzută și de următoarele documente strategice ale Republicii Moldova: 1) Agenda de reforme aferentă Planului de creștere al Republicii Moldova pentru 2025-2027 (Hotărârea Guvernului nr. 260/2025) – măsura 2.3.11, Condiția de plată și linia de referință: „Pentru a pune în aplicare noul său Program național de acțiuni în domeniul securității cibernetice pentru perioada 2025-2030, Moldova își face Agenția pentru Securitate Cibernetică pe deplin operațională și înființează Echipa națională de intervenție în caz de urgență informatică (CERT).” 2) Foaia de parcurs privind „Statul de drept” (criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană) (Hotărârea Guvernului nr. 275/2025) – acț. 4.4 din Rezultatul strategic nr. 4. „Consolidarea capacității de prevenire și combatere a criminalității cibernetice”. 3) Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029 (Hotărârea Guvernului nr. 306/2025) – Cap.10, proiectul 40. 4) Planul național de reglementări pentru anul 2025 (Hotărârea Guvernului nr. 841/2024) – acțiunea 24. 5) Strategia de transformare digitală a Republicii Moldova (Hotărârea Guvernului nr. 650/2023) - Obiectivul general nr. 5. „Crearea unui mediu digital accesibil, sigur și incluziv”.
2.2. Descrierea situației actuale și a problemelor care impun intervenția, inclusiv a cadrului normativ aplicabil și a deficiențelor/lacunelor normative Digitalizarea a impulsionat dezvoltarea economică și interconectarea globală, dar a crescut și expunerea la riscuri cibernetice. La nivel european, numărul incidentelor cu impact semnificativ este în creștere, iar costurile încălcărilor de securitate au atins niveluri record. Criminalitatea

cibernetică generează pierderi economice considerabile, estimate la circa 0,3% din PIB, ceea ce pentru Republica Moldova ar însemna anual circa 49 milioane USD.

În plan intern, se observă o creștere alarmantă a atacurilor cibernetice asupra cetățenilor și instituțiilor statului. Conștientizarea publică este în creștere, dar nivelul de familiarizare cu tipurile de amenințări rămâne scăzut. Potrivit Indicelui Global de Securitate Cibernetică (UIT), Moldova se află la un nivel mediu de performanță, cu lacune la capitolele măsuri tehnice și dezvoltarea capacităților.

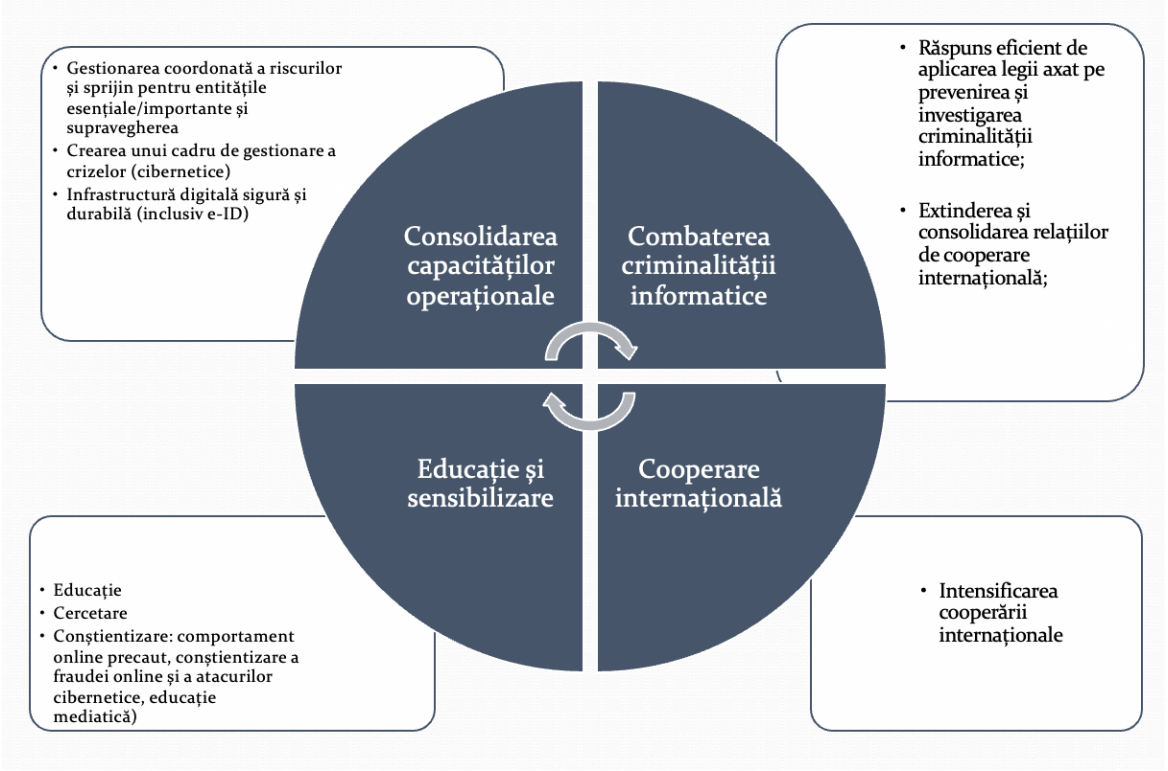
Sectorul TIC contribuie semnificativ la PIB, însă lipsa cadrelor calificate și investițiile reduse în cercetare și educație au impact asupra rezilienței digitale. Totodată, Strategia de securitate națională subliniază vulnerabilitatea țării la atacuri cibernetice și riscuri hibride, inclusiv dezinformare. În prezent, Moldova nu dispune de un cadru clar pentru gestionarea crizelor cibernetice, ceea ce o face dependentă de suport din partea instituțiilor UE.

Procesul de aderare la UE aduce noi obligații, în special punerea în aplicare a Legii 48/2023 și operaționalizarea Agenției pentru Securitate Cibernetică, inclusiv consolidarea capacităților furnizorilor de servicii critice și transpunerea cadrului normativ european (NIS2, Actul privind reziliența cibernetică, securitatea 5G).

Poate fi menționat că Republica Moldova se confruntă cu multiple provocări în domeniul securității cibernetice, dintre care se evidențiază următoarele:

- Creșterea numărului și complexității atacurilor cibernetice.
- Extinderea criminalității informatice și a fraudei online.
- Riscuri geopolitice și hibride, inclusiv dezinformare.
- Capacitate instituțională insuficientă.
- Nivel scăzut de conștientizare și educație digitală.
- Lipsa unui parteneriat public-privat funcțional.
- Vulnerabilitatea infrastructurilor critice.
- Cooperare internațională limitată.

Ca răspuns la aceste provocări, Programul prevede 4 subdomenii principale de intervenție:



Consolidarea capacităților operaționale

Modelul instituțional de securitate cibernetică din Republica Moldova este fragmentat, cu multiple autorități implicate în proces, dar cu o coordonare limitată și resurse insuficiente.

În ultimii ani, Republica Moldova a dezvoltat un cadru strategic, normativ și organizațional, pentru protecția spațiului său cibernetic și asigurarea securității rețelelor și sistemelor informatice, în vederea creșterii nivelului de reziliență cibernetică. Procedurile de raportare și gestionare a incidentelor în autoritățile publice sunt încă într-un stadiu de dezvoltare și este nevoie de un cadru interinstituțional mai bine structurat și funcțional, care să includă toți actorii relevanți, pentru a asigura un răspuns eficient și coordonat la atacurile cibernetice.

În prezent, principalele provocări sunt legate de lipsa resurselor umane specializate și a infrastructurii tehnice adecvate, dar și de dependența de proiecte externe pentru formare și echipamente. Responsabilitățile sunt dispersate între instituții, iar cooperarea și schimbul de date rămân reduse. Registrul național al incidentelor cibernetice nu este încă funcțional, fiind în dezvoltare, ceea ce face ca raportarea să fie fragmentară și incompletă, limitând capacitatea de prevenire și reacție. În același timp, mulți furnizori de servicii critice nu aplică încă proceduri de securitate bazate pe risc, iar Republica Moldova nu dispune de un mecanism integrat pentru gestionarea crizelor cibernetice la nivel național. Infrastructurile digitale, inclusiv identitatea digitală și semnătura electronică, rămân vulnerabile, cu un nivel scăzut de utilizare și încredere.

Combaterea criminalității informatice

Republica Moldova se confruntă cu o expunere ridicată la criminalitatea informatică, reflectată atât prin atacurile directe asupra instituțiilor și infrastructurilor critice, cât și prin rolul său de bază operațională pentru grupări infracționale transnaționale. Poziționarea țării pe locul 15 în clasamentul „World Cybercrime Index" indică vulnerabilități în mecanismele de prevenire și combatere, dar și asocierea nedorită cu state implicate activ în criminalitate cibernetică.

Principalele provocări sunt legate de atacurile sponsorizate de actori statali care vizează destabilizarea proceselor democratice și afectarea încrederii publice. Creșterea incidentelor de tip ransomware și fraudă online pune presiune pe instituțiile statului și mediul privat, în timp ce atacurile asupra infrastructurii critice subminează funcționarea serviciilor esențiale și generează percepții de insecuritate. În paralel, crima organizată online se dezvoltă rapid, alimentată de noi tehnologii precum inteligența artificială.

Un deficit structural îl reprezintă lipsa de profesioniști pe întreg lanțul de prevenire, investigare și urmărire penală a infracțiunilor informatice, accentuat de exodul de competențe către alte jurisdicții. Această slăbiciune afectează capacitatea autorităților de a reacționa eficient la incidente și de a construi o practică judiciară uniforme. Întreprinderile mici și mijlocii sunt în mod special vulnerabile la atacuri, din cauza resurselor limitate și a nivelului scăzut de conștientizare.

Deși Republica Moldova participă la parteneriate internaționale și este parte la Convenția de la Budapesta, nivelul de integrare în schimburile globale de informații și exerciții rămâne insuficient pentru a contracara complexitatea fenomenului.

Educație și sensibilizare

În prezent, Republica Moldova se confruntă cu un nivel scăzut de conștientizare în rândul autorităților publice, mediului privat, societății civile și al cetățenilor cu privire la riscurile cibernetice și măsurile de protecție. Există, de asemenea, un deficit de personal specializat, ceea ce afectează prevenirea, detectarea și gestionarea incidentelor cibernetice. Accesul la educație digitală de calitate și la programe de securitate cibernetică în instituțiile de învățământ formal și non-formal este încă limitat, iar resursele disponibile nu sunt suficiente pentru formarea unor specialiști competenți.

Igiena cibernetică și siguranța online nu sunt gestionate strategic la nivel național, iar inițiativele de sensibilizare existente au avut un impact redus, nefiind coordonate între actorii publici și cei privați.

În lipsa unor mecanisme centralizate și a unor evaluări periodice ale impactului programelor de educație și campaniilor de conștientizare, Republica Moldova întâmpină dificultăți în creșterea

gradului de pregătire a cetățenilor și a instituțiilor pentru prevenirea și gestionarea incidentelor cibernetice.

Cooperare internațională

În plan internațional, Republica Moldova este tot mai integrată în programe și inițiative UE și NATO, participă la schimburi de formare și face parte din rețele multilaterale de reziliență. Totodată, diplomația cibernetică rămâne insuficient dezvoltată, lipsind unitățile specializate responsabile, inclusiv, de negocierea acordurilor internaționale pe segmentul dat.

Provocările majore includ armonizarea legislației naționale cu reglementările UE și integrarea în formatele internaționale de cooperare, precum și natura transnațională a amenințărilor cibernetice. Majoritatea incidentelor și infracțiunilor cibernetice implică autori și victime din jurisdicții diferite, ceea ce face prevenirea și combaterea acestora dependentă de cooperarea internațională eficientă. De asemenea, tehnologiile de securitate și metodele de atac sunt similare la nivel global, iar grupările de crimă organizată operează adesea dincolo de granițele naționale, accentuând necesitatea unor relații strânse și schimburi constante de informații cu autorități și organizații internaționale.

O altă provocare este coordonarea internă și valorificarea eficientă a resurselor limitate. Colaborarea între entitățile guvernamentale, mediul de afaceri și comunitatea de cercetare este esențială pentru maximizarea expertizei în securitate cibernetică și consolidarea rezilienței țării.

Toate cele 4 subdomenii de intervenție sunt descrise în capitolul „Analiza situației” din partea descriptivă a Programului.

3. Obiectivele urmărite și soluțiile propuse

3.1. Principalele prevederi ale proiectului și evidențierea elementelor noi

Programul își propune să contribuie la realizarea obiectivelor și direcțiilor prioritare stabilite în documentele de politici publice de nivel superior, în special în Strategia națională de securitate a Republicii Moldova, Strategia de transformare digitală 2023–2030, precum și în alte documente strategice și de planificare, cum ar fi Strategia de dezvoltare „Educație 2030” și a Programului de implementare a acesteia pentru anii 2023–2025, Strategia de dezvoltare a domeniului afacerilor interne 2022–2030, Strategia națională de apărare a Republicii Moldova pentru anii 2024–2034, Programul național de prevenire și de combatere a criminalității pentru anii 2026–2030 și Programul național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029.

În urma analizei acestor documente strategice și a realizării unui inventar detaliat al situației în domeniul securității cibernetice, au fost formulate patru obiective generale, prezentate în tabelul de mai jos.

Fiecare obiectiv general este detaliat în mai multe obiective specifice care oferă o direcție mai focusată cu privire la modul în care urmează a fi obținute rezultatele așteptate. Toate aceste obiective sunt însoțite de acțiuni, care sunt reflectate în Planul de acțiuni al Programului.

Obiectiv general	**Obiectiv specific**	**Indicator**	**Valoarea de referință (2025)**	**Țintă(2028)**	**Țintă(2030)**
1.Consolidarea capacităților operaționale	1.1 Consolidarea capacităților de răspuns la incidentele cibernetice ale Agenției pentru Securitate Cibernetică	Creșterea scorului de țară la capitolul “dezvoltarea capacităților” *Sursa: Indicele global de securitate cibernetică (GCI) al UIT*	8,04 (2024)	12.5	17,5

	1.2 Consolidarea rezilienței furnizorilor de servicii în sectoarele critice împotriva amenințărilor cibernetice și a incidentelor cibernetice.	Creșterea scorului de țară la capitolul "măsurile tehnice" *Sursa: Indicele global de securitate cibernetică (GCI) al UIT*	6,68 (2024)	10,5	15,5
	1.3 Îmbunătățirea răspunsului la crizele cibernetice prin asigurarea unei abordări coordonate și prin valorificarea structurilor existente pentru menținerea funcțiilor societale vitale	Creșterea scorului de țară la capitolul "măsurile tehnice" *Sursa: Indicele global de securitate cibernetică (GCI) al UIT*	6,68 (2024)	10,5	15,5
2.Consolidarea rezilienței țării împotriva criminalității informatice	2.1 Consolidarea competențelor și abilităților autorităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice şi infracţiunilor în domeniul comunicaţiilor electronice	Numărul instrumentelor inteligente de investigare dezvoltate *Sursa: Ministerul Afacerilor Interne*	8 instrumente (2024)	Minim 9 instrumente	minim 10 instrumente
	2.2. Implementarea unor instrumente și soluții moderne în vederea prevenirii și combaterii criminalității cibernetice	Dotarea cu instrumente și soluții inteligente de investigare *Sursa: Ministerul Afacerilor Interne*	8 instrumente (2024)	Minim 9 instrumente	minim 10 instrumente

3. Dezvoltarea competențelor și a culturii de securitate cibernetică în societate	3.1 Dezvoltarea unei forțe de muncă calificate în domeniul securității cibernetice prin extinderea oportunităților educaționale	Ponderea specialiștilor în TIC în rândul populației ocupate *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	2,7 % (2022)	3,3 %	4%
		Ponderea absolvenților STEAM în rezerva totală de absolvenți de studii universitare *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	13,7 % (2022)	15 %	16%
	3.2 Dezvoltarea unui mecanism național de monitorizare continuă și evaluare a dezvoltării societății digitale	Ponderea populație cu competențe digitale de bază *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	N/A	40 %	80%
	3.3. Consolidarea cooperării interne între autoritățile și instituțiile publice, precum și cu mass-media pentru a combate eficient manipulările electorale și atacurile cibernetice.	Ponderea persoanelor care verifică veridicitatea informațiilor întâlnite pe internet *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	N/A	40 %	80%
	3.4. Protejarea drepturilor și libertăților persoanelor atunci când datele lor cu caracter personal sunt prelucrate	Ponderea utilizatorilor de internet care aplică măsuri active de gestionare a confidențialității și a datelor personale *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	N/A	40 %	80%
4. Cooperarea internațională pentru a deveni	4.1 Consolidarea cooperării	Creșterea scorului de țară la capitolul "măsuri de cooperare"	15,51 (2024)	16,5	18,5

un partener de încredere în comunitatea internațională de aplicare a legii și securitate cibernetică	internaționale prin integrarea Republicii Moldova în cadrele de cooperare în materie de aplicare a legii și securitate cibernetică la nivelul UE	*Sursa: Indicele global de securitate cibernetică al ITU*			
	4.2 Dezvoltarea platformelor de comunicare strategică externă pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova	Creșterea scorului de țară la capitolul "măsuri de cooperare" *Sursa: Indicele global de securitate cibernetică al ITU*	15,51 (2024)	16,5	18,5
	4.3 Consolidarea capacității de diplomație cibernetică internațională	Creșterea scorului de țară la capitolul "măsuri de cooperare" *Sursa: Indicele global de securitate cibernetică al ITU*	15,51 (2024)	16,5	18,5

3.2. Opțiunile alternative analizate și motivele pentru care acestea nu au fost luate în considerare

Nu sunt opțiuni alternative.

Cadrul normativ prevede în mod imperativ obligativitatea elaborării unui document de politici în domeniul securității cibernetice, aspect reflectat într-un șir de strategii, printre care Strategia securității naționale a Republicii Moldova, Strategia de transformare digitală a Republicii Moldova pentru anii 2023–2030 etc.

4. Analiza impactului de reglementare

4.1. Impactul asupra sectorului public

Implementarea Programului va produce un impact sistemic asupra sectorului public, având impact direct asupra modului în care autoritățile și instituțiile publice își gestionează resursele, riscurile și responsabilitățile în domeniul securității cibernetice.

Impactul asupra sectorului public este vizibil prin mai multe dimensiuni esențiale precum:

- ***Consolidarea cadrului instituțional și a guvernanței*** - va fi consolidat mecanismul de coordonare între autoritățile și instituțiile publice cu responsabilități în domeniul securității cibernetice.
- ***Creșterea rezilienței operaționale*** – toate autoritățile și instituțiile publice vor fi obligate să implementeze un set minim de măsuri de securitate, ceea ce va reduce vulnerabilitatea sistemelor guvernamentale.
- ***Instruirea și formarea funcționarilor publici*** - programul prevede instruirea funcționarilor și angajaților din autoritățile și instituțiile publice, ceea ce va ridica nivelul de alfabetizare cibernetică.

- ***Îmbunătățirea transparenței și responsabilității*** - raportarea obligatorie a incidentelor cibernetice către autoritățile competente va genera o imagine clară asupra nivelului real de amenințări și va permite o planificare mai eficientă a resurselor. Publicarea rapoartelor anuale privind nivelul de maturitate cibernetică va responsabiliza instituțiile și va încuraja respectarea standardelor minime.
- ***Eficiență financiară și utilizarea optimă a resurselor*** - investițiile coordonate în soluții comune (licențe, infrastructură SOC/SIEM, servicii de audit) vor permite economii, reducând cheltuielile individuale ale instituțiilor. Prin prevenirea incidentelor majore, se vor diminua costurile de remediere post-incident și pierderile asociate întreruperii serviciilor publice.
- ***Aliniere la standardele europene și integrare internațională*** – transpunerea legislației Uniunii Europene la nivel național și a altor instrumente europene va facilita interoperabilitatea instituțiilor naționale cu instituțiile partenere europene. Participarea instituțiilor publice la exerciții comune și la mecanisme de schimb de informații va contribui la recunoașterea Republicii Moldova ca partener de încredere în domeniul securității cibernetice.

4.2. Impactul financiar şi argumentarea costurilor estimative

Implementarea Programului se va realiza din contul și în limitele alocațiilor aprobate în bugetele autorităților responsabile, precum și prin intermediul asistenței financiare și tehnice acordate de organizațiile internaționale și partenerii de dezvoltare, și din alte surse permise de legislație.

În urma evaluării costurilor, cheltuielile necesare pentru realizarea acțiunilor planificate sunt estimate la circa 73,1 milioane lei. Dezagregarea pe obiective specifice și ani este prezentată la capitolul costuri în proiectul Programului, precum și la nivel de acțiuni în Planul de acțiuni al Programului.

Deși aproximativ 2/3 din aceste cheltuieli nu dispune, la acest moment, de acoperire financiară din partea partenerilor de dezvoltare și urmează a fi reflectată în Cadrul Bugetar pe Termen Mediu și bugetul de stat, autoritățile și instituțiile responsabile vor continua dialogul cu partenerii de dezvoltare și alți actori relevanți, în vederea identificării și mobilizării surselor externe de finanțare. Acest proces va contribui la diminuarea presiunii asupra bugetului național.

Implementarea Programului se va realiza preponderent prin următoarele programe bugetare:

- Programul „03. Executivul și serviciile de suport”
  - Subprogramul „0303. e-Transformare a Guvernării”
- Programul „15. Edificarea societății informaționale”
  - Subprogramul „1501. Politici și management în domeniul dezvoltării informaționale”
  - Subprogramul „1504. Tehnologii informaționale”
- Programul „50. Servicii generale economice și comerciale”
  - Subprogramul “5001-Politici și management în domeniul macroeconomic și de dezvoltare a economiei”

4.3. Impactul asupra sectorului privat

Realizarea acțiunilor în baza implementării Programului va avea un impact asupra mediului privat, în special asupra furnizorilor de servicii identificați de Agenția pentru Securitate Cibernetică conform Hotărîrii Guvernului nr. 860/2024.

Totodată, impactul acțiunilor din proiectul Programului ce țin de crearea cadrului normativ va fi evaluat la etapa elaborării actelor normative în cauză.

Impactul asupra sectorului privat este vizibil prin mai multe dimensiuni esențiale, precum:

- ***Creșterea nivelului de conformitate și securitate*** – furnizorii de servicii implementând cerințe minime de securitate și respectând procedurile standardizate de raportare a

incidentelor vor reduce expunerea la riscuri și vor asigura continuitatea serviciilor esențiale furnizate cetățenilor și economiei.

- ***Stimularea investițiilor în securitatea cibernetică*** - prin implementarea cerințelor de securitate obligatorii, mediul privat va fi motivat să investească în infrastructuri, soluții și personal specializat, ceea ce va permite prevenirea pierderilor financiare și va spori competitivitatea companiilor pe piață.
- ***Crearea de mecanisme de cooperare public–privat*** - instituirea mecanismelor de cooperare va permite schimbul regulat de informații despre amenințări și bune practici între autorități și furnizorii de servicii, ceea ce va contribui la detectarea timpurie a atacurilor și o reacție mai rapidă și coordonată.
- ***Dezvoltarea capitalului uman în sectorul privat*** - Programul prevede instruirea și certificarea unui număr semnificativ de specialiști IT din mediul privat, ceea ce va contribui la reducerea deficitului de competențe și la creșterea calității serviciilor de securitate cibernetică oferite pe piață.
- ***Creșterea încrederii consumatorilor și a partenerilor*** - consolidarea securității infrastructurilor și a serviciilor private va spori încrederea clienților și a partenerilor internaționali. Aceasta va facilita atragerea de investiții străine directe și integrarea companiilor naționale în lanțurile valorice la nivel internațional.

4.4. Impactul social

Implementarea Programului va avea impact asupra societății în ansamblu, contribuind la protecția drepturilor cetățenilor, care vor beneficia de servicii reziliente din partea statului și a mediului privat. Printre cele importante rezultate se numără:

- ***Creșterea alfabetizării digitale și a culturii de securitate*** - campaniile de informare, instruirile și introducerea elementelor de igienă cibernetică în educația formală și non-formală vor contribui la ridicarea nivelului de conștientizare al populației.
- ***Reducerea fraudei și a escrocheriilor online*** - crearea unor mecanisme accesibile de raportare și instruirea cetățenilor vor duce la scăderea numărului de victime ale fraudelor cibernetice.
- ***Creșterea încrederii în serviciile digitale*** - consolidarea securității cibernetice va încuraja populația să utilizeze mai activ serviciile electronice din sănătate, educație, plăți și comerț electronic, ceea ce va fi stimulată incluziunea digitală și va crește calitatea vieții.
- ***Consolidarea responsabilității colective*** - Programul promovează ideea că securitatea cibernetică este o responsabilitate comună a statului, companiilor și cetățenilor. Astfel, se va crea o cultură socială de prevenire și reacție rapidă la incidente.

4.4.1. Impactul asupra datelor cu caracter personal

Programul va contribui direct la îmbunătățirea protecției datelor cu caracter personal, reducând riscurile de compromitere și sporind încrederea cetățenilor în mediul digital. Printre cele mai importante rezultate se numără:

- ***Reducerea riscului de incidente de securitate -*** implementarea cerințelor minime obligatorii va diminua probabilitatea accesului neautorizat la date personale.
- ***Raportare și transparență*** - obligația instituțiilor și operatorilor privați de a raporta incidentele cibernetice în termene stricte va permite o reacție rapidă și va contribui la protejarea drepturilor persoanelor vizate.
- ***Creșterea capacității instituționale a autorităților de supraveghere*** - Programul prevede crearea de mecanisme de cooperare între Agenția pentru Securitate Cibernetic și Centrul Național pentru Protecția Datelor cu Caracter Personal, ceea ce va întări capacitatea de monitorizare și sancționare.
- ***Responsabilizarea operatorilor și a angajaților*** - prin instruiri și mecanisme, operatorii de date vor fi obligați să adopte practici mai stricte de protecție, reducând riscul de scurgeri cauzate de erori umane sau neglijență.

- ***Creșterea încrederii cetățenilor*** - o mai bună protecție a datelor va consolida încrederea populației în serviciile digitale publice și private, stimulând utilizarea lor mai largă și sprijinind transformarea digitală a Republicii Moldova.

4.4.2. Impactul asupra echității și egalității de gen

Implementarea Programului va contribui la promovarea echității și egalității de gen în sectorul digital și în domeniul securității cibernetice. Prin acțiunile planificate, Programul va stimula participarea activă a femeilor în formare, instruire și certificare, asigurând acces egal la oportunități profesionale.

4.5. Impactul asupra mediului

Programul nu are un impact direct asupra mediului înconjurător. Acțiunile prevăzute vizează în principal consolidarea cadrului instituțional, dezvoltarea capacităților tehnice, formarea capitalului uman și creșterea rezilienței digitale, fără a genera efecte semnificative asupra mediului.

Totuși, prin promovarea digitalizării serviciilor și utilizarea infrastructurilor partajate, Programul poate avea efecte indirecte pozitive, contribuind la reducerea consumului de resurse materiale. Aceste efecte sunt secundare și nu constituie obiectiv explicit al Programului.

4.6. Alte impacturi și informații relevante

Alte impacturi nu au fost identificate.

5. Compatibilitatea proiectului actului normativ cu legislația UE

5.1. Măsuri normative necesare pentru transpunerea actelor juridice ale UE în legislația națională

Prezentul proiect de Hotărîre a Guvernului nu conține norme privind transpunerea actelor juridice ale UE în legislația națională. Totodată, Programul include acțiuni specifice care vizează transpunerea ulterioară a actelor juridice ale UE în legislația națională, asigurând astfel alinierea cadrului normativ la cerințele europene.

5.2. Măsuri normative care urmăresc crearea cadrului juridic intern necesar pentru implementarea legislației UE

În procesul elaborării proiectului Programului și, implicit, a planului de acțiuni, s-a luat în considerare prevederile Comunicării Comune către Parlamentul European și Consiliu „Strategia de securitate cibernetică a UE pentru deceniul digital", precum și a Comunicării Comune către Parlamentul European și Consiliu „Raport privind punerea în aplicare a Strategiei de securitate cibernetică a UE pentru deceniul digital".

6. Avizarea și consultarea publică a proiectului actului normativ

În vederea respectării prevederilor art. 8 și 9 din Legea nr. 239/2008 privind transparența în procesul decizional, precum și conform prevederilor pct. 177 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, a fost publicat anunțul privind inițierea procesului de elaborare a proiectului Programului național în domeniul securității cibernetice (https://particip.gov.md/ru/document/stages/anunt-privind-initierea-procesului-de-elaborare-a-proiectului-programului-national-in-domeniul-securitatii-cibernetice-pentru-anii-2026-2030/14107).

Totodată, în vederea respectării prevederilor pct. 63.8 al Regulamentului cu privire la planificarea strategică, aprobat prin Hotărârea Guvernului nr. 386/2020, conceptul revizuit Programului în baza opiniei Cancelariei de Stat a fost plasat pe site-ul web al Ministerului Dezvoltării Economice și Digitalizării și platforma particip.gov.md.

Adițional, în vederea respectării prevederilor 63.14 al aceluiași Regulament, proiectul a fost supus evaluării calităţii şi a conformităţii de către Cancelaria de Stat și Ministerul Finanţelor. Ulterior, proiectul a fost definitivat în baza recomandărilor acestor autorități.

Suplimentar, la data de 11.11.2025, în vederea respectării pct. 63.5, proiectul a fost supus examinării în cadrul Consiliului pentru coordonarea dezvoltării durabile.

Totodată, a fost supus procesului de avizare oficială cu toate autoritățile publice relevante și plasat pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării mded.gov.md și pe particip.gov.md (https://particip.gov.md/ro/document/stages/*/15523) pentru consultare publică.

Proiectul Hotărârii de Guvern a fost transmis Comisiei Europene pentru consultare la data de 28.10.2025. La data de 22.12.2025 reprezentanții DG ENEST au informat că opinia oficială urmează să fie transmisă după data de 15.01.2026 (întârziere cauzată de perioada concediilor). Totodată, s-a menționat că pentru a respecta termenul limită din Agenda de Reforme, este esențial ca Republica Moldova să aprobe proiectul Hotărîrii de Guvern în forma actuală, în timp ce ajustări suplimentare pot fi făcute ulterior în caz de necesitate, după eventualele comentarii parvenite din partea DG CNECT.

7. Concluziile expertizelor

Proiectul a fost supus expertizei juridice din partea Ministerului Justiției și expertizei anticorupție de către Centrul Național Anticorupție.

8. Modul de încorporare a actului în cadrul normativ existent

Proiectul se integrează în sistemul legislației, este corelat cu prevederile actelor normative conexe în vigoare, iar implementarea prevederilor acestui proiect nu necesită modificarea altor acte normative

9. Măsurile necesare pentru implementarea prevederilor proiectului actului normativ

Nu necesită careva măsuri pentru implementare.

Secretar de stat **Michelle Iliev**

SINTEZA

obiecțiilor și propunerilor/recomandărilor la proiectul hotărîrii Guvernului cu privire la aprobarea Programului național de securitate cibernetică pentru anii 2026-2030

Evaluarea calităţii şi conformităţii

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat** *(Nr. 21/1-113-10423 din 10.10.2025)*	**1.**	**La Capitolul II. ANALIZA SITUAȚIEI** Analiza situației prezintă evoluțiile cadrului instituțional și normativ în domeniul securității cibernetice, însă nu abordează explicit dimensiunea vulnerabilității sau a inechităților sociale, inclusiv din perspectiva de gen, în contextul securității cibernetice. Deși tema este una tehnologică, aspectele legate de accesul inegal la competențe digitale, diferențele de gen în domeniul IT sau expunerea diferitelor categorii sociale la riscuri cibernetice ar fi putut fi menționate pentru a asigura o abordare incluzivă. Se recomandă completarea analizei cu referiri la grupurile mai expuse (ex. elevi, persoane vârstnice, femei, mediul rural), precum și la efectele potențiale ale problemelor identificate asupra acestora.	**Se acceptă parțial.** Observația este pertinentă din perspectiva cadrului metodologic al Hotărârii Guvernului nr. 386/2020 și a Ghidului privind planificarea strategică, care prevăd abordarea dimensiunilor de echitate și incluziune acolo unde este relevant. Deși securitatea cibernetică are o natură preponderent tehnologică, nivelul de reziliență digitală este influențat și de factori socio-economici, precum accesul inegal la competențe digitale în domeniul IT. Prin urmare, reieșind din faptul că la momentul actual nu este ținută o evidență dezagregată a datelor pe grupurile vulnerabile, se propune ca rapoartele privind situația din spațiul cibernetic național să includă, pe viitor, analize care să evidențieze nivelul de expunere al diferitelor categorii (elevi, persoane vârstnice, femei, mediul rural), iar eventualele

				politici ulterioare în domeniul securității cibernetice să reflecte și aceste dimensiuni.
		2.	Totodată, documentul nu include o prognoză a evoluției problemelor în cazul neintervenției Guvernului. Deși analiza actuală sugerează indirect posibile efecte negative, o astfel de analiză este importantă pentru a evidenția riscurile de stagnare, creșterea vulnerabilităților sistemice și posibilele consecințe negative asupra securității și continuității serviciilor publice. Prin urmare, analiza situației ar trebui completată cu o evaluare cauzală și prospectivă, care să asigure o înțelegere realistă a provocărilor existente și o argumentare solidă a necesității politicii propuse.	**Se acceptă.** Analiza situației a fost completată în baza datelor disponibile și a tendințelor constatate cu privire la numărul de incidente cibernetice. Au fost actualizate datele și introdus un paragraf bazat pe datele statistice privind numărul de incidente cibernetice înregistrate în perioada 2018–2024, care evidențiază evoluția ascendentă a riscurilor și impactul potențial în lipsa intervenției guvernamentale.
		3.	**La Capitolul III. OBIECTIVE GENERALE ȘI SPECIFICE** Obiectivul general 2 din Program „*Consolidarea rezilienței țării împotriva criminalității informatice*” este integral acoperit de Programul național de prevenire și combatere a criminalității pentru anii 2026-2030 (Hotărârea Guvernului nr. 654/2025). În aceste condiții, includerea sa în programul analizat nu aduce valoare adăugată și nu are relevanță, întrucât domeniul este deja reglementat și acoperit de un document strategic de politici publice existent.	**Precizare.** Obiectivul menționat este, într-adevăr, conex celui prevăzut în Programul național de prevenire și combatere a criminalității 2026–2030, însă abordarea din cadrul Programului Național de Securitate Cibernetică este complementară, nu contradictorie, asigurându-se o corelare dintre cele două documente. Documentul privind combaterea criminalității informatice se axează pe dimensiunea penală și de aplicare a legii, în timp ce Programul Național de Securitate Cibernetică are ca scop consolidarea capacităților tehnice, instituționale și operaționale ale

				statului în domeniul protecției și reacției la incidente cibernetice. Acțiunile ce se regăseau în Programul național de prevenire și combatere a criminalității 2026–2030, au fost excluse din proiect.
		4.	Analiza indicatorilor asociați obiectivelor specifice relevă mai multe aspecte care necesită clarificare și ajustare pentru a asigura o monitorizare eficientă a progresului. În unele cazuri, indicatorii sunt formulați ca acțiuni, cum este exemplul pentru obiectivul specific 1.4 „*Stabilirea unui cadru pentru controlul și certificarea produselor de protecție criptografică și de semnătură electronică*", ceea ce limitează capacitatea de a evalua rezultatele intervenției. În alte situații, indicatorii propuși sunt de impact și nu reflectă rezultatele imediate ale activităților, cum este cazul scorului de țară pentru obiectivele specifice 1.1 și 1.2. Este necesară o delimitare clară între indicatorii de rezultat și cei de impact. Astfel, la Capitolul III. OBIECTIVE GENERALE ȘI SPECIFICE vor fi incluși exclusiv indicatori de rezultat, care reflectă rezultatul direct al setului de acțiuni aferent fiecărui obiectiv specific. În schimb, la Capitolul IV. IMPACT, vor fi incluși doar indicatorii de impact, care măsoară efectele de ansamblu ale implementării documentului asupra societății pe termen lung, beneficii la nivel macro și îmbunătățiri în relația dintre cetățeni, mediul de afaceri și administrația publică.	**Se acceptă parțial.** Obiectivul specific 1.4 și acțiunile aferente acestuia au fost fuzionate cu obiectivele specifice 1.2 și 3.1, pentru a evita suprapunerile tematice și a consolida coerența logică a programului. În ceea ce privește indicatorii pentru obiectivele specifice 1.1 și 1.2, aceștia nu reflectă scorul de țară în ansamblu (care este inclus la Capitolul IV – indicator de impact), ci doar anumite dimensiuni relevante pentru obiectivele respective. Păstrarea acestor indicatori oferă o bază metodologică solidă și independentă de măsurare a progresului, asigurând o evaluare obiectivă, comparabilă și constantă în timp. Totodată, indicatorii întrunesc criteriile SMART, fiind specifici, măsurabili, accesibili, relevanți și delimitați în timp. Referitor la indicatorii de impact din Capitolul IV, aceștia au fost formulați în conformitate cu prevederile Ghidului privind planificarea

				strategică, ținând cont de indicatorii de impact din strategia sectorială din care derivă prezentul program, în special de indicatorul stabilit pentru Obiectivul general 5 al Strategiei de transformare digitală a Republicii Moldova pentru anii 2023–2030.
		5.	Pentru obiectivul specific 1.3 „*Îmbunătățirea răspunsului la crizele cibernetice prin asigurarea unei abordări coordonate și prin valorificarea structurilor existente pentru menținerea funcțiilor societale vitale*”, indicatorul privind instituirea unui mecanism integrat de gestionare a crizelor cibernetice nu definește rezultatul așteptat. Nu sunt clar indicate tipul mecanismului, componentele, responsabilitățile și modul de funcționare, ceea ce împiedică evaluarea progresului. Este necesară precizarea detaliată a parametrilor și caracteristicilor mecanismului pentru a asigura o evaluare obiectivă a rezultatelor.	**Se acceptă.** Indictorul a fost substituit cu indicator care să ofere o bază metodologică solidă și independentă de măsurare a progresului, asigurând o evaluare obiectivă, comparabilă și constantă în timp.
		6.	Obiectivul specific 3.3 „*Consolidarea cooperării interne între autoritățile și instituțiile publice, precum și cu mass- media pentru a combate eficient manipulările electorale și atacurile cibernetice*” are asociat indicatorul *„Mai multă populație are competențe digitale”* care nu se corelează cu scopul consolidării cooperării între autorități și mass-media pentru combaterea manipulărilor electorale și a atacurilor cibernetice. Este necesară identificarea unui indicator de rezultat relevant, care să reflecte în mod direct eficiența cooperării vizate.	**Nu se acceptă.** Indicatorul „*Mai multă populație are competențe digitale*” este relevant pentru obiectivul specific 3.3, întrucât acesta reflectă rezultatul direct și măsurabil al acțiunilor de conștientizare publică, informare și educare digitală, realizate prin cooperarea între autorități, instituții publice și mass-media. Consolidarea acestei cooperări urmărește tocmai creșterea nivelului de alfabetizare digitală și a rezilienței informaționale a populației, ceea ce contribuie la

				reducerea eficienței manipulărilor și atacurilor cibernetice.
		7.	Se constată că anumiți indicatori, cum ar fi „*Creșterea scorului de țară la capitolul „măsuri de cooperare”*”, se regăsesc la mai multe obiective specifice. Această suprapunere poate genera redundanță și reduce claritatea evaluării progresului pentru fiecare obiectiv în parte, fiind recomandată revizuirea indicatorilor pentru a asigura măsurarea distinctă a rezultatelor fiecărui obiectiv specific.	**Precizare.** Observația este înțeleasă și analizată, însă menținerea indicatorului „*Creșterea scorului de țară la capitolul măsuri de cooperare*” este justificată prin relevanța sa transversală pentru mai multe obiective specifice. Acesta permite o evaluare unitară, obiectivă și comparabilă a progresului în domeniile ce contribuie la consolidarea cooperării instituționale și a capacităților naționale în securitatea cibernetică. De asemenea, indicatorul asigură continuitate în monitorizare și facilitează raportarea coerentă asupra rezultatelor obținute, inclusiv în contextul angajamentelor internaționale. Totodată, cadrul metodologic aplicabil nu exclude utilizarea aceluiași indicator pentru mai multe obiective, atunci când acesta reflectă în mod adecvat rezultatele comune și contribuie la o evaluare consecventă a progresului.
		8.	**La Capitolul IV. IMPACT** Impacturile anticipate ale intervențiilor sunt descrise în mod detaliat, incluzând protecția infrastructurilor critice, consolidarea capacității instituționale, creșterea	**Se acceptă parțial.** Observația este pertinentă din perspectiva cadrului metodologic al Hotărârii Guvernului nr. 386/2020 și

			rezilienței cibernetice a societății, încrederea în serviciile digitale, cooperarea internațională și combaterea criminalității informatice. În contextul creșterii rezilienței cibernetice a societății, ar fi oportun ca documentul să evidențieze și potențialele efecte diferențiate asupra grupurilor sociale, inclusiv din perspectiva de gen, pentru a sprijini incluziunea și echitatea în domeniul securității cibernetice.	a Ghidului privind planificarea strategică, care prevăd integrarea dimensiunilor de echitate și incluziune acolo unde acestea sunt relevante. Deși securitatea cibernetică are o natură predominant tehnologică, reziliența digitală a societății este influențată și de factori socio-economici, precum accesul inegal la competențe digitale și la infrastructură. Prin urmare, reieșind din faptul că, la momentul actual, nu este ținută o evidență dezagregată a datelor privind grupurile vulnerabile, se propune ca, pe viitor, rapoartele privind situația în spațiul cibernetic național să includă analize care să evidențieze nivelul de expunere al diferitelor categorii sociale (elevi, persoane vârstnice, femei, populația din mediul rural). Ulterior, aceste constatări vor putea fundamenta politici și măsuri complementare menite să consolideze incluziunea și echitatea în domeniul securității cibernetice.
		9.	Totodată, indicatorii de impact propuși necesită extindere, astfel încât să reflecte progresul în raport cu toate obiectivele generale ale Programului. În acest sens, se recomandă includerea unor indicatori suplimentari de impact, ancorați logic în obiectivele generale și corelați cu rezultatele strategice urmărite. Sursele de informații	**Precizare.** Observația este înțeleasă și analizată. La stabilirea indicatorilor de impact au fost examinate toate documentele strategice de nivel superior, inclusiv Strategia Națională de Dezvoltare

			pentru identificarea indicatorilor relevanți pot include Tabelul 5 „Indicatorii de evaluare a impactului de dezvoltare a SND” din Strategia Națională de Dezvoltare „Moldova Europeană 2030” (Legea nr. 315/2022), indicatorii de monitorizare a Agendei de dezvoltare durabilă 2030, aprobați prin Hotărârea Guvernului nr. 953/2022, indicatorii de impact prevăzuți în strategia-umbrelă, precum și alți indicatori majori care reflectă impactul politicilor promovate în domeniu.	„Moldova Europeană 2030” și Strategia securității naționale a Republicii Moldova. În cadrul acestor documente nu sunt prevăzuți indicatori care să reflecte în mod direct domeniul securității cibernetice. Prin urmare, singura referință relevantă rămâne Strategia de transformare digitală a Republicii Moldova pentru anii 2023–2030, care a fost utilizată ca bază pentru stabilirea indicatorului de impact. Deși Programul conține un singur indicator de impact, acesta este ambitious și are o relevanță transversală, acoperind toate obiectivele specifice și reflectând, în esență, impactul general al întregului Program.
		10.	**La Capitolul V. COSTURI** Conform sbpct. 18.7 din Regulament, Progamul urmează să detalieze costurile, prin indicarea resurselor financiare necesare pentru implementarea fiecărui obiectiv specific în parte, corelate cu programele/subprogramele bugetare, cu indicarea resurselor financiare planificate pentru perioada următoare, în conformitate cu prevederile Cadrului bugetar pe termen mediu, și a resurselor financiare estimate pentru perioada care excedează Cadrul bugetar pe termen mediu în momentul aprobării programului. De asemenea, se vor indica resursele disponibile din asistența externă și a costurilor	**Se acceptă.** Capitolul costuri a fost modificat conform sugestiilor prezentate.

			neacoperite. Pentru orientare se propune următoarea structură de prezentare a costurilor: Tabelul 1. Estimarea costurilor financiare pentru implementarea obiectivelor ...	
		11.	**La Capitolul VI. RISCURI DE IMPLEMENTARE** Riscurile identificate în document reflectă principalele constrângeri administrative, financiare și instituționale care pot influența implementarea Programului. Autorul va specifica evaluările, analizele sau rapoartele care au stat la baza identificării acestor riscuri. Totodată, analiza poate fi consolidată prin includerea unor riscuri de natură tehnologică, generate de evoluția rapidă și imprevizibilă a amenințărilor cibernetice, de apariția tehnologiilor emergente sau de eventuale întârzieri în adaptarea infrastructurii și a capacităților naționale la noile realități digitale. O asemenea completare ar asigura o abordare mai cuprinzătoare a vulnerabilităților și ar contribui la creșterea rezilienței în procesul de implementare a Programului.	**Se acceptă.** Capitolul VI. RISCURI DE IMPLEMENTARE a fost completat prin indicarea surselor relevante și prin includerea riscurilor de natură tehnologică.
		12.	**La Planul de acțiuni pentru implementarea Programului:** Planul de acțiuni respectă prevederile pct. 19 din Regulament, însă necesită ajustări pentru a fi aliniat la șablonul orientativ anexat (*Anexa Structura planului de acțiuni*), care facilitează prezentarea acțiunilor cu dezagregarea pe ani și evidențierea costurilor acoperite și neacoperite.	**Se acceptă.** Formatul planului de acțiun a fost modificat conform șablonului orientativ prezentat.
		13.	Planul de acțiuni va include exclusiv acțiuni de reformă, axate pe schimbarea sistemului în domeniul de politici publice, care să fie unice și identificabile, și nu va cuprinde acțiuni recurente sau intermediare executate periodic de autoritățile publice. De asemenea, aceste	**Precizare.** La elaborarea Planului de acțiuni s-a ținut cont de cadrul normativ și metodologic aplicabil, asigurând coerența dintre acțiuni și obiectivele

			acțiuni nu trebuie să se suprapună cu cele deja planificate în alte documente sectoriale. De exemplu: Acțiunea nr. 1.2.5. „Crearea cadrului normativ privind securitatea cibernetică a rețelelor 5G” este deja planificată în Programului de implementare, pentru anii 2025-2027, a Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030 (Hotărârea Guvernului nr. 308/2025) – acțiunea nr. 5.1.5.	propuse. Acțiunile au fost formulate astfel încât să reflecte contribuția directă la realizarea obiectivelor specifice ale Programului, punând accent pe măsuri de reformă cu impact sistemic. În ceea ce privește suprapunerea unor acțiuni cu alte documente de politici publice sau de planificare, acestea sunt complementare și nu contradictorii, fiind concepute pentru a consolida eforturile de implementare și a asigura o corelare logică între documentele de politici publice existente.
		14.	Cu referire la acțiunea nr. 1.1.5 „*Publicarea evaluărilor periodice și rapoartelor privind situația din spațiul cibernetic național*” se constată că aceasta ține de activitatea curentă a Agenției pentru Securitate Cibernetică și nu reflectă un rezultat de reformă sau consolidare instituțională. În acest sens, recomandăm reconsiderarea includerii sale în Planul de acțiuni.	**Se acceptă.** Acțiunea a fost reformulată pentru a reflecta o abordare strategică, incluzând realizarea de analize dezagregate privind nivelul de expunere al diferitelor grupuri sociale (elevi, persoane vârstnice, femei, mediul rural). Totodată, aceasta nu vizează activitățile curente ale Agenției pentru Securitate Cibernetică, ci are drept scop oferirea unei radiografii complexe a spațiului cibernetic național, care să servească drept bază pentru formularea și ajustarea ulterioară a politicilor publice în domeniul securității cibernetice.

		15.	Indicatorii de monitorizare asociați acțiunilor din Planul de acțiuni trebuie să fie cuantificați și să reflecte efectele concrete ale intervențiilor, indicând explicit valoarea acestora. De exemplu, pentru acțiunea nr. 3.1.1, indicatorul propus „*Programe de formare continuă elaborate și disponibile pentru diferite grupuri țintă*” are un caracter exclusiv calitativ și nu permite măsurarea concretă a progresului. Pentru evaluarea eficienței acțiunii, indicatorul trebuie cuantificat, de exemplu prin stabilirea unui număr estimativ de programe dezvoltate, de beneficiari instruiți sau de grupuri țintă acoperite. Astfel, se asigură o monitorizare mai clară a rezultatelor și a gradului de acces la formare, inclusiv pentru grupurile vulnerabile și pentru femei.	**Se acceptă.** Indicatorii care nu indicau explicat valoarea acestora au fost revăzuți**.**
		16.	Cu referire la acțiunea nr. 1.2.2 „*Instruirea furnizorilor de servicii din sectoarele critice să utilizeze standardele naționale în domeniul securității informațiilor și a securității cibernetice în cadrul organizațiilor lor pentru a sprijini conformitatea cu Legea nr. 48/2023 privind securitatea cibernetică*”, indicatorul propus „*Cel puțin 90% dintre funcționarii publici vor fi instruiți în domeniul securității cibernetice*” nu este direct relevant pentru acțiunea vizată, care se referă la instruirea furnizorilor de servicii din sectoarele critice. În forma actuală, nu este clar ce rezultate se urmăresc și care este grupul țintă efectiv. Se recomandă revizuirea indicatorului pentru a reflecta obiectivul real al acțiunii și pentru a asigura o monitorizare coerentă.	**Se acceptă.** Acțiunea a fost reformulată, menționând că se referă la furnizorii de servicii din sectoarele critice din domeniul public.
		17.	De asemenea, în contextul aceleiași acțiuni (nr. 1.2.2), indicatorul „*Necesitățile sectoriale de formare/dezvoltare profesională în domeniul securității*	**Se acceptă.** Indicatorul a fost reformulat pentru a măsura rezultatul efectiv al acestuia.

			cibernetice sunt sistematizate în baza solicitărilor” are caracter de activitate pregătitoare și nu măsoară rezultatul efectiv al instruirii. În mod similar, toți indicatorii care nu reflectă progresul sau impactul concret al acțiunilor trebuie revizuiți pentru a fi relevanți, măsurabili și corelați cu obiectivele specifice ale Programului.	
		18.	În analiza acțiunii nr. 1.2.4. „*Consolidarea capacității instituționale a autorităților și instituțiilor publice pentru alinierea acestora la cerințele de securitate stabilite de cadrul normativ în domeniul securității cibernetice*”, se constată că indicatorul propus „*80% din efectivul limită al Agenției pentru Securitate Cibernetică angajați*” nu reflectă în mod direct rezultatul acțiunii. Angajarea personalului în cadrul Agenției pentru Securitate Cibernetică, deși importantă pentru funcționarea acesteia, nu asigură automat consolidarea capacităților la nivelul tuturor autorităților și instituțiilor publice. În acest sens, se recomandă ajustarea indicatorului pentru a măsura efectiv progresul consolidării capacității instituționale în rândul tuturor autorităților vizate.	**Nu se acceptă.** Indicatorul „80% din efectivul limită al Agenției pentru Securitate Cibernetică angajați” reflectă în mod direct rezultatul acțiunii, întrucât consolidarea capacității instituționale începe cu asigurarea resurselor umane necesare pentru funcționarea eficientă a autorității responsabile de coordonarea și implementarea politicilor naționale în domeniul securității cibernetice. Nivelul de ocupare a efectivului-limită al Agenției reprezintă o precondiție esențială pentru dezvoltarea competențelor, oferirea asistenței metodologice și coordonarea proceselor interinstituționale, având un impact direct asupra capacității generale a instituțiilor publice de a se alinia la cerințele cadrului normativ în domeniu.
		19.	Remarcăm că acțiunea nr. 1.2.10. „*Implementarea unei platforme de identificare și management al vulnerabilităților cibernetice pentru infrastructuri critice*” nu precizează clar ce tip de platformă va fi și ce funcționalități va avea. Se recomandă definirea acesteia	**Se acceptă.** Acțiunea și indicatorul au fost reformulați.

			ca „*o platformă informatică centralizată de raportare și gestionare a vulnerabilităților cibernetice, accesibilă furnizorilor de servicii din sectoarele critice*”. De asemenea, indicatorul asociat „*Platforma implementată; cel puțin 90% din furnizorii de servicii integrați*” poate fi clarificat astfel: „*Platforma implementată și funcțională, cu cel puțin 90% dintre furnizorii de servicii identificați conectați și utilizând platforma pentru raportarea vulnerabilităților*”, pentru a asigura o monitorizare precisă a progresului.	
		20.	Obiectivul specific 4.3 „*Consolidarea capacității de diplomație cibernetică internațională*” și acțiunile aferente nu reflectă măsuri de reformă, ci activități curente care derivă din mandatul general al Ministerului Afacerilor Externe în domeniul cooperării internaționale. Crearea unei unități de diplomație cibernetică necesită o justificare clară, întrucât diplomația în domeniul securității cibernetice este deja parte integrantă a atribuțiilor ministerului. Totodată, potrivit raportului de activitate al Ministerului Afacerilor Externe pentru anul 2024[2], au fost deja realizate acțiuni de cooperare bilaterală în domeniul securității cibernetice, inclusiv semnarea unui acord cu Țările de Jos, ceea ce confirmă că obiectivul propus și acțiunile asociate nu aduc o valoare adăugată distinctă și ar putea fi reconsiderate.	**Nu se acceptă.** Necesitatea creării unei unități de diplomație cibernetică este reflectată în capitolul Analiza situației, la domeniul de intervenție IV – cooperare internațională, unde se evidențiază insuficiența capacității instituționale dedicate gestionării și promovării diplomației cibernetice la nivel național. Ministerul Afacerilor Externe, prin intermediul Direcției Cooperare Multilaterală (DCM), asigură implementarea obiectivelor de politică externă ale Republicii Moldova în domeniul securității internaționale, drepturilor omului, apărării, cooperării politico-militare etc., inclusiv cooperarea cu structurile internaționale cu competențe în aceste domenii precum: ONU, OSCE, NATO și

				Consiliul Europei, dar și altele decât cele menționate. Astfel, evoluțiile la nivel global, precum și situația de securitate regională impune necesitatea fortificării cooperării Republicii Moldova pe noi și diverse dimensiuni, inclusiv diplomația cibernetică. În această ordine de idei, se impune necesitatea creării în cadrul MAE a unei subdiviziuni noi cu portofoliu distinct de coordonare a cooperării Republicii Moldova la nivel internațional pe dimensiunea diplomație cibernetică, care a devenit partea esențial în relații cu organizații internaționalei și, dar și în relațiile bilaterale. Crearea subdiviziunii noi propuse va spori reprezentativitatea diplomatică a țării noastre în cadrul platformelor internaționale, precum și contribui la o mai bună analizare și formulare a pozițiilor naționale în cadrul sistemului organizațiilor internaționale. În consecință, va crește importanța funcțională și strategică a MAE în realizarea procesului de participare activă a Republicii Moldova la mecanismul decizional multilateral.

		21.	Pentru acțiunile planificate a fi realizate continuu pe parcursul întregii perioade de implementare a programului, termenul de realizare se va indica în Planul de acțiuni sub forma „2026–2030 (anual)”. Totodată, indicatorii aferenți acestor acțiuni trebuie dezagregați pe fiecare an, astfel încât să permită evaluarea progresului gradual în rapoartele anuale. Această dezagregare facilitează ajustările și permite identificarea timpurie a eventualelor întârzieri sau blocaje în implementare.	**Se acceptă.** Termenii și indicatorii au fost reformulați respectând formatul propus**.**
		22.	Având în vedere observațiile și exemplele prezentate anterior, se recomandă revizuirea întregului Plan de acțiuni, pentru a asigura că fiecare acțiune și indicator asociat este relevant, măsurabil și corelat cu obiectivele de reformă. Exemplele menționate au caracter ilustrativ și nu epuizează toate elementele care pot necesita o evaluare suplimentară.	**Se acceptă.** Planul de acțiuni a fost revizuit, conform sugestiilor prezentate.
		23.	În conformitate cu prevederile pct. 6, sbpct. 2) și 6) din Regulamentul-cadru al subdiviziunii coordonare politici publice și integrare europeană din cadrul aparatului central al ministerului, aprobat prin Hotărârea Guvernului nr. 462/2021, subdiviziunea de coordonare a politicilor din cadrul Ministerului Dezvoltării Economice și Digitalizării va fi implicată direct în procesul de elaborare/coordonare a proiectului.	**Se acceptă.**
2.	**Ministerul Finanțelor** *(Nr. 05-17/209/1411 din 26.09.2025)*	**1.**	Referitor la argumentarea economico-financiară a proiectului (Capitolul V "Costuri” și pct. 4.2 din Nota de fundamentare privind impactul financiar). Autorul prezintă informația privind costul estimativ al implementării proiectului în sumă de cca 99,2 mil. lei și stipulează că o parte considerabilă a acestor cheltuieli nu au acoperire financiară. Subiectul dat urmează a fi detaliat și anume: costuri acoperite pe ani, subprograme	**Se acceptă.** Capitolul V "Costuri” a fost revizut conform șablonului prezentat de Cancelaria de Stat.

			bugetare și autorități/instituții responsabile, precum și costuri neacoperite şi/sau eventual acoperite de către partenerii de dezvoltare**.**	
		2.	Pentru examinarea proiectului Planului de acțiuni pentru implementarea Programului Național de Securitate Cibernetică pentru anii 2026-2030, autorul urmează să prezinte informația detaliată referitor la costurile estimative, sursa de acoperire, perioada de implementare pentru fiecare acțiune/subacțiune în parte, cu specificarea codului programului/subprogramului bugetar, divizate pe ani.	**Se acceptă.** Planul de acțiuni a fost revizut conform șablonului prezentat de Cancelaria de Stat.

Ședința Consiliului pentru coordonarea dezvoltării durabile

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Biroul Național de Statistică**	1.	I. În tabelul 1 „Indicatori de rezultat pentru obiective specifice”: La Obiectivul specific 3.1 „Dezvoltarea unei forțe de muncă calificate în domeniul securității cibernetice prin extinderea oportunităților educaționale”, indicatorul se va expune în următoarea redacție „Ponderea specialiștilor în TIC în rândul populației ocupate”.	**Se acceptă**
		2.	La Obiectivul specific 3.3 „Consolidarea cooperării interne între autoritățile și instituțiile publice, precum și cu mass-media pentru a combate eficient manipulările electorale și atacurile cibernetice”, indicatorul se va expune în următoarea redacție: „Ponderea persoanelor care verifică veridicitatea informațiilor întâlnite pe internet”.	**Se acceptă**

		3.	La Obiectivul Specific 3.4: „Protejarea drepturilor și libertăților persoanelor atunci când datele lor cu caracter personal sunt prelucrate” indicatorul se va expune în următoarea redacție: „Ponderea utilizatorilor de internet care aplică măsuri active de gestionare a confidențialității și a datelor personale”.	**Se acceptă**
			Nota: Indicatorii propuși la obiectivele specifice 3.1, 3.3 și 3.4 vor fi elaborați de BNS în rezultatul cercetării statistice TIC în gospodării care urmează a fi implementată din 2027.	
		4.	II. În Planul de acțiuni pentru implementarea Programului național de securitate cibernetică pentru anii 2026-2030: La acțiunea 3.2.1. „Dezvoltarea unui mecanism național de monitorizare continuă și evaluare a conștientizării riscurilor și implementarea măsurilor de securitate cibernetică de către persoanele fizice și întreprinderi”, din coloana „Autoritate/instituția responsabilă” se va exclude textul „Biroul Național de Statistică”.	**Se acceptă**
2.	**CCDD** ***(Procesul-verbal nr. 22 al ședinței Consiliului pentru coordonarea dezvoltării durabile din 10.11.2025)***	1.	va asigura definitivarea proiectului, ținând cont de observațiile și recomandările din Raportul de evaluare a calității și conformității transmise de Cancelaria de Stat, și va exclude acțiunile care se suprapun sau se dublează cu cele prevăzute în „Programul național de prevenire și de combatere a criminalității pentru anii 2026-2030” și în „Programul de implementare pe anii 2025-2027, a Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030”;	**Se acceptă parțial** Acțiunile ce se dublează cu Programul național de prevenire și de combatere a criminalității pentru anii 2026-2030 au fost excluse. Acțiunea privind „Crearea cadrului normativ privind securitatea cibernetică a rețelelor 5G” considerăm necesar a fi păstrată în acest Program, întrucît proiectul prezentat se alinează Strategiei de securitate cibernetică a UE pentru deceniul digital, care prevede implementarea setului de

				instrumente pentru securitatea cibernetică a rețelelor 5G în statele menmbre, precum și efectuarea, în acest sens, a unei analize aprofundate a ecosistemului 5G și a lanțului de aprovizionare pentru a se identifica și a se monitoriza mai bine principalele active și eventualele dependențe critice. Totodată, în scopul evitării suprapunerii sau dublării acțiunilor, considerăm oportun excluderea acțiunii nr. 5.1.5 din „Programul de implementare pe anii 2025-2027, a Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030”.
	CCDD ***(Procesul-verbal nr. 22 al ședinței Consiliului pentru coordonarea dezvoltării durabile din 10.11.2025)***	2.	pentru Obiectivul specific 4.3 din proiectul Programului, va purta discuții cu Ministerul Afacerilor Externe, inclusiv prin prisma aspectelor menționate în extrasul din procesul-verbal nr. 4 al ședinței Grupului de lucru privind examinarea inițiativelor de instituire/reorganizare a autorităților administrative și a structurilor organizaționale din sfera lor de competență, nr. 30-69-5905 din 30.05.2025;	**Se acceptă** Urmare a discuțiilor dintre MDED și MAE, s-a decis crearea unei unități de diplomație cibernetică în cadrul Ministerului Afacerilor Externe. Ministerul Afacerilor Externe, prin intermediul Direcției Cooperare Multilaterală (DCM), asigură implementarea obiectivelor de politică externă ale Republicii Moldova în domeniul securității internaționale, drepturilor omului, apărării, cooperării politico-militare etc., inclusiv cooperarea cu structurile internaționale cu competențe în aceste domenii

				precum: ONU, OSCE, NATO și Consiliul Europei, dar și altele decât cele menționate. Astfel, evoluțiile la nivel global, precum și situația de securitate regională impune necesitatea fortificării cooperării Republicii Moldova pe noi și diverse dimensiuni, inclusiv diplomația cibernetică. În această ordine de idei, se impune necesitatea creării în cadrul MAE a unei subdiviziuni noi cu portofoliu distinct de coordonare a cooperării Republicii Moldova la nivel internațional pe dimensiunea diplomație cibernetică, care a devenit partea esențial în relații cu organizații internaționalei și, dar și în relațiile bilaterale. Crearea subdiviziunii noi propuse va spori reprezentativitatea diplomatică a țării noastre în cadrul platformelor internaționale, precum și contribui la o mai bună analizare și formulare a pozițiilor naționale în cadrul sistemului organizațiilor internaționale. În consecință, va crește importanța funcțională și strategică a MAE în realizarea procesului de participare activă a

				Republicii Moldova la mecanismul decizional multilateral.
	CCDD ***(Procesul-verbal nr. 22 al ședinței Consiliului pentru coordonarea dezvoltării durabile din 10.11.2025)***	3.	va include Ministerul Energiei în lista autorităților și instituțiilor responsabile la punctul 94 al proiectului Programului, conform solicitării acestuia.	**Se acceptă.**

Avizare

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Cancelaria de Stat** *(nr. 21/1-78-11868 din 24.11.2025)*	1.	***La partea descriptivă a Programului:*** 1. La pct. 4, textul face referire la Programul de activitate al Guvernului „Moldova prosperă, sigură, europeană” (Hotărârea Parlamentului nr. 28/2023). Având în vedere adoptarea Programului de activitate al Guvernului „UE, Pace, Dezvoltare” (Hotărârea Parlamentului nr. 269/2025), această trimitere urmează a fi analizată în contextul noului program de guvernare.	**Se acceptă.** Pct. 4 din proiect a fost modificat în corespundere cu Hotârârea Parlamentului nr. 269/2025, după cum urmează: „4. Totodată, Programul răspunde priorității privind consolidarea securității cibernetice și a infrastructurii IT critice, stabilită în Programul de activitate al Guvernului „UE, Pace, Dezvoltare”, aprobat prin Hotărârea Parlamentului nr. 269/2025.”
		2.	La pct. 7, denumirile documentelor de politici publice necesită corectare pentru a corespunde formelor lor oficiale. În acest sens: • La pct. 7.3, denumirea corectă este *„Strategia națională de apărare a Republicii Moldova pentru anii 2024–2034”*, aprobată prin Hotărârea Parlamentului nr. 319/2024.	**Se acceptă.**

			• La pct. 7.4, se va utiliza titulatura completă: *„Strategia de dezvoltare „Educația 2030” și a Programului de implementare a acesteia pentru anii 2023–2025”*, aprobată prin Hotărârea Guvernului nr. 114/2023. • La pct. 7.6, referința la Programul pentru anii 2026–2030 urmează a fi actualizată forma corectă fiind *„Programul național de prevenire și de combatere a criminalității pentru anii 2026–2030”*, aprobat prin Hotărârea Guvernului nr. 654/2025. Actualizările menționate se aplică și Notei de fundamentare, care necesită corectarea denumirilor documentelor respective.	
		3.	Referitor la Tabelul 1. „Indicatori de rezultat pentru obiective specifice”, din Capitolul III. Obiective generale și specifice, în cazul obiectivului specific 2.1 *„Consolidarea competențelor și abilităților autorităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice și infracțiunilor în domeniul comunicațiilor electronice”*, indicatorul de rezultat *„Creșterea numărului de cauze cu privire la infracțiunile informatice și infracțiunile în domeniul comunicațiilor electronice remise în judecată”* nu reflectă consolidarea capacităților instituționale și poate fi interpretat eronat, întrucât sugerează că progresul ar depinde de creșterea numărului de infracțiuni investigate. Pentru o corelare directă cu obiectivul, se recomandă utilizarea unor indicatori care să măsoare dezvoltarea competențelor, calitatea și eficiența procesului de investigare, precum și efectele acțiunilor implementate. Exemple relevante de indicatori de rezultat includ: timpul mediu de soluționare a unui caz de infracțiune informatică; procentul investigațiilor în care sunt utilizate instrumente criminalistice digitale; numărul sesizărilor depuse de	**Se acceptă.** În vederea asigurării unei corelări coerente și complementare între prezentul Program și Programul național de prevenire și combatere a criminalității pentru anii 2026–2030 aprobat prin Hotărârea Guvernului nr. 654/2025, au fost aliniați indicatorii celor două documente, pentru a garanta consistența și coerența acestora.

			populație prin platforma online de raportare a infracțiunilor informatice.	
		4.	***La partea operațională a Programului:*** Cu referire la acțiunea 2.1.1, nu este clar ce tip de mecanism de coordonare urmează a fi instituit, respectiv structura, forma de organizare și modalitatea de funcționare a acestuia. Se recomandă precizarea naturii mecanismului, inclusiv rolurile autorităților implicate și procesele concrete de cooperare interinstituțională.	**Se acceptă.** Acțiunea și indicatorul au fost revizuiți la propunerea Ministerului Afacerilor Interne.
2.	**Ministerul Apărării** *(nr. 11/1354 din 19.11.2025)*		Lipsa obiecțiilor și propunerilor.	
3.	**Ministerul Sănătății** *(Nr. 27/3655 din 21.11.2025)*		Prin prezenta, Ministerul Sănătății a examinat proiectul de hotărâre cu privire la aprobarea proiectului hotărârii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 (număr unic 905/MDED/2025), autor – Ministerul Dezvoltării Economice și Digitalizării, și vă comunică următoarea cu referire la punctul 47.9 din proiect („Fragmentare și soluții digitale învechite – Existența mai multor sisteme informaționale și registre medicale cu niveluri diferite de maturitate tehnică și securitate, interoperabilitate limitată și dependențe de tehnologii legacy”). Ministerul Sănătății propune ajustarea formulării prin excluderea sintagmei „registre medicale”, întrucât aceasta poate genera interpretări eronate privind funcționalitatea sistemelor digitale din domeniul sănătății. Redacție propusă: 47.9. Fragmentare și soluții digitale învechite – Existența mai multor soluții digitale aflate la niveluri diferite de maturitate tehnică și securitate, cu interoperabilitate limitată și dependențe de tehnologii nealiniate standardelor moderne.	**Se acceptă.** Redacția nouă: *“Fragmentare și soluții digitale învechite – Existența mai multor soluții digitale aflate la niveluri diferite de maturitate tehnică și securitate, interoperabilitate limitată și dependente de tehnologii legacy.”*

4.	**Ministerul Energiei** *(nr. 02-2994 din 25.11.2025)*	1.	Proiectul utilizează art. 6 alin. (3) din Legea nr. 48/2023 ca temei pentru elaborarea Programului, însă articolul respectiv prevede elaborarea și aprobarea de către Parlament a Strategiei naționale de securitate cibernetică, nu a unui Program. Temeiul corect este art. 23 alin. (2) lit. d) din Legea nr. 48/2023, care obligă Guvernul să elaboreze și să prezinte Parlamentului Strategia în termen de 12 luni de la intrarea în vigoare a legii.	**Nu se acceptă.** Temeiul pentru aprobarea Hotărârii Parlamentului este art. 6 alin. (3) din Legea nr. 48/2023.
		2.	Programul național nu include, în lista de documente strategice (pct. 7), Programul de transformare digitală a domeniului energetic 2026–2030, deși acesta stabilește obiective, acțiuni și investiții critice în securitatea cibernetică a domeniului energetic, definit ca sector critic conform HG nr. 860/2024.	**Se acceptă.** Pct. 7 a fost completat cu prevederi privind Programul de transformare digitală a domeniului energetic al Republicii Moldova pentru anii 2026-2030.
		3.	La pct. 30, în lista instituțiilor cu rol și responsabilități în implementarea Programului, Ministerul Energiei nu este inclus, deși sectorul energetic este unul dintre sectoarele critice reglementate, iar Ministerul Energiei coordonează politicile, digitalizarea, implementarea infrastructurii critice energetice și supravegherea conformității operatorilor.	**Precizare.** Ministerul Energiei se regăsește în lista autorităților și instituțiilor menționată la pct. 94 (94.11), urmare a propunerii parvenite în cadrul ședinței Consiliului pentru coordonarea dezvoltării durabile.
		4.	Completarea pct. 7 cu subpct. 7.8: ”7.8. Programul de transformare digitală a domeniului energetic al Republicii Moldova pentru anii 2026–2030, aprobat de Guvern, care stabilește cadrul digitalizării infrastructurii critice energetice, modernizării sistemelor IT/OT, implementării platformelor RNLC, PNME, SINEE, ADMS, HES/MDM, fortificării capacităților cibernetice și creșterii rezilienței în rândul operatorilor de infrastructură energetică.”	**Se acceptă.** Pct. 7 a fost completat cu Programul de transformare digitală a domeniului energetic, urmare a propunerii nr. 2 din aviz, care cuprinde următorul text: ”7.8 Programul de transformare digitală a domeniului energetic al Republicii Moldova pentru anii 2026-2030, aprobat prin Hotărârea Guvernului nr. 652/2025:

				7.8.1 Fortificarea capacităților de securitate cibernetică în domeniul energetic până în anul 2030; 7.8.2 Asigurarea monitorizării 24/7 a infrastructurii critice energetice prin consolidarea capacităților de securitate cibernetică ale operatorilor de infrastructură energetică, inclusiv prin implementarea de mecanisme moderne de detectare și răspuns rapid, în conformitate cu cerințele naționale și directivele UE (inclusiv Directiva NIS2); 7.8.3 Asigurarea certificării tuturor operatorilor de infrastructură critică energetică conform standardelor ISO/IEC 27001 și cerințelor Directivei NIS2; 7.8.4 Asigurarea reducerii timpului de recuperare după incidente cibernetice cu impact semnificativ la maximum patru ore pentru serviciile critice.”
		5.	Completarea pct. 30 (lista autorităților responsabile) cu: ”Ministerul Energiei – autoritate cu responsabilități sectoriale în domeniul securității cibernetice pentru infrastructura critică energetică, în conformitate cu Legea nr. 48/2023, HG nr. 562/2025 și Programul de transformare digitală 2026 2030.”	**Se acceptă.** Proiectul a fost completat cu pct. 42, după cum urmează: „42. Ministerul Energiei este autoritatea cu responsabilități sectoriale în domeniul securității cibernetice

				pentru infrastructura critică energetică.”
		6.	Includerea unui obiectiv specific esențial pentru securitatea cibernetică în domeniul energetic, aliniat cu acțiunile și indicatorii deja aprobați în Programul de transformare digitală a domeniului energetic 2026–2030: ”Implementarea monitorizării 24/7 a infrastructurii critice energetice, în cooperare cu ASC, cu indicatorii: 100% (2028) infrastructură monitorizată și timp de detecție a incidentelor	**Nu se acceptă.** Obiectivele Programului național de securitate cibernetică pentru anii 2026–2030 sunt orientate către consolidarea capacităților și rezilienței cibernetice la nivel național, având un caracter transversal și intersectorial. În acest sens, Programul nu dezvoltă obiective sectoriale specifice, acestea fiind în responsabilitatea documentelor de politici publice sectoriale, inclusiv cele din domeniul energetic. În același timp, obiectivul propus de autorul obiecției este deja reflectat în mod adecvat în partea narativă a Programului, la pct. 7.8.2, unde sunt integrate obiectivele și direcțiile strategice stabilite prin Programul de transformare digitală a domeniului energetic 2026–2030. Astfel, coerența între cele două documente este asigurată fără necesitatea introducerii unui obiectiv specific suplimentar în prezentul Program.
5.	**Ministerul Educației și Cercetării** *(nr. 15/18/25 din 21.11.2025)*		La *Planul de acțiuni pentru implementarea Programului Național de Securitate Cibernetică pentru anii 2026-2030*, Obiectivul general 3. Dezvoltarea competențelor și a culturii de securitate cibernetică în societate, Obiectivul	**Se acceptă.**

			specific 3.1. Dezvoltarea unei forțe de muncă calificate în domeniul securității cibernetice prin extinderea oportunităților educaționale: - La pct. 3.1.1., în coloana *Acțiuni unice identificabile*, cuvintele „programe de recalificare și perfecționare” se vor substitui cu cuvintele „formare profesională”; în coloana *Indicatori de monitorizare*, cuvintele „Program de formare continuă” se vor substitui cu cuvintele „Programe de formare profesională”; - La pct. 3.1.4, în coloana *Indicatori de monitorizare*, sintagma „Mecanism de certificare a calificărilor elaborate” se va substitui cu sintagma „Programe elaborate (inclusiv pentru formatori) și persoane de instruire”; - La pct. 3.1.5., în coloana *Indicatori de monitorizare*, indicatorul se va expune în următoarea redacție: „Curriculumul universitar STEAM actualizat”; - La pct. 3.1.7., în coloana *Indicatori de monitorizare*, indicatorul se va expune în următoarea redacție: „Cel puțin 3 campanii de promovare organizate anual”.	
6.	**Ministerul Infrastructurii și Dezvoltării Regionale** *(nr. 05-6196 din 26.11.2025)*		Lipsa obiecțiilor și propunerilor.	
7.	**Ministerul Afacerilor Interne** *(nr. 38/4187 din 27.11.2025)*	1.	**De ordin conceptual:** Deși proiectul Programului include măsuri orientate spre consolidarea rezilienței sectoarelor critice și protecția serviciilor esențiale, nu este clarificată corelarea acestora cu atribuțiile autorităților sectoriale și cu mecanismele deja instituite în domeniul infrastructurilor critice naționale.	**Nu se acceptă.** Prevederile propuse constituie obiectul unei Hotărîri de Guvern distincte, care, actualmente, este în proces de elaborare și avizare - *proiectul hotărârii Guvernului privind aprobarea Regulamentului cu*

			Caracterul transversal al Programului cu incidență asupra sectoarelor energetice, transporturilor, comunicațiilor, sănătății și ordinii publice, creează riscul suprapunerii responsabilităților, al apariției unor zone neacoperite sau al unei aplicări neuniforme a măsurilor prevăzute. În lipsa unei arhitecturi clare de coordonare interinstituțională, implementarea Programului poate deveni fragmentată și dificil de armonizat cu cadrurile sectoriale existente. În acest context, se recomandă precizarea explicită a cadrului de coordonare interinstituțională, inclusiv rolurile și responsabilitățile autorității competente în domeniul securității cibernetice, ale autorităților sectoriale și ale instituțiilor implicate în reziliența infrastructurilor critice. Aceasta poate fi realizată prin completarea Programului cu o secțiune dedicată mecanismelor de cooperare, fluxurilor de informații și procedurilor comune de intervenție. O astfel de clarificare ar asigura o implementare unitară, coerentă și complementară a acțiunilor prevăzute, evitând suprapunerile și consolidând coordonarea între sectoarele critice.	*privire la elaborarea, actualizarea și implementarea Planului național de răspuns la incidentele cibernetice și crizele cibernetice.* *Obiectivele specifice* ale proiectului de hotărâre de Guvern sunt crearea mecanismelor de interacțiune între entitățile cu competențe sau activități în domeniul securității cibernetice și protecției infrastructurii critice, în vederea elaborării, menținerii în stare de actualitate și implementare a Planului național de răspuns la incidente cibernetice și gestionare a crizelor în domeniul securității cibernetice. Proiectul de act normativ are ca *obiect de reglementare* cerințele față de conținutul Planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice, procesul de elaborare, inclusiv etapele acestui proces, modul de actualizare și implementare a Planului, atribuțiile autorităților și instituțiilor publice în acest proces, drepturile și obligațiile persoanelor juridice implicate în procesul de elaborare, actualizare și implementare a Planului, precum și procedurile de interacțiune dintre acestea.
		2.	Având în vedere că proiectul Programului atribuie o importanță esențială infrastructurilor critice și	**Se acceptă.**

			menționează impactul potențial al incidentelor cibernetice asupra serviciilor esențiale, se constată absența oricărei referințe la Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale. În acest context, se recomandă completarea secțiunii dedicate cadrului normativ din partea introductivă a Programului prin includerea trimiterii la Legea nr. 223/2025, precum şi armonizarea terminologiei utilizate din această lege (de ex.: „gestionar de infrastructură critică națională”, „criterii sectoriale și intersectoriale”), în vederea asigurării coerenței conceptuale şi a alinierii conținutului proiectului Programului la cadrul juridic aplicabil în domeniul infrastructurilor critice de importanță strategică națională.	Proiectul a fost completat corespunzător.
		3.	**La proiectul Programului:** La Capitolul I „Introducere”, pct. 7.6, textul *„Programul de prevenire și combatere a criminalității pentru anii 2022-2025 (HG nr. 948/2022)”* urmează a fi exclus, întrucât Programul național de securitate cibernetică nu cuprinde perioada anilor 2022-2025. Totodată, textul *„și Proiectul de Program”* se va substitui cu cuvântul *”Programul”*, iar după anul 2030, în paranteze, se va indica (HG nr. 654/2025).	**Se acceptă.**
		4.	Capitolul I „Introducere”, urmează a fi completat cu informația privind părțile implicate în elaborarea Programului (conform pct. 18.1 din Regulamentul cu privire la planificarea strategică, aprobat prin HG nr. 386/2020).	**Precizare.** Pct. 15 al Programului face trimitere generică la autoritățile implicate în proces, care au atribuții relevante domeniului securității cibernetice sau conexe acestuia.
		5.	În tot textul Programului, înainte de cifre, propozițiile vor fi completate cu cuvântul „anul/anii” la cazul gramatical corespunzător.	**Se acceptă.**

		6.	Din pct. 31, textul *„cu privire la instituirea, organizarea și funcționarea Consiliului coordonator în domeniul securității cibernetice”* se propune a fi exclus, acesta fiind de prisos (se repetă).	**Nu se acceptă.** Este expres stipulată denumirea hotărîrii de Guvern.
		7.	În punctele 34 și 35, textul *„în subordinea Cancelariei de Stat”* urmează a fi substituit cu textul *„instituție publică în subordinea Guvernului”*.	**Se acceptă parțial.** Textul a fost modificat în corespundere cu Hotărârea Guvernului nr. 414/2018.
		8.	Punctul 37 urmează a fi expus în următoarea redacție: *„37. Centrul pentru combaterea crimelor informatice al Inspectoratului național de investigații al Inspectoratului General al Poliției al Ministerului Afacerilor Interne este unitatea principală de investigare și prevenire a infracțiunilor informatice și a celor conexe, precum și a infracțiunilor grave, deosebit de grave și excepțional de grave cu rezonanță socială sporită, comise prin utilizarea sistemelor informatice, prin organizarea activității speciale de investigații. Centrul acordă suport și asistență subdiviziunilor teritoriale ale poliției în materie de criminalitate cibernetică și dovezi electronice. Centrul are un acord bilateral cu CERT-GOV pentru schimbul de informații privind incidentele cibernetice. Centrul cooperează, de asemenea, cu Serviciul de Informații și Securitate și le oferă, la solicitare, informații despre situația din spațiul cibernetic național”.* Noua redacție a punctului 37 are ca scop clarificarea și consolidarea rolului Centrului pentru combaterea crimelor informatice al Inspectoratului național de investigații (în continuare - Centru), subliniind importanța acestuia în combaterea infracțiunilor informatice și conexe. Prin reformularea propusă, se dorește o mai bună precizare a responsabilităților și	**Se acceptă.**

			atribuțiilor acestui Centru, în contextul unei coordonări mai eficiente cu celelalte autorități naționale și internaționale implicate în securitatea cibernetică. În primul rând, prin utilizarea expresiei „principalul organism responsabil”, se subliniază statutul de lider al Centrului. Astfel, se elimină orice ambiguitate cu privire la rolul său esențial, consolidându-se ideea că Centrul este autoritatea centrală în combaterea criminalității cibernetice, ce include atât infracțiunile informatice directe, cât și cele conexe, ce pot afecta grav securitatea națională și ordinea publică. De asemenea, prin această propunere se urmărește detalierea tipurilor de infracțiuni vizate de activitatea Centrului, făcând referire explicită la „infracțiunile grave, deosebit de grave și excepțional de grave cu impact social semnificativ”. Aceasta adaugă o dimensiune mai precisă a tipologiilor de infracțiuni pe care Centrul le investighează, evidențiind importanța deosebită a cazurilor cu rezonanță socială, ce pot avea un impact major asupra siguranței naționale. Astfel, activitatea Centrului devine mult mai bine conturată, iar rolul său în gestionarea unor astfel de cazuri devine evident. Mai mult decât atât, formularea propusă pune accent pe colaborarea activă și continuă a Centrului cu alte structuri ale Ministerului Afacerilor Interne și cu autorități externe. Prin referirea la „suportul tehnic” și „managementul dovezilor electronice”, se subliniază importanța asistenței acordate subdiviziunilor teritoriale al Poliției în investigarea infracțiunilor informatice, dar și valoarea adăugată pe care Centrul o aduce în domeniul	

			colectării și procesării probelor digitale, esențiale în cadrul procedurilor judiciare. De asemenea, prin introducerea unei referințe explicite la acordurile de cooperare, precum cel cu CERT-GOV pentru schimbul de informații privind incidentele cibernetice, se demonstrează angajamentul Centrului de a lucra în sinergie cu alte instituții naționale relevante în gestionarea incidentelor de securitate cibernetică. Acest tip de cooperare inter-instituțională este esențial pentru o reacție rapidă și eficientă în fața atacurilor cibernetice. Nu în ultimul rând, formularea propusă include și cooperarea cu Serviciul de Informații și Securitate, prin furnizarea de informații „la solicitare”, ceea ce reflectă rolul activ al Centrului în cadrul unui sistem mai larg de securitate națională, asigurând o monitorizare constantă a amenințărilor din spațiul cibernetic. Acesta subliniază importanța schimbului de informații și a unui răspuns coordonat între autoritățile de securitate națională.	
		9.	Se constată că Programul este fundamentat pe acquis-ul Uniunii Europene şi pe instrumentele juridice sectoriale relevante (inclusiv Directiva (UE) 2022/2555 (Directiva NIS 2), prevederile Comunicării Comune către Parlamentul European și Consiliul „Strategia de securitate cibernetică a UE pentru deceniul digital”, precum și alte acte europene în curs de implementare). În acest context, documentul operează justificat cu terminologia specifică acquis-ului, inclusiv termeni ce țin de sectoarele critice, entitățile esențiale şi furnizorii de servicii în domenii de importanță strategică. Din perspectiva aplicării la nivel național, este necesară consolidarea conexiunii dintre Program şi arhitectura deja existentă în materie de securitate națională, continuitatea guvernării și gestionarea crizelor, astfel	**Se acceptă parțial.** La punctul 56 din Program conține prevederi referitor la Legea nr. 248/2025. În același timp, acesta a fost ajustat în vederea asigurării unei terminologii uniforme cu Legea nr. 248/2025.

			încât acțiunile prevăzute să fie absorbite uniform în mecanismele instituționale actuale, evitându-se paralelismele procedurale și eventualele suprapuneri funcționale. Având în vedere prevederile pct. 42-44 din Program, care descriu cadrul național de management al crizelor şi rolul Centrului Național de Management al Crizelor, se impune necesitatea precizării raportării mecanismelor de gestionare a incidentelor şi crizelor cibernetice la sistemul general instituit prin Legea nr. 248/2025 privind managementul situațiilor de criză, întrucât ar asigura corelarea proceselor specifice domeniului securității cibernetice cu arhitectura națională de coordonare a crizelor şi ar conferi Programului coerență instituțională. În acest sens, este oportună completarea proiectului după pct. 44, cu pct. 45 cu următoarea prevedere: *„45. Gestionarea incidentelor şi crizelor de securitate cibernetică se realizează în concordanță cu mecanismele şi procedurile naționale de management al situațiilor de criză prevăzute de Legea nr. 248/2025 privind managementul situațiilor de criză”.* Respectiv pct. 45 din actuala redacție devine pct. 46.	
		10.	Totodată, dacă la pct. 42 se face trimitere la Legea Nr. 248/2025 privind managementul situațiilor de criză, respectiv crearea și reglementarea activității Centrului Național de Management al Crizelor, respectiv, într-o consecutivitate logică, urmează a fi indicate actele normative prin care au fost create și celelalte autorități/instituții enumerate mai sus în Program.	**Se acceptă parțial.** Referința la Legea nr. 248/2025 a fost exclusă din acest punct și completat capitolul Introducere.
		11.	La pct. 61, subpct. 61.4 din Capitolul II, textul: „Insuficiența de profesioniști în securitatea cibernetică pe întregul ciclu de descoperire, constatare, investigare, urmărire și judecare a faptelor ilegale comise”, urmează	**Se acceptă.**

			a fi substituit cu textul „Insuficiența personalului calificat în securitatea cibernetică pe întregul ciclu de prevenire, investigare, urmărire și judecare a faptelor ilegale comise în spațiul cibernetic”. Noua redacție urmărește să clarifice și să reflecte mai fidel provocările reale cu care se confruntă Republica Moldova în ceea ce privește resursele umane din domeniul securității cibernetice. Formularea anterioară, deși corectă conceptual, nu surprindea în mod suficient întregul spectru al responsabilităților instituțiilor statului implicate în reacția la amenințările cibernetice. Prin utilizarea expresiei „personalului calificat”, textul propus evidențiază faptul că problema nu se rezumă doar la numărul insuficient de specialiști, ci și la competențele avansate necesare pentru a face față naturii din ce în ce mai complexe a infracțiunilor comise în mediul digital. Astfel, accentul se mută pe calitatea și nivelul de pregătire al personalului, nu doar pe simpla prezență numerică a acestuia. În plus, redactarea nouă introduce o formulare mai completă a etapelor în care este necesar personal specializat. În locul enunțului anterior, care se referea doar la „descoperire, constatare, investigare, urmărire și judecare”, noua versiune încorporează expres termenul „prevenire”, o componentă crucială într-un sistem modern de securitate cibernetică. Prevenirea incidentelor, prin monitorizare, anticipare și evaluarea riscurilor, este un element fundamental care contribuie la reducerea costurilor și a impactului atacurilor informatice. Astfel, noul text reflectă mai bine abordarea proactivă adoptată de statele moderne în gestionarea amenințărilor cibernetice. Totodată, completarea cu sintagma „faptele ilegale comise în spațiul cibernetic” conferă o claritate juridică superioară. Această precizare	

			permite conturarea exactă a domeniului vizat, evitând interpretările ambigue și făcând trimitere directă la natura specifică a infracțiunilor pentru care este necesară formarea și consolidarea capacităților instituționale.	
		12.	În cadrul proiectului de Program, se constată o eroare la numerotarea subpunctelor. Mai exact, subpunctele 84.1–84.6 sunt incluse la punctul 85, ceea ce reprezintă o nepotrivire în numerotarea și structurarea documentului. Astfel, se impune corectarea acestei erori, astfel încât subpunctele 84.1–84.6 să fie incluse corect în cadrul punctului 84, pentru a asigura o numerotare consecventă și logică în document.	**Se acceptă.**
		13.	Deși în Capitolul II „Analiza situației” au fost descrise problemele existente în domeniu, totuși acesta nu se referă la posibilele consecințe și impactul acestora asupra grupurilor principale vulnerabile afectate, cu folosirea datelor disponibile dezagregate conform criteriilor de gen, vârstă, etnie etc. (pct. 18.2 din Regulamentul cu privire la planificarea strategică, aprobat prin HG nr. 386/2020).	**Se acceptă parțial.** Observația este pertinentă din perspectiva cadrului metodologic al Hotărârii Guvernului nr. 386/2020 și a Ghidului privind planificarea strategică, care prevăd abordarea dimensiunilor de echitate și incluziune acolo unde este relevant. Deși securitatea cibernetică are o natură preponderent tehnologică, nivelul de reziliență digitală este influențat și de factori socio-economici, precum accesul inegal la competențe digitale în domeniul IT. Prin urmare, reieșind din faptul că la momentul actual nu este ținută o evidență dezagregată a datelor pe grupurile vulnerabile, se propune ca rapoartele privind situația din spațiul cibernetic național să includă, pe viitor, analize care să evidențieze

				nivelul de expunere al diferitelor categorii (elevi, persoane vârstnice, femei, mediul rural), iar eventualele politici ulterioare în domeniul securității cibernetice să reflecte și aceste dimensiuni.
		14.	Capitolul III „Obiective generale și specifice” se propune a fi divizat în două capitole separate – „Obiective generale” și „Obiective specifice” și vor fi completate cu informații relevante, conform cerințelor stipulate în (pct. 8 subpunctele 18.3 și 18.4 din Regulamentul cu privire la planificarea strategică, aprobat prin HG nr. 386/2020).	**Nu se acceptă.** Hotărârea Guvernului nr. 386/2020 cu privire la planificarea strategică nu stabilește obligativitatea divizării în capitole distincte a obiectivelor generale de cele specifice. Abordarea de a avea aceste două capitole este reflectată în majoritatea programelor (ex. Program național de prevenire și de combatere a criminalității pentru anii 2026–2030, aprobat prin Hotărârea Guvernului nr. 654/2025). În același timp, acestea respectă cerințele stabilite de pct. 18 subpunctele 18.3 și 18.4 din Regulamentul cu privire la planificarea strategică.
		15.	În pct. 81, textul „Programul de prevenire și combatere a criminalității 2022–2025 (și proiectul pentru perioada 2026–2030)”, se va substitui cu textul „Programul de prevenire și combatere a criminalității pentru anii 2026-2030”.	**Se acceptă.**
		16.	Un compartiment separat va constitui Capitolul „Indicatori de monitorizare”, care va fi completat conform cerințelor prevăzute în (subpunct. 18.5 din Regulamentul cu privire la planificarea strategică, aprobat prin HG nr. 386/2020).	**Precizare.** Indicatorii de monitorizare sunt integrați în mod corespunzător în structura Programului: indicatorii de rezultat sunt prezentați pentru fiecare

				obiectiv specific în Capitolul III, iar indicatorii de impact, corelați cu obiectivele generale, sunt incluși în Capitolul IV. Această abordare respectă cerințele metodologice prevăzute la subpunctul 18.5 din Regulamentul aprobat prin HG nr. 386/2020, fără a impune necesitatea creării unui capitol separat dedicat indicatorilor.
		17.	Cu referire la beneficiul indicat la pct. 85 subpct. 85.1 „Îmbunătățirea protecției infrastructurilor critice”, se constată că Programul utilizează sintagma „infrastructură critică” fără a delimita cadrul juridic la care aceasta se raportează, deși noțiunea este definită diferit prin Legea nr. 120/2017 privind prevenirea și combaterea terorismului şi prin Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale. În acest sens, se impune clarificarea expresă a faptului dacă măsurile propuse vizează infrastructurile critice în accepțiunea Legii nr. 120/2017, pentru care Nomenclatorul este deja constituit şi gestionat de autoritatea competentă, sau infrastructurile critice naționale în sensul Legii nr. 223/2025, pentru care procesul de identificare şi desemnare se află în curs, urmând a fi finalizat până la data de 22 februarie 2027 de către Centrul Național de Coordonare a Protecției Infrastructurilor Critice. Precizarea este necesară întrucât nivelul de maturitate instituțională, cadrul operațional și competențele autorităților implicate diferă substanțial între cele două categorii, iar formularea actuală nu permite determinarea domeniului exact asupra căruia Programul urmărește să	**Precizare.** Programul abordează protecția infrastructurilor critice din perspectivă strategică, fără a redefini sau restrânge sfera juridică stabilită de legislația în vigoare. Delimitarea exactă a cadrului aplicabil — fie cel prevăzut de Legea nr. 120/2017 privind prevenirea și combaterea terorismului, fie cel stabilit prin Legea nr. 223/2025 privind identificarea, desemnarea și protecția infrastructurilor critice naționale — urmează a fi realizată la etapa de elaborare și implementare a intervențiilor normative. În acest sens, toate acțiunile programului vor fi corelate cu procesele instituționale aflate în derulare, inclusiv cu identificarea și desemnarea infrastructurilor critice naționale până în anul 2027. Această abordare permite menținerea

			intervină în sensul „îmbunătățirii protecției”, ceea ce poate genera dificultăți de implementare şi monitorizare.	coerenței cu cadrul legal existent, evită suprapunerile și asigură flexibilitatea necesară pentru adaptarea intervențiilor la arhitectura juridică definitivă stabilită de autoritățile competente.
		18.	La Capitolul VII „Autorități și instituții responsabile”, subpunctul 94.9 „Inspectoratul General al Poliției”, urmează a fi exclus și trecut în paranteze, la subpunctul 94.3 - Ministerul Afacerilor Interne, similar subpunctului 94.8.	**Se acceptă.**
		19.	Capitolului VII „Monitorizare, evaluare și raportare”, urmează a fi revizuit, un exemplu pozitiv în acest sens constituind Capitolul IX din Programul național de prevenire și combatere a criminalității pentru anii 2026-2030, aprobat prin HG nr. 654/2025, în special referitor la completarea capitolului cu informații privind modalitatea de evaluare intermediară, precum și referitor la conținutul rapoartelor de evaluare.	**Nu se acceptă.** Capitolului VII „Monitorizare, evaluare și raportare” întrunește toate elementele stabilite de Hotărârea Guvernului 386/2020 cu privire la planificarea strategică și cadrul metodologic aferent.
		20.	**La proiectul Planului de acțiuni:** Cu referire la acțiunile 1.1.1 şi 1.1.2 din Obiectivul specific 1.1, Obiectivul general 1, se constată că acestea prevăd dezvoltarea a două sisteme informaționale separate, deşi ambele au, în esență, aceeași finalitate, asigurarea schimbului de informații şi a raportării, inclusiv a incidentelor. În aceste condiții, crearea distinctă a unui Registru de stat al incidentelor și paralel, a unui sistem destinat exclusiv schimbului de informații între furnizorii de servicii din sectoarele critice apare ca nejustificată, întrucât divizarea artificială a funcționalităților poate genera suprapuneri, fragmentarea fluxurilor informaționale şi dificultăți ulterioare de integrare.	**Precizare** La această etapă de planificare strategică, Programul stabilește doar direcțiile de intervenție, fără a decide în mod definitiv arhitectura tehnică a sistemelor informaționale. În procesul de elaborare sau revizuire a conceptelor tehnice pentru acțiunile 1.1.1 și 1.1.2 va fi evaluată oportunitatea creării a două sisteme distincte sau a unui singur sistem integrat. Decizia finală privind arhitectura sistemului va fi fundamentată pe

			În acest sens, se menționează că Legea nr. 223/2025 prevede posibilitatea instituirii în cadrul Ministerului Afacerilor Interne a unui mecanism de comunicare şi avertizare timpurie, cu rol de sistem național securizat de informare în domeniul protecției infrastructurilor critice naționale, destinat gestionării integrate a incidentelor, amenințărilor, vulnerabilităților şi riscurilor aferente acestor infrastructuri. Acest mecanism are rolul de a asigura un cadru unitar de schimb de informații, necesar atât în procesul de prevenire şi contracarare a riscurilor, cât și în diminuarea impactului asupra serviciilor esențiale. În aceste circumstanțe, se impune analizarea oportunității integrării funcționalităților prevăzute la acțiunile 1.1.1 şi 1.1.2 într-o singură platformă interoperabilă, corelată cu mecanismul prevăzut de Legea nr. 223/2025, în vederea evitării paralelismelor, asigurării eficienței instituționale şi consolidării arhitecturii naționale de schimb de informații în domeniul securității infrastructurilor critice.	criterii de eficiență operațională, interoperabilitate, optimizarea resurselor și consolidarea cadrului național de schimb de informații în domeniul securității cibernetice și protecției infrastructurilor critice.
		21.	La acțiunea 1.2.3. din rubrica „Instituție responsabilă” textul „alte autorități și instituții responsabile” se va exclude, acesta fiind înlocuit cu denumirea unor instituții concrete, care ar urma să execute acțiunea.	**Se acceptă.**
		22.	Indicatorul de monitorizare prevăzut la acțiunea 2.1.1. din Obiectivul specific 2.1 exprimat prin redacția: „Instituirea unui mecanism de coordonare și cooperare interinstituțională și stabilirea principiilor obiective strategice de funcționare a acestuia pentru combaterea criminalității informatice, cu implicarea autorităților publice responsabile de aplicarea legii și cele responsabile de securitatea națională” se recomandă a fi substituit cu textul: „2.1.1. Acord de schimb de informații și de coordonare între autoritățile publice”. Propunerea	**Se acceptă.**

			de modificare a indicatorului de monitorizare, astfel încât să se substituie formularea actuală cu un text mai concis și mai direct, are la bază mai multe considerente esențiale care vizează eficiența implementării măsurilor de combatere a criminalității informatice. În redacția actuală, indicatorul prevede instituirea unui mecanism complex de „coordonare și cooperare interinstituțională” și stabilirea „principiilor obiective strategice de funcționare” pentru combaterea criminalității informatice. Deși scopul enunțat este clar, formularea este destul de amplă și generală, ceea ce poate duce la dificultăți în înțelegerea exactă a acțiunilor specifice ce trebuie întreprinse și, de asemenea, la provocări în ceea ce privește evaluarea progresului și impactului acestor măsuri. Astfel, propunerea de reformulare a indicatorului în termenii „Acord de schimb de informații și de coordonare între autoritățile publice” aduce un nivel de claritate și pragmatism necesar. Această formulare pune accent pe concretizarea acțiunilor interinstituționale prin intermediul unui acord formal de cooperare, ceea ce presupune un mecanism operativ de schimb de informații și coordonare între autoritățile publice relevante. Substituirea termenilor vagi cu unul specific - „Acord”, asigură o bază legală și operațională clară, care va facilita implementarea măsurilor de securitate și monitorizare a activităților de combatere acriminalității informatice. În plus, modificarea propusă reflectă o abordare mai eficientă, concentrată pe cooperarea între autoritățile cheie responsabile de aplicarea legii și securitatea națională, fără a implica proceduri excesiv de complexe care pot întârzia procesul de implementare. În locul unei descrieri teoretice a unui mecanism de funcționare, noul	

			text se concentrează pe esențialul schimbului de informații și coordonării, esențiale pentru combaterea rapidă și eficientă a infracționalității informatice.	
		23.	În cazul în care totuși se menține acțiunea actuală (acțiunea 2.1.1.) cuvântul ,,principiilor" se va substitui cu cuvântul ,,principalelor".	**Se acceptă.**
		24.	Redacția acțiunii nr.2.1.2 din Obiectivul specific 2.1 – Consolidarea competențelor și abilităților ale entităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice şi infracțiunilor în domeniul comunicațiilor electronice se recomandă a fi expusă după cum urmează: *„2.1.2. Consolidarea continuă a capacităților de investigare a infracțiunilor informatice, inclusiv în domeniul criminalisticii digitale"*. Propunerea de reformulare are avantajul de a adresa mai clar direcțiile de acțiune specifice, punând accentul pe dezvoltarea „capacităților de investigare" în mod continuu. Această modificare subliniază ideea de formare și actualizare constantă a resurselor instituționale și a personalului, ceea ce este esențial într-un domeniu în continuă evoluție, cum este cel al criminalității informatice. De asemenea, introducerea termenului „criminalistica digitală" în formularea nouă adaugă o dimensiune esențială activităților de investigare a infracțiunilor informatice. Criminalistica digitală se referă la tehnicile și procedurile specifice necesare în colectarea, păstrarea, analiza și prezentarea probelor digitale, un domeniu esențial pentru succesul anchetelor în cazurile de criminalitate cibernetică. Aceasta subliniază importanța specializării în acest domeniu, având în vedere complexitatea și tehnologia avansată implicată în atacurile informatice.	**Se acceptă.**

			În plus, formularea „capacităților de investigare” este mai eficientă decât „competentele și abilitățile”, întrucât se referă la un ansamblu mai larg de resurse, abilități tehnice, proceduri și infrastructuri care trebuie consolidate în mod continuu, pe măsură ce noile provocări din domeniul securității cibernetice apar. Astfel, se creează o viziune mai coerentă și integrată asupra capacităților instituțiilor responsabile de aplicarea legii.	
		25.	Acțiunea 2.1.3 din Obiectivul specific 2.1 „Consolidarea competențelor și abilităților ale entităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice şi infracțiunilor în domeniul comunicațiilor electronice” se recomandă a fi transferată la Obiectivul specific 3.3, întrucât ține de atribuțiile exclusive ale Agenției Securitate Cibernetică, în special ”cooperarea cu operatorii de infrastructură critică” și ”detectarea și raportarea amenințărilor și incidentelor cibernetice și a vulnerabilităților serviciilor și produselor de tehnologie a informației”. Respectiv, Ministerul Afacerilor Interne urmează a fi exclus ca instituție responsabilă din această acțiune. În acest context, este esențial să se facă o distincție clară între rolul Ministerului Afacerilor Interne, care se concentrează pe aplicarea legii și investigarea criminalității informatice, și responsabilitățile specifice ale Agenției Securitate Cibernetică în ceea ce privește protecția infrastructurilor critice și gestionarea incidentelor de securitate cibernetică. De asemenea, activitățile de detectare, raportare și prevenire a amenințărilor și incidentelor cibernetice, precum și cooperarea cu operatorii de infrastructură critică, sunt funcții directe ale Agenției Securitate Cibernetică, care dispune de expertiza tehnică și	**Se acceptă parțial.** Instituția responsabilă a fost modificată, în vederea stabilirii Agenției de Securitate Cibernetică drept autoritate prim responsabilă de realizarea acestei acțiuni. Totodată, menționăm că acțiunea este integrată logic în Obiectivul specific 2.1, care se concentrează pe consolidarea capacităților organelor de aplicare a legii.

			resursele necesare pentru a gestiona aceste aspecte. În acest sens, propunerea de a muta această acțiune în cadrul Obiectivului specific 3.3, care este dedicat securității cibernetice și protecției infrastructurilor critice, reflectă mai corect structura responsabilităților instituționale în domeniul securității cibernetice și clarifică atribuțiile fiecărei instituții. Transferul este, de asemenea, justificat de evoluția specifică a domeniului securității cibernetice, care presupune un nivel înalt de specializare și un răspuns rapid și coordonat la incidentele cibernetice, competențe care sunt în mod exclusiv deținute de Agenția Securitate Cibernetică. Aceasta este instituția națională responsabilă pentru coordonarea tuturor activităților de prevenire, detectare și răspuns la amenințările cibernetice, inclusiv în domeniul infrastructurii critice, și nu se poate confunda cu rolul Ministerului Afacerilor Interne, care se ocupă în principal cu prevenirea și combaterea criminalității informatice, acoperind alte aspecte legate de aplicarea legii.	
		26.	Se propune ca titlul Obiectivului specific 2.2 să fie reformulat în „Implementarea unor instrumente și soluții moderne în vederea prevenirii și combaterii criminalității cibernetice”, cu scopul de a reflecta mai clar și mai concis direcția strategică a acțiunilor prevăzute. Noua redacție subliniază importanța adoptării unor instrumente și soluții moderne, accentuând nu doar aspectul operațional, ci și cel tehnologic, esențial pentru eficiența măsurilor de securitate cibernetică. În plus, formularea pune în prim plan obiectivul principal al acestui domeniu, și anume prevenirea și combaterea criminalității cibernetice, astfel încât titlul să reflecte în mod direct scopul și finalitatea activităților incluse în cadrul	**Se acceptă.**

			obiectivului specific. Această reformulare contribuie la o mai bună claritate conceptuală și facilitează înțelegerea acțiunilor, măsurilor și rezultatelor așteptate, asigurând coerența și consistența întregului Program național de securitate cibernetică.	
		27.	De asemenea, este necesară verificarea suplimentară a țintelor la obiectivul specific 2.2. „Crearea de instrumente tehnologice eficace și avansate pentru prevenirea, detectarea și investigarea eficientă a criminalității informatice” (în tabel), unde pentru anii 2024 și 2028 țintele constituie „număr de instrumente”, iar pentru anul 2030 – „soluții și procente”.	**Se acceptă.** Țintele au fost revăzute.
		28.	La acțiunea 4.2.1. „Elaborarea politicilor de comunicare strategică internă și conectarea 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” din Obiectivul specific 4.2, urmează excluderea Inspectoratului General al Poliției al Ministerului Afacerilor Interne ca instituție responsabilă, având în vedere natura specifică a activităților implicate în această acțiune. Comunicarea strategică, atât internă, cât și externă, necesită o abordare mai complexă și mai specializată, care să integreze atât politici de securitate informațională, cât și o coordonare eficientă între diverse entități naționale și internaționale. Totodată, excluderea Inspectoratului General al Poliției al Ministerului Afacerilor Interne din această acțiune este justificată prin faptul că activitățile de comunicare strategică și promovare a securității informaționale sunt în mod direct legate de competențele altor autorități și instituții naționale, vizate inclusiv în această acțiune, cu	**Se acceptă parțial.** Lista autorităților a fost revăzută cu includerea tutoror autorităților care au funcții în domeniul securității, apărării și ordinii publice.

			responsabilități în domeniul comunicării strategice și al securității informaționale, nu ale Poliției. Inspectoratul General al Poliției se concentrează mai degrabă pe prevenirea și combaterea infracțiunilor, inclusiv a celor informatice, dar nu are atribuții directe în elaborarea și coordonarea politicilor de comunicare strategică pe plan național sau în integrarea acestora la nivel extern.	
8.	**Ministerul Finanțelor** *(05-17/221/1650 din 28.11.2025)*		Ministerul Finanțelor a examinat, repetat, proiectul hotărârii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 și comunică că conștientizează importanța proiectului. Cu toate acestea, implementarea proiectului necesită resurse financiare considerabile care la moment sunt planificate doar parțial în proiectul Legii bugetului de stat pe anul 2026. Astfel, asumarea unor activități fără acoperire financiară poate duce la realizarea incompletă a indicatorilor propuși și valorificarea ineficientă a mijloacelor financiare. Astfel, la argumentarea economico-financiară a proiectului (Capitolul V "Costuri" și pct. 4.2 din Nota de fundamentare privind impactul financiar) autorul prezintă costul estimativ al implementării proiectului în sumă de cca 79,9 mil lei, aceasta fiind actualizată (comparativ cu versiunea inițială a proiectului) prin diminuarea cu 19,3 mil lei, nefiind prezentate argumente justificative în acest sens. În ce privește realizarea Programului din contul și limita alocațiilor aprobate în bugetele autorităților responsabile, ținem să evidențiem că acest aspect va fi posibil de estimat ulterior aprobării și publicării Legii bugetului de stat pentru anul 2026. În aceste condiții, autorul urmează să revină cu precizarea costurilor detaliate și sumelor aprobate pe subprograme	**Precizare.** Costul a fost diminuat urmare a revizuirii planului de acțiuni, inclusiv excluderea acțiunii privind crearea instrumentului inteligent pentru combaterea amenințărilor cibernetice și a atacurilor împotriva criminalității cibernetice achiziționate. De asemenea, urmare a propunerii parvenite de la Agenția de Securitate Cibernetică de excludere a unor indicatori ale acțiunilor 1.1.1 și 1.1.2 a fost, din nou, diminuat costul estimativ al implementării proiectului. În același timp, pentru toate acțiunile au fost indicate costurile estimative, sursa de acoperire, perioada de implementare pentru fiecare acțiune/subacțiune în parte, cu specificarea codului programului/ subprogramului bugetar, divizate pe ani.

			bugetare și autorități/instituții responsabile în contextul confirmării acoperii cheltuielilor invocate. Prin urmare, pentru examinarea proiectului Planului de acțiuni pentru implementarea Programului Național de Securitate Cibernetică pentru anii 2026-2030, autorul urmează să prezinte, repetat, Ministerului Finanțelor proiectul care să conțină informația detaliată referitor la costurile estimative, sursa de acoperire, perioada de implementare pentru fiecare acțiune/subacțiune în parte, cu specificarea codului programului/subprogramului bugetar, divizate pe ani, care să corespundă prevederilor Legii bugetului de stat pentru anul 2026.	
9.	**Ministerul Afacerilor Externe** *(nr. DI/3/041- 12206 din 25 noiembrie 2025)*	1.	***La pct. 76 din proiectul Programului național de securitate cibernetică pentru anii 2026-2030*** Pct. 76 din proiectul PNSC stipulează că „Ministerul Afacerilor Externe al Republicii Moldova nu a dezvoltat încă o unitate de diplomație cibernetică". MAE precizează că în ultimii 2 ani a întreprins un șir de acțiuni îndreptate spre instituirea unei subdiviziuni noi în cadrul ministerului, care ar fi responsabilă de diplomația cibernetică. În acest context, în scopul punerii în aplicare a Hotărârii Guvernului nr. 284/2025 privind reglementarea modului de organizare și funcționare a autorităților administrației publice centrale de specialitate, MAE a elaborat proiectul noului Regulament de organizare și funcționare a ministerului (în continuare Regulament), inclusiv noua structură a aparatului central, care prevede instituirea Serviciului diplomație cibernetică în cadrul Direcției cooperare multilaterală. Proiectul hotărârii de Guvern pentru aprobarea Regulamentului se află la etapa de consultare publică. Respectiv, urmează a fi ajustată redacția pct. 76 din PNSC reieșind din evoluțiile curente.	**Se acceptă.** Punctul 76 a fost reformulat.

		2.	***La acțiunea 4.3.4. din proiectul Planului de acțiuni pentru implementarea Programului Național de Securitate Cibernetică pentru anii 2026-2030*** Acțiunea 4.3.4. din Planul de acțiuni pentru implementarea PNSC prevede că MAE este singura autoritate responsabilă de negocierea acordurilor bilaterale sau regionale de cooperare cibernetică cu aliații strategici. MAE consideră că, în conformitate cu dispozițiile art. 2 și art. 5 din Legea nr. 595/1999 privind tratatele internaționale ale Republicii Moldova, organul responsabil pentru încheierea tratatelor internaționale de cooperare cibernetică este Agenția pentru Securitate Cibernetică (ASC). Respectiv, MAE solicită substituirea MAE cu ASC în rubrica „Instituție responsabilă la acțiunea 4.3.4., cu menținerea MAE în aceeași rubrică în calitate de autoritate responsabilă secundară.	**Se acceptă**
10.	**Ministerul Mediului** *(Nr. 12/2-07/3134 din 21.11.2025)*		Lipsa obiecțiilor și propunerilor.	
11.	**Aparatul Președintelui Republicii Moldova** *(Nr. 2/2-06-1703 din 28.11.2025)*	1.	Remarcăm că proiectul Hotărârii Parlamentului este elaborat în conformitate cu prevederile art. 6 alin. (3) din Legea nr. 48/2023 privind securitatea cibernetică, care stabilește obligația autorităților competente de a elabora strategii naționale de securitate cibernetică, având ca scop atingerea și menținerea unui nivel sporit de securitate cibernetică. În acest context, se impune excluderea textului „lit. a)” din temeiul legal de adoptare a actului normativ (în speță, proiectul hotărârii Parlamentului), întrucât art. 6 alin. (3) ibidem nu se divizează pe litere, pentru a asigura conformitatea	**Se acceptă.**

			proiectului cu cadrul legal aplicabil și cu obiectivele strategice stabilite.	
		2.	Descrierea rolului și competențelor Centrului Național de Management al Crizelor în pct. 42 din proiectul Programul național de securitate cibernetică pentru anii 2026-2030 (în continuare - Program) este formulat în conformitate cu prevederile Legii nr. 248/2025 privind managementul situațiilor de criză, fiind totodată definit în corespondență cu Hotărârea Guvernului nr. 579/2025 privind organizarea și funcționarea Centrului Național de Management al Crizelor. Astfel, se propune completarea pct. 42 cu trimiterile de rigoare la hotărârea menționată.	**Se acceptă parțial.** Pentru a asigura o abordare uniformă pe parcursul întregului capitol, trimiterea la Legea nr. 248/2025 privind managementul situațiilor de criză a fost exclusă.
		3.	În tot cuprinsul Programului, sintagma „Strategia națională de securitate a Republicii Moldova” urmează a fi substituită cu denumirea oficială „Strategia securității naționale a Republicii Moldova”, în conformitate cu Hotărârea Parlamentului nr. 391/2023 privind aprobarea Strategiei securității naționale a Republicii Moldova.	**Se acceptă.**
		4.	La compartimentul „Domeniul de intervenție IV - Cooperare internațională” din Program, considerăm oportună substituirea sintagmei „rezervele de securitate cibernetică ale UE” cu formularea consacrată „Rezerva de Securitate Cibernetică a UE”.	**Se acceptă.**
12.	**Serviciul de Informații și Securitate** *(nr. IE/12432 din 26.11.2025)*	1.	În partea ce se referă la proiectul ***Programului național de securitate cibernetică pentru anii 2026-2030*** (în continuare - Program), Serviciul propune completarea la **Capitolul VII - Autorități și instituții responsabile** cu punctul 94.15 în care să fie indicată Instituția publică „Centrul de Tehnologii Informaționale în Finanțe", în calitate de dezvoltator și administrator al sistemelor informaționale pentru autorități publice în domeniile: finanțe publice, achiziții publice, fiscal și vamal, conform Hotărîrii Guvernului nr. 125/2018 cu privire la Instituția	**Se acceptă**

			publică „Centrul de Tehnologii Informaționale în Finanțe".	
		2.	Totodată, în partea ce vizează ***Planul de acțiuni pentru implementarea Programului Național de Securitate Cibernetică pentru anii 2026-2030*** (în continuare - Plan), relevăm următoarele aspecte: 2.1 propunem includerea în Plan a unei secțiuni separate intitulate *„Instituție coresponsabilă"*, întru delimitarea clară a acțiunii specifice fiecărei autorități/instituții cu competențe în realizarea politicii statului în domeniul securității cibernetice și combaterea criminalității cibernetice.	**Nu se acceptă.** Planul este structurat conform HG 386/2020, precum și a modelului prezentat de Cancelaria de Stat. Totodată, instituțiile coresponsabile sunt enumerate ulterior celor prim-responsabile.
		3.	La obiectivul specific **1.2. Consolidarea rezilienței furnizorilor de servicii în sectoarele critice împotriva amenințărilor cibernetice și a incidentelor cibernetice** din Plan, constatăm că acțiunile indicate la punctele 1.2.5 - 1.2.8 și 1.2.13 nu au nimic în comun cu obiectivul specific trasat, ce se referă la consolidarea rezilienței furnizorilor. În acest sens, considerăm imperativ de a introduce următoarele acțiuni, care vin să asigure reziliența furnizorilor și conformarea acestora cu cerințele cadrului normativ privind securitatea cibernetică și anume: *„Instituirea cadrului normativ de certificare/autorizare a entităților ce vor efectua auditul de securitate cibernetică a furnizorilor de servicii"*, iar în calitate de indicator de monitorizare să fie indicat *„Cel puțin 5 entități specializate în audit de securitate cibernetică autorizate"*; *„Efectuarea auditului de securitate cibernetică a furnizorilor de servicii"*, iar în calitate de indicator de monitorizare să fie indicat *„100% furnizori de servicii auditați"* (către anul 2027).	**Se acceptă parțial.** Acțiunea 1.2.1 fost completată cu un indicator nou, după cum urmează: *„Cadrul de reglementare privind acreditarea entităților ce vor avea dreptul de a efectua evaluarea conformității cu cerințele privind măsurile de securitate a rețelelor şi sistemelor informatice ale furnizorilor de servicii în sectoarele critice"* Cu referire la acțiunea privind efectuarea auditului de securitate cibernetică, aceasta ține de realizarea HG 562/2025 cu privire la modul de realizare a obligaţiilor de asigurare a securităţii cibernetice de către furnizorii de servicii în sectoarele critice.

		4.	La acțiunea menționată la punctul 1.2.4 *„Consolidarea capacității instituționale a autorităților și instituțiilor publice pentru alinierea acestora la cerințele de securitate stabilite de cadrul normativ în domeniul securității cibernetice”* din Plan, considerăm că indicatorul de monitorizare stabilit este irelevant pentru autoritățile publice. În acest sens, propunem stabilirea următorului indicator de monitorizare – *„Cel putin o (1) persoană responsabilă de domeniul securității cibernetice (cu atribuții și fișă de post distincte de domeniul IT) desemnată (angajată) în toate autoritățile publice centrale.”*	**Se acceptă parțial** Acțiunea a fost completată cu indicatorul propus, în vederea desemnării unei persoane responsabile de domeniul securității cibernetice.
		5.	Subsidiar, acțiunea specificată la punctul 1.2.11 *„Implementarea unei solutii de protectie DDOS si WAF pentru furnizorii de servicii din sectoarele critice”* din Plan, precum și indicatorul de monitorizare *„Cel puțin 50 de furnizori de servicii integrați pe platforma”* nu este relevantă și presupune cheltuirea irațională a mijloacelor financiare. Astfel, soluțiile DDOS și WAF sunt destinate pentru entități ce prestează servicii online, respectiv entitățile publice găzduite pe platforma MCloud beneficiază de serviciile date, iar cele private, dacă au nevoie de astfel de soluții de securitate, trebuie să și le asigure din mijloacele financiare proprii. În acest sens, propunem revizuirea sau excluderea acțiunii enunțate supra.	**Nu se acceptă.** Acțiunea dată vizează entitățile care au necesitate de serviciul respectiv și vor apela la Agenția pentru Securitate Cibernetică în acest sens. Totodată, este necesar de menționat că nu toți furnizorii de servicii au acces la platforma MCloud. Ținem să menționăm că mecanismele existente nu se dublează.
		6.	Acțiunea indicată la punctul 1.2.13 *„Elaborarea și promovarea cadrului normativ secundar în vederea evaluării conformității mijloacelor de protecție criptografică și a semnăturilor electronice și certificarea produselor criptografice în conformitate cu normele UE”* din Plan, propunem a fi exclusă din motiv că aspectele ce vizează serviciile de încredere sunt incluse	**Nu se acceptă.** Acțiunile incluse în program, au caracter complementar și asigură corelarea și congruență cu acțiunile prevăzute în alte documente de politici și de planificare.

			în Programul Național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025-2029, aprobat prin Hotarîrea Guvemului nr. 306/2025.	
		7.	În partea ce se referă la acțiunea de la punctul 3.1.7 *„Promovarea utilizării instrumentelor securizate de identificare digitală și introducerea unor principii unificate ale UE pentru gestionarea serviciilor de încredere, a identificării electronice și a criptografiei”,* propunem a fi exclusă din motiv că la secțiunea - indicator de monitorizare este menționat *„cel puțin 3 campanii de conștientizare a publicului organizate anual”*, însă organizarea campaniilor de conștientizare nu țin de competența Serviciului.	**Se acceptă.** Acț. 3.1.7 a fost modificată, după cum urmează: „Promovarea utilizării instrumentelor securizate de identificare digitală”. Respectiv, instituția responsabilă a fost modificată.
13.	**Serviciul Tehnologia Informației și Securitate Cibernetică** *(nr. 1.4/1829/25 din 24.11.2025)*		Lipsa obiecțiilor și propunerilor.	
14.	**Agenția de Guvernare Electronică** *(nr. 3007-230 din 25.11.2025)*		La **Obiectivul specific 3.1, Acțiunile 3.1.1 și 3.1.7**, solicităm excluderea AGE din coloana aferentă instituțiilor responsabilă pentru realizarea acțiunilor respective. La acest subiect, menționăm că mandatul AGE, așa cum este definit în **Statutul Instituției publice „Agenția de Guvernare Electronică”, aprobat prin Hotărârea Guvernului nr. 760/2010**, este orientat prioritar spre transformarea digitală, dezvoltarea serviciilor publice electronice, interoperabilitate și consolidarea infrastructurii de guvernare digitală. Astfel, activitățile de instruire și de formare, precum și campaniile de comunicare pe care AGE le organizează sistematic, sunt axate, în mod esențial, pe promovarea și creșterea adopției serviciilor digitale, sporirea încrederii	**Se acceptă**

			în serviciile publice guvernamentale electronice și conștientizarea beneficiilor utilizării acestora. În cadrul acestor activități sunt atinse subiecte conexe, **precum comportamentul digital responsabil sau principii de bază a securității în utilizarea serviciilor electronice**. Aceste aspecte sunt tratate în contextualizarea utilizării serviciilor digitale, dar nu ca obiectiv principal. Astfel, implicarea plenară a instituției în realizarea Acțiunilor 3.1.1 și 3.1.7 este dificilă în lipsa planificării unor surse financiare și de personal, în condițiile în care AGE deja organizează sistematic activități de instruire și de formare, precum și campanii de comunicare privind utilizarea soluțiilor electronice guvernamentale și a serviciilor publice electronice. De asemenea, atragem atenția că responsabilitățile prevăzute la Acțiunile 3.1.1 și 3.1.7 depășesc domeniile de competență ale instituției. Astfel, AGE nu dispune de competențe de elaborare și asigurare a promovării celor mai bune practici și îndrumări în gestionarea riscurilor, inclusiv pentru îndeplinirea cerințelor specifice de securitate privind rețelele și sistemele informatice, în domeniul gestionării cheilor publice și a altor servicii conexe semnăturii electronice sau în domeniul securității informației, protejării criptografice și tehnice a informațiilor. În acest sens, recomandăm autorului identificarea corespunzătoare a persoanelor juridice de drept public cu competențe în domeniile menționate și includerea acestora în calitate de instituții responsabile pentru realizarea Acțiunilor 3.1.1 și 3.1.7. Totodată, AGE rămâne deschisă să contribuie la promovarea identificării digitale securizate sau a educației în domeniul securității cibernetice, în limitele rolului său, prin:	

			- integrarea unor elemente generale de conștientizare privind utilizarea sigură a serviciilor digitale în programele sale de transformare digitală; - includerea unor obiective educaționale în campaniile sale de comunicare, atunci când acestea țin de încrederea în utilizarea serviciilor publice digitale.	
15.	**Procuratura Generală** *(nr. 4-1d/25-361 din 26.11.2025)*	1.	Apreciind conţinutul proiectului prin prisma principiilor activităţii de legiferare prevăzute de art.3 din Legea nr. 100/2017 cu privire la actele normative, în limita domeniului de competenţă al Procuraturii Generale, prezentăm următoarele constatări şi propuneri: În „Conceptul Programului Naţional de Securitate Cibernetică” sunt identificate patru domenii principale de intervenţie: - consolidarea capacităţilor operaţionale; - lupta împotriva criminalităţii informatice; - rezidenţa cibernetică a societăţii; - cooperarea internaţională şi naţională. Conceptul presupune implicarea activă a mai multor actori, precum Ministerul Dezvoltării Economice şi Digitalizării, MAI, Agenţia de Securitate Cibernetică etc. Totuşi, Procuratura apare insuficient de explicit în lista părţilor implicate, atribuţiile sale fiind practic omise. Pct. 38 din proiect, referindu-se la rolul Procuraturii, menţionează doar existenţa unei secţii specializate, însă atribuţiile acesteia sunt formulate greşit. Deşi PNSC recunoaşte rolul „autorităţilor de aplicare a legii” în investigarea crimelor cibernetice (obiectiv specific 2.1), documentul atribuie în mod explicit o serie de acţiuni (dotare tehnologică, instrumente, formare) Ministerului Afacerilor Interne şi nu menţionează Procuratura în acţiunile concrete din planul de implementare.	**Se acceptă.** Pct. 38 a fost modificat conform textului propus.

			Această omisiune diminuează rolul Procuraturii şi reduce lupta împotriva criminalităţii informatice la un nivel preponderent tehnic sau preventiv, fără un mecanism clar de anchetă şi sancţionare penală. În consecinţă, persistă riscul unui „gol instituţional” pe segmentul penal al securităţii cibernetice. Dacă doar MAI este vizat în dotare şi formare pentru investigarea infracţiunilor cibernetice, există riscul ca Procuratura să nu îşi poată exercita pe deplin funcţiile sale (anchetă, urmărire penală, cooperare internaţională, susţinerea acuzării de stat). Programul urmează a fi revăzut astfel încât Procuratura să fie inclusă explicit în anumite acţiuni (anchete, schimb de date, formare), nu doar generic. Este necesară instituirea unor mecanisme clare de raportare şi coordonare (protocoale) între Procuratură, MAI şi autorităţile de securitate cibernetică, pentru a creşte eficienţa investigării şi judecării infracţiunilor informatice. În consecinţă, se propune reformularea punctului menţionat, ţinând cont de funcţiile şi atribuţiile legale ale Procuraturii şi ale Secţiei combatere crime cibernetice din cadrul acesteia. La redactarea pct. 38 urmează a fi avute în vedere următoarele prevederi: Articolul 5 lit. g) din Legea cu privire la Procuratură nr. 3 din 25.02.2016, potrivit căruia Procuratura „participă la implementarea unitară a politicii naţionale şi internaţionale a statului în materie penală”. Articolul 4 alin. (4) din Legea nr. 20 din 03.02.2009 privind prevenirea şi combaterea criminalităţii informatice, potrivit căruia Procuratura Generală: a) coordonează, conduce şi exercită urmărirea penală;	

			b) dispune conservarea imediată a datelor informatice sau a datelor privind traficul informatic atunci când există pericolul distrugerii ori alterării acestora; c) reprezintă învinuirea, în numele statului, în instanţele judecătoreşti. Regulamentul Procuraturii, aprobat prin Ordinul Procurorului General nr. 33/3 din 03.05.2022, Capitolul IV, Secţiunea 16, pct. 78, care stabileşte atribuţiile Secţiei combatere crime cibernetice, inclusiv: a) contribuirea la implementarea unitară a politicii naţionale şi internaţionale în investigarea criminalităţii informatice; b) generalizarea şi unificarea practicii privind examinarea sesizărilor şi conducerea urmăririi penale în cauzele de criminalitate informatică; c) acordarea de sprijin practic şi metodologic; d) colectarea şi analiza informaţiilor privind investigarea criminalităţii infonuatice; e) coordonarea şi controlul activităţii procurorilor în domeniu; f) efectuarea de studii privind cauzele şi condiţiile care favorizează criminalitatea informatică; g) formularea de propuneri pentiu perfecţionarea legislaţiei şi participarea la elaborarea actelor normative. Rezumând cele expuse, propunem următoarea redacţie pentru pct. 38: „38. Procuratura Generală, în cadrul căreia este instituită şi funcţionează Secţia combatere crime cibernetice, contribuie la implementarea politicii naţionale şi internaţionale a statului în domeniul investigării criminalităţii informatice, coordonează, conduce şi exercită urmărirea penală, reprezintă învinuirea în instanţele de judecată şi asigură cooperarea juridică	

			internaţională în conformitate cu standardele stabilite de Convenţia Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, precum şi de alte acte internaţionale la care Republica Moldova este parte.”	
		2.	Privitor la indicatorii de monitorizare ai acţiunii 2.1.2 Acţiunea 2.1.2 prevede: „Investiţii continue în competenţe şi abilităţi digitale ale autorităţilor de aplicare a legii, inclusiv în capacităţile şi competenţele criminalistice digitale şi în noi metode de investigare a criminalităţii informatice şi a infracţiunilor conexe.” Din analiza documentelor reiese că indicatorul de monitorizare aferent acestei acţiuni este formulat într-un mod ambiguu, întrucât lasă impresia că se referă exclusiv la competenţele criminalistice digitale, fără a reflecta întreaga sferă a competenţelor necesare autorităţilor. Având în vedere că Procuratura Generală este desemnată drept instituţie responsabilă pentru această acţiune, se consideră necesară ajustarea indicatorului în scopul reflectării corecte a obiectivelor acţiunii. Propunere de reformulare: „Cel puţin 20 de profesionişti instruiţi în securitate cibernetică, inclusiv cei certificaţi în domeniul criminalisticii digitale.” Scopul reformulării acţiunii enunţate rezidă în: 1) acoperirea tuturor tipurilor de competenţe relevante (digitale, criminalistice, investigative); 2) claritate în privinţa rezultatelor aşteptate; 3) posibilitatea de monitorizare concretă şi verificabilă.	**Se acceptă parțial** Indicatorul a fost reformulat, având următorul text: „Cel puțin 20 de profesioniști instruiți în securitate cibernetică și/sau certificați în domeniul criminalisticii digitale”.
16.	**Consiliul Audiovizualului** *(nr. 122/02 din 24.11.2025)*	1.	În Planul de acțiuni pentru implementarea Programului național de securitate cibernetică pentru anii 2026-2030, Obiectivul specific 3.3. Consolidarea cooperării interne	**Se acceptă.**

			între autoritățile și instituțiile publice, precum și mass-media pentru a lupta eficient împotriva manipulărilor electorale și a atacurilor cibernetice, rubrica „Acțiuni unice identificabile nr. 3.3.1” prevede *„Elaborarea și organizarea de cursuri tematice de instruire pentru radiodifuzori, distribuitori de servicii media, formatori de opinie publică, jurnaliști și organizații neguvernamentale privind tehnicile de dezinformare și/sau manipulare a informațiilor utilizate pentru a afecta securitatea informațională a statului", instituții responsabile fiind indicate „Centrul pentru Comunicare Strategică și Combatere a Dezinformării; Serviciul de Informații și Securitate; Consiliul Audiovizualului”*. Atragem atenția asupra faptului că Codul serviciilor media audiovizuale al Republicii Moldova nr.174/2018 nu reglementează noțiunea de „radiodifuzor". Astfel, pentru uniformizarea terminologiei utilizate, propunem substituirea sintagmei de *„radiodifuzori”* cu sintagma *„furnizor de servicii media”* în tot textul actului supus avizării și în forma gramaticală corespunzătoare.	
		2.	Totodată, în ceea ce ține de acțiunea privind elaborarea și organizarea de cursuri tematice, este de menționat că, potrivit competențelor sale, Consiliul Audiovizualului nu organizează și nu desfășoară instruiri, așa cum prevede Planul de acțiuni, respectiv, se propune excluderea Consiliului Audiovizualului de la compartimentul „Instituție responsabilă" pentru acțiunea nr. 3.3.1.	**Se acceptă.**
17.	**Biroul Național de Statistică** *(nr. 24-01/18 din 25.11.2025)*		Lipsa de obiecții și propuneri.	
18.	**Centrul Național pentru Protecția Datelor cu Caracter Personal**		Lipsa de obiecții și propuneri.	

	(nr. 04-01/4100 din 26.11.2025)			
19.	**Comisia Electorală Centrală** *(nr. CEC-8/9668 din 26.11.2025)*		Lipsa de obiecții și propuneri.	
20.	**Institutul de Standardizare din Moldova** *(nr. 04-03/545 din 28.11.2025)*	1.	ISM este nominalizat drept responsabil pentru realizarea acțiunii 1.2.1 prevăzută în Plan, în ceea ce privește aprobarea și actualizarea standardelor naționale în domeniul securității informației și securității cibernetice. Atribuții privind aprobarea și actualizarea standardelor reies inclusiv din art. 6 din Legea nr. 20 privind standardizarea națională, astfel, se constată că suma de bani alocată acestei acțiuni nu este fundamentată în mod explicit, nefiind prezentate criteriile care au stat la baza calculării costurilor, în lipsa acestor justificări, instituția nu poate evalua adecvat fezabilitatea financiară a sarcinilor ce îi revin și nici corela proporțional resursele interne necesare. Solicităm respectuos, prezentarea informației privind destinația bugetului alocat (procurarea standardelor de către furnizorii de servicii în sectoarele critice, adoptarea/actualizarea standardelor etc.) sau redefinirea și prezentarea mai explicită a indicatorului de monitorizare.	**Precizare** Estimarea costurilor pentru acțiunea 1.2.1 a fost realizată, pentru 1 standard, în conformitate cu *Manualul privind estimarea costurilor documentelor de politici publice din Republica Moldova*, instrument metodologic recomandat de Cancelaria de Stat și Ministerul Finanțelor pentru toate documentele de politici. În același timp, având în vedere expertiza specifică a Institutului de Standardizare din Moldova în calcularea costurilor aferente proceselor de standardizare, rămânem deschiși ca ISM să prezinte o estimare ajustată a resurselor necesare. Aceasta va putea fi reflectată în versiunea finală a Programului și integrată în procesul ulterior de planificare bugetară.
		2.	De asemenea, acțiunea 1.2.2 în domeniul instruirii furnizorilor de servicii din sectoarele critice privind aplicarea standardelor naționale în securitatea informațiilor și securitatea cibernetică nu vizează explicit ca responsabil sau co-responsabil Institutul de	**Se acceptă**

			Standardizare din Moldova, cu toate că, ISM dispune și dezvoltă capacitățile tehnice și instituționale necesare pentru prestarea unor astfel de activități de instruire, în special, expertiză în aplicarea și implementarea standardului SM EN ISO/IEC 27001:2023 „Tehnologia informației, securitatea cibernetică și protecția vieții private. Sisteme de management al securității informației. Cerințe" În acest context, propunem includerea ISM în calitate de partener/co-responsabil pentru acțiunile care vizează, instruirea furnizorilor de servicii din sectoarele critice și dezvoltarea competențelor de utilizare a standardelor naționale privind securitatea informațiilor și securitatea cibernetică. ISM își exprimă disponibilitatea de a contribui la implementarea acțiunilor prevăzute în acest Plan, cu condiția clarificării bugetelor alocate și a rolului instituțional aferent. Considerăm că includerea explicită a instituției noastre în acțiunile de instruire în domeniul securității informaționale și cibernetice ar spori eficiența implementării Planului și ar asigura alinierea la bunele practici europene și internaționale.	
21.	**Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „CYBERCOR")** *(nr. 01-3260 din 02.12.2025)*	1.	În urma analizei de fond, UTM/CYBERCOR emit un AVIZ POZITIV, formulînd totodată propuneri tehnice orientate spre consolidarea capacităților instituționale și naționale în domeniul securității cibernetice. Programul este aliniat cadrului legal național și european, inclusiv obiectivelor de integrare europeană, prevederilor Legii nr. 48/2023 privind securitatea cibernetică și angajamentelor asumate de Republica Moldova în domeniul rezilienței digitale. Observații generale	**Precizare.** Propunerile înaintate de Instituția Publică Universitatea Tehnică a Moldovei / Institutul Național de Inovații în Securitatea Cibernetică „CYBERCOR" reprezintă intervenții cu caracter operațional și tehnic detaliat, care depășesc nivelul de granularitate al unui program național, al cărui rol este să

			1.1. Documentul configurează în mod corect arhitectura națională de securitate cibernetică și include măsuri de prevenire, protecție, detecție și răspuns, în conformitate cu practicile europene. 1.2. Se evidențiază abordarea interinstituțională și integrarea responsabilităților relevante pentru autorități, entități publice, infrastructuri critice și sectorul educațional. 1.3. Sunt bine conturate direcțiile privind maturitatea cibernetică, managementul riscurilor și consolidarea mecanismelor CSIRT, inclusiv cooperarea cu mediul privat. 1.4. Rolul instituțiilor de cercetare și educație este prezent, însă pentru eficiență practică recomandăm extinderea și operaționalizarea acestuia în acțiuni specifice din Program.	stabilească direcțiile strategice și obiectivele de nivel macro pentru consolidarea securității cibernetice. Programul deja integrează contribuția mediului academic și a instituțiilor de cercetare printr-o serie de acțiuni relevante (ex. 1.2.2, 1.2.3, 3.1.1, 3.1.4 ș.a.), care prevăd cooperarea cu instituțiile responsabile de formare, cercetare și inovare. În acest cadru, rolul UTM/CYBERCOR este recunoscut și rămâne unul esențial, însă modalitățile concrete de implicare urmează a fi stabilite la etapa de implementare, în strânsă coordonare cu auttorițile și instituțiile responsabile pentru fiecare acțiune.
		2.	Formarea profesională și dezvoltarea resursei umane. Se recomandă includerea explicită a UTM/CYBERCOR în lista instituțiilor responsabile pentru: ✓ formarea profesională continuă în securitate cibernetică, ✓ microcalificări și programe avansate pentru specialiști, ✓ instruirea personalului IT&C din sectorul public și infrastructurile critice, ✓ programe de certificare în conformitate cu standardele internaționale. Această includere operaționalizează capacitățile deja existente la nivel național.	
		3.	Instituirea unui Program național de formare continuă. Propunem introducerea unei acțiuni distincte privind dezvoltarea unui cadru național unificat de formare, cu:	

			✓ module obligatorii pe niveluri (de bază, intermediar, avansat), ✓ conținut adaptat structurii pe sectoare și infrastructuri critice, ✓ mecanisme de certificare și reînnoire periodică a competențelor.	
		4.	Consolidarea parteneriatului cu mediul academic. Recomandăm instituirea unui mecanism formal prin care UTM/CYBERCOR și instituțiile de cercetare să contribuie la: ✓ elaborarea ghidurilor tehnice, ✓ dezvoltarea laboratoarelor și platformelor naționale, ✓ evaluarea maturității cibernetice, ✓ cercetare aplicată și dezvoltarea tehnologiilor de securitate.	
		5.	Crearea unui hub național de exerciții (cyber range). Propunem includerea acțiunii de constituire a unui centru național de exerciții cibernetice coordonat de CYBERCOR, utilizat pentru: ✓ Simulări tehnice și tactice, ✓ exerciții CSIRT interinstituționale, ✓ testare a rezilienței infrastructurilor critice, ✓ scenarii complexe de atac și reacție.	
		6.	Introducerea indicatorilor de performanță (KPI). Recomandăm includerea unor indicatori măsurabili privind: ✓ numărul specialiștilor instruiți, ✓ gradul de acoperire sectorială, ✓ scoruri de maturitate cibernetică, ✓ reducerea timpilor de reacție la incidente, ✓ procentul de instituții care implementează politici de securitate actualizate.	

		7.	Universitatea Tehnică a Moldovei și Institutul Național de Inovații în securitatea Cibernetică „CYBERCOR" susțin adoptarea proiectului Hotărîrii Parlamentului și consideră că Programul național de securitate cibernetică 2026-2030 este un instrument strategic crucial pentru consolidarea rezilienței digitale naționale. Avizul este emis în limitele competențelor instituției și nu conține obiecții de ordin juridic asupra proiectului.	
22.	**Agenția pentru Securitate Cibernetică** *(Nr. 09-689 din 05.12.2025)*	1.	La obiectivul specific 1.1 *Consolidarea capacităților de răspuns la incidente cibernetice al Agenției pentru Securitate Cibernetică*, considerăm relevant ca la subpct: 1.1.1 indicatorul de monitorizare „Protocoalele standardizate de raportare sunt testate prin cel puțin un exercițiu anual" să fie exclus, reieșind din faptul că Sistemul informațional urmează să fie documentat printr-un Concept informațional și un Regulament care urmează să stabilească modul de organizare și funcționare a acestuia. Nu este oportun stabilirea de protocoale la asemenea acțiune.	**Se acceptă**
		2.	1.1.2 La subpct. dat propunem reformularea acestuia în următoarea redacție „Crearea unui mecanism centralizat pentru schimbul de informații cu furnizorii de servicii în sectoarele critice", iar indicatorul de monitorizare „Protocoale standardizate pentru schimbul de informații pentru autoritățile publice și pentru furnizorii de servicii din sectoarele critice sunt adoptate." și Protocoale standardizate pentru schimbul de informații pentru autoritățile publice și pentru furnizorii de servicii din sectoarele critice testate prin cel puțin un exercițiu anual", urmează a fi excluse de sub acțiunea dată, fiindcă asemenea indicatori de monitorizare nu pot fi realizați la acțiunea menționată.	**Se acceptă**

		3.	1.1.3 La subpct. dat se propune următoarea redacție a acțiunii „Instruirea furnizorilor de servicii în sectoarele critice privind mecanismele și instrumentele de raportare a incidentelor și a schimbului de informații”. Redacția dată este necesară pentru oferirea unei clarități a acțiunii identificabile în raport cu indicatorul de monitorizare a acesteia.	**Se acceptă**
		4.	1.1.4 La subpct. dat se propune ajustarea indicatorului de monitorizare în următoarea redacție „Cel puțin un exercițiu de răspuns la incidente cibernetice la nivel național și cel puțin un exercițiu la nivel sectorial /intersectorial organizate anual”. Se propune cate cel puțin un exercițiu si sectorial, reieșind din faptul că si la exercițiile naționale sunt invitați reprezentanți din diferite sectoare, respectiv ei sunt implicați atât la exercițiile naționale, și urmează a fi implicați și sectorial, respectiv se propune ajustarea dată.	**Se acceptă**
		5.	1.1.5 acțiunea dată se propune să-i fie oferită următoarea redacție: „Publicarea evaluărilor periodice și rapoartelor privind situația din spațiul cibernetic național”. Propunerea dată derivă din faptul că o focusare pe anumite categorii nu ar prezenta o situație în ansamblu a spațiului național cibernetic, inclusiv ar crea confuzie în competențele avute de către Agenție.	**Se acceptă**
		6.	La obiectivul specific 1.2: *Consolidarea rezilienței furnizorilor de servicii în sectoarele critice împotriva amenințărilor cibernetice și a incidentelor cibernetice,* considerăm relevant la subpct: 1.2.2 urmează a avea următoarea redacție „Instruirea furnizorilor de servicii din sectoarele critice să utilizeze standardele naționale în domeniul securității informațiilor și a securității cibernetice în cadrul organizațiilor lor pentru a asigura conformitatea cu Legea	**Se acceptă** Acțiunea a fost modificată după cum a fost propus, indicatorul a fost expus după cum urmează: „Necesitățile sectoriale de formare și dezvoltare profesională în domeniul securității cibernetice identificate în baza solicitărilor parvenite de la

			nr. 48/2023 privind securitatea cibernetică”., iar ca indicator de monitorizare se propune „Identificarea necesităților sectoriale de formare și dezvoltare profesională în domeniul securității cibernetice în baza solicitărilor parvenite de la furnizorii de servicii în sectoarele critice, Anul 2026 - 25% de funcționari instruiți, Anul 2027 - 40% de funcționari instruiți”	furnizorii de servicii în sectoarele critice”
		7.	1.2.3 indicatorul de monitorizare se propune în următoarea redacție „identificarea necesităților sectoriale de formare/dezvoltare profesională în domeniul securității cibernetice sunt sistematizate în baza solicitărilor”. Efectuarea de studiu, ar presupune cheltuieli bugetare, iar rezultatul dorit nu poate fi atins prin asemenea studiu.	**Se acceptă.** Indicatorul a fost formulat după cum urmează: „Necesitățile sectoriale de formare/dezvoltare profesională în domeniul securității cibernetice sunt identificate și sistematizate în baza solicitărilor ”
		8.	1.2.4 se propune o nouă redacție acțiunii identificate „Consolidarea capacității instituționale a Agenției pentru Securitate Cibernetică pentru asigurarea implementării cerințelor de securitate stabilite de cadrul normativ în domeniul securității cibernetice.”, iar la indicator de monitorizare, sa fie indicat 75%. Propunerea dată derivă din conexiunea între indicator și acțiune, redacția actuală nu este uniformă, indicatorul de monitorizare nu corespunde cu acțiunea menționată.	**Se acceptă parțial.** Pentru a corespunde indicatorul și acțiunea dată, a fost completat cu un indicator nou în acest sens, conform propunerii parvenite de la SIS („Cel puțin o (1) persoană responsabilă de domeniul securității cibernetice desemnată în toate autoritățile publice centrale.”)
		9.	1.2.9 se propune următoarea redacție a acțiunii „Crearea unei platforme centralizate de raportare și gestionare a vulnerabilităților cibernetice.”. Redacția dată oferă o claritate indicatorului respectiv.	**Se acceptă**
		10.	La obiectivul specific 3.2. *Dezvoltarea unui mecanism național de monitorizare continuă și evaluare a dezvoltării societății digitale,* considerăm relevant la subpct: 3.2.1 propunem excluderea cuvintelor „de către persoanele fizice și intreprinderi”, deoarece creează	**Se acceptă**

			confuzie și îngrădește cercul de efectuare a sondajelor respective.	
		11.	Obiectivul specific 3.4. *Protejarea drepturilor și libertăților persoanelor atunci când datele lor cu caracter personal sunt prelucrate*, considerăm relevant la subpct: 3.4.1 indicatorul de monitorizare să-i fie oferită următoarea redacție: „Semnarea unui Memorandum de colaborare între autorități”. Necesitatea de redactare derivă din conținutul neclar al redacției propuse.	**Se acceptă**
		12.	3.4.2 la indicatorul de monitorizare propunem sa fie cate cel puțin o campanie comună de promovare a conștientizării cibernetice cibernetice, a confidențialității și a protecției datelor desfășurate organizate anual.	**Se acceptă.**
		13.	La obiectivul specific 4.2 *Dezvoltarea platformelor de comunicare strategică externă pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova,* considerăm relevant la subpct: 4.2.1 la indicatorul de monitorizare „Planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice aprobat”, să fie indicat ca termen de realizare T4 anul 2026. Necesitatea de intervenție derivă din termenul stabilit în proiectul de hotărâre privind adoptarea planului respectiv.	**Se acceptă.**
23.	**Centrul pentru Comunicare Strategică și Contracarare a Dezinformării** *(Nr. 300/25 din 04.12.2025)*	1.	Potrivit prevederilor art.2 a Legii privind Centrul pentru Comunicare Strategică și Contracarare a Dezinformării și privind modificarea unor acte normative, nr. 242/2023 prenotate, **Centrul pentru Comunicare Strategică și Contracarare a Dezinformării** (în continuare – **Centru**) este o autoritate administrativă care funcționează la nivel național ca o structură unică.	**Se acceptă.**

			Misiunea Centrului este de a consolida și îmbunătăți eforturile interinstituționale în lupta împotriva dezinformării, manipulării informațiilor și ingerințelor străine, care prezintă pericol sau pot periclita realizarea intereselor naționale sau a obiectivelor naționale de securitate. Totodată, în conformitate cu art.9 a Legii nr.242/2023, în vederea realizării atribuțiilor sale, Centrul are dreptul să înainteze autorităților publice propuneri privind elaborarea și modificarea cadrului normativ și să emită recomandări în conformitate cu atribuțiile conferite. 1. Astfel, prin Legea pentru modificarea unor acte normative *(aspecte referitoare la activitatea Centrului pentru Comunicare Strategică și Contracarare a Dezinformării)*, nr. 247/2025 *(publicată în Monitorul Oficial nr.426-429 din 12.08.25 art.584; în vigoare 12.08.25)* au fost operate modificări la Legea nr. 242/2023. Astfel, în cuprinsul Legii, sintagma „Centrul pentru Comunicare Strategică și *Combatere* a Dezinformării”, la orice formă gramaticală, s-a substituit cu sintagma „Centrul pentru Comunicare Strategică și *Contracarare* a Dezinformării”. În context, la proiectul Programului național de securitate cibernetică pentru anii 2026-2030, se consideră întemeiat substituirea în tot proiectul, a denumirii de *„Centrul pentru Comunicare Strategică și Combatere a Dezinformării”*, la orice formă gramaticală, cu sintagma *„Centrul pentru Comunicare Strategică și Contracarare a Dezinformării”*.	
		2.	Totodată, la proiectul Planului de acțiuni pentru implementarea Programului Național de Securitate Cibernetică pentru anii 2026-2030, Obiectivul specific	**Se acceptă.**

			1.3. „Îmbunătățirea răspunsului la crizele cibernetice prin asigurarea unei abordări coordonate și valorificarea structurilor existente pentru menținerea funcțiilor societale vitale”, **Acțiunea 1.3.2 „Îmbunătățirea capacităților de comunicare strategică în situații de criză prin exerciții”, Centrul urmează de a fi exclus** ca instituție responsabilă, reieșind din mandatul atribuit prin Lege și înlocuit cu Centrul Național de Management al Crizelor, din considerentele ce urmează. 2.1. În conformitate cu prevederile art.8 a Legii nr.242/2023, la îndeplinirea funcțiilor stabilite, Centrul exercită următoarele atribuții: - *oferă instruire, elaborează materiale metodologice, inclusiv pentru scenarii de criză, şi dezvoltă alte măsuri pentru a consolida capacitățile statului de comunicare strategică şi de contracarare a acțiunilor de manipulare a informațiilor şi ingerințelor străine;* - *la necesitate, acordă sprijin în procesul de comunicare strategică în situaţii de criză.* 2.2. Prin scrisorile înregistrate cu nr.136 din 06.06.2025 și nr. 249 din 02.10.2024, Centrul, în conformitate cu art.7 şi art.8 din Legea cadru nr. 242/2023, a elaborat și înaintat (către Cancelaria de Stat, Consiliului Suprem de Securitate, Unității responsabile pentru instituirea Centrului Unic de Gestionare a Crizei), *spre informare, studiere şi aplicare, modele şi instrumente de lucru destinate autorităților publice, instituțiilor, agențiilor şi organizațiilor guvernamentale necesare în gestionarea intersectorială a comunicării strategice şi de criză.* Astfel, documentele (toate cu regim strict confidențial), după cum urmează:	Instituție prim-responsabilă a fost inclusă - Centrul Național de Management al Crizelor.

			I. ***Procedură operațională standard pentru comunicare strategică în situații de criză care pot afecta securitatea Republicii Moldova, la nivel interinstituțional;*** II. ***Model pentru Registrul riscurilor şi evaluarea lor în procesele care ar putea afecta securitatea națională a Republicii Moldova;*** III. ***Model pentru Protocoale de comunicare strategică şi echipele de comunicare pentru diminuarea efectelor şi contracararea riscurilor.*** Aceste materiale reprezintă elemente de plecare în stabilirea riscurilor la nivel instituțional, interinstituțional şi național, care pot afecta securitatea națională pe cei 5 Piloni de bază, în scopul îmbunătățirii şi consolidării activităților de planificare şi gestionare a comunicării strategice, comunicării de criză şi de contracarare a dezinformării, manipulării informaționale și ingerințelor străine, integrată la nivel național pentru diminuarea efectelor nocive produse de posibile crize. De asemenea, Centrul a susținut un curs sistemic pe subiectul **managementul riscurilor şi crizelor de comunicare cu prezentarea modelului registrului riscurilor**. În acest sens, la data de 27 mai 2024 a avut loc o întâlnire de lucru la nivel înalt "Instrumente necesare pentru îmbunătățirea controlului managerial, ca obligație în procesul de aderare la UE (managementul crizei)" destinat conducătorilor structurilor Guvernului. Întrevederea a avut scopul de a informa şi prezenta modalități de diminuare a efectelor generate de crize în sistemul guvernamental. 2.3. Totodată, în conformitate cu prevederile art.39 și art.45 a Legii privind managementul situațiilor de criză, nr.248/2025, Centrul Național de Management al Crizelor (denumit în continuare și Centru) este o	

			autoritate administrativă centrală, aflată în subordinea Guvernului, *care coordonează la nivel național ansamblul activităților de management al crizelor.* Una din competențele Centrului în faza de prevenire și de pregătire pentru crize sunt următoarele, este de a organiza, independent sau în cooperare cu alte autorități și instituții publice, module de pregătire standardizate în domeniul managementului crizelor, ***asigurând instruirea continuă*** a persoanelor implicate în prevenirea, managementul și răspunsul la situații de crize. În contextul celor expuse, se menționează că Centrul pentru Comunicare Strategică și Contracarare a Dezinformării a elaborat pe parcursul anului 2024 *modele şi instrumente de lucru destinate autorităţilor publice în gestionarea intersectorială a comunicării strategice şi de criză, inclusiv desfăşurarea de instruiri*, iar odată cu înființarea Centrului Național de Management al Crizelor, acesta este responsabil de realizarea acțiunii 1.3.2 „Îmbunătățirea capacităților de comunicare strategică în situații de criză prin exerciții", potrivit mandatului atribuit prin lege.	
		3.	La Acțiunea 3.3.1. *„Elaborarea şi organizarea de cursuri tematice de instruire pentru radiodifuzori, distribuitori de servicii media, formatori de opinie publică, jurnalişti şi organizaţii neguvernamentale privind tehnicile de dezinformare şi/sau manipulare a informaţiilor utilizate pentru a afecta securitatea informaţională a statului", sintagma „manipulare a informaţiilor"* se substituie cu sintagma *„manipulare a informaţiilor şi ingerinţelor străine"*, iar cuvintele *„securitatea informaţională a statului"*, se vor substitui	**Se acceptă.** Acțiunea a fost reformulată în următoarea redacție: „*Elaborarea şi organizarea de cursuri tematice de instruire pentru furnizori de servicii media, distribuitori de servicii media, formatori de opinie publică, jurnalişti şi organizaţii neguvernamentale privind tehnicile de dezinformare şi/sau manipulare a informaţiilor şi ingerinţelor străine*

			cu *„securitatea spațiului informațional”/„securitatea națională”*. Or, în art.4 a Legii nr. 242/2023, se regăsește noțiunea de *acțiuni de manipulare a informațiilor și ingerințe străine* – model de comportament manipulator, desfășurat în mod intenționat și coordonat, care amenință sau are potențialul de a avea un impact negativ asupra valorilor, a procedurilor și a proceselor politice, economice și sociale, promovat de actori statali sau nonstatali, inclusiv de intermediari din interiorul sau exteriorul statului, și care sunt de natură să cauzeze prejudicii securității, intereselor naționale sau obiectivelor naționale de securitate. Motiv din care, se consideră indispensabilă utilizarea noțiunii segregate.	*utilizate pentru a afecta securitatea spațiului informațional al statului”*
		4.	La Acțiunea 4.2.1. *„Elaborarea politicilor de comunicare strategică internă și conectarea 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”*, considerăm întemeiat reformularea acțiunii, și expunerea în redacția *„Integrarea în documentele de politici a <u>modelor și instrumentelor de lucru necesare în gestionarea intersectorială a comunicării strategice și de criză</u> la nivel național și cooperarea cu platformele de comunicare strategică internaționale ale structurilor sistemului de securitate, apărare și ordine publică pentru asigurarea securității spațiului informaționale și promovarea intereselor naționale sau obiectivelor naționale de securitate ale Republicii Moldova”*. Or, Centrul pentru Comunicare Strategică și Contracarare a Dezinformării a elaborat pe parcursul	**Nu se acceptă.** Reformularea propusă extinde scopul acțiunii într-o direcție care depășește mandatul Programului național de securitate cibernetică, introducând elemente ce țin de comunicarea strategică intersectorială în general și integrarea acestora în documentele de politici ale tuturor autorităților publice. Acțiunea 4.2.1 este însă aliniată obiectivului specific din Program, care vizează *dezvoltarea platformelor și mecanismelor de comunicare strategică externă pentru asigurarea securității informaționale*, având un accent clar pe **dimensiunea de**

			anului 2024 *modele şi instrumente de lucru destinate autorităților publice în gestionarea intersectorială a comunicării strategice şi de criză, inclusiv desfășurarea de instruiri,* iar autoritățile urmează de a le integra în documentele de planificare și documentele de politici publice (vezi argumentarea de la pct.2).	**securitate informațională**, parte integrantă a securității cibernetice.
		5.	Concomitent, autorul urmează a se conforma principiilor activității de legiferare, potrivit cărora actul normativ trebuie să se integreze organic în cadrul normativ în vigoare, scop în care proiectul actului normativ trebuie corelat cu prevederile actelor normative de nivel superior sau de același nivel cu care se află în conexiune. Subsidiar, învederăm că autorul proiectului urmează a se conforma prevederilor art.54 a Legii cu privire la actele normative, și a expune conținutul proiectului într-un limbaj simplu, clar și concis, pentru a se exclude orice echivoc, cu respectarea strictă a regulilor gramaticale, de ortografie și de punctuație.	**Se acceptă.**
24.	**Centrul Național de Management al Crizelor** *(nr. 20 din 05.12.2025)*	1.	O analiză a Notei de fundamentare și a Planului de acțiuni relevă un risc de suprapunere a competențelor și de interferență decizională cu CNMC, a cărui organizare și funcționare este reglementată de Hotărârea de Guvern nr. 579/2025, în baza Legii nr. 248/2025 privind managementul situațiilor de criză. Intervenția vizează asigurarea faptului că Programul nu creează o structură paralelă de criză, ci se integrează în cadrul existent, respectând definițiile legale: **Punctul problemei în proiect:** Obiectivul general (Notă de fundamentare): Vizează crearea unui *mecanism* nou de gestionare a crizelor cibernetice. **Analiza în baza Legii nr. 248/2025:** O criză/criză majoră (Art. 3 pct. 3, 4) presupune o coordonare la nivel național (competența CNMC), deoarece depășește	**Precizare** Programul nu urmărește instituirea unui mecanism distinct de gestionare a crizelor cibernetice și nu interferează cu responsabilitățile Centrului Național pentru Managementul Crizelor. Intervențiile propuse se încadrează în arhitectura instituțională deja existentă și își propune să consolideze cooperarea dintre structurile responsabile. În logica cadrului legal actual, CNMC rămâne structura cu rol strategic în gestionarea situațiilor de criză, iar Agenția pentru Securitate

			resursele instituției principale. Un *mecanism nou* contravine acestui principiu. **Propunerea de remediere (pentru a evita suprapunerile):** *Remedierea obiectivului:* Modificarea formulării din *crearea unui mecanism nou* în „Elaborarea și adoptarea procedurilor operaționale integrate, care să definească interacțiunea și atribuțiile CNMC, în calitate de coordonator strategic al crizei, cu autoritatea competentă în sensul Legii nr. 48/2023 (Agenția pentru Securitate Cibernetică) în calitate de autoritate de răspuns operațional.”	Cibernetică deține atribuțiile operaționale în domeniul securității cibernetice. În acest sens, acțiunile prevăzute în Program sunt orientate spre îmbunătățirea capacității de răspuns, a schimbului de informații și a cooperării instituționale, rămânând pe deplin aliniate cadrului legal și operațional stabilit prin Legea nr. 248/2025 și actele normative aferente.
		2.	**Punctul problemei în proiect:** Acțiunea 1.3.1 din Planul de acțiuni: Elaborarea cadrului normativ privind răspunsul coordonat la incidente și crize. **Analiza în baza Legii nr. 248/2025:** Orice *situație de criză* (art. 3 pct. 5) pornește de la *incidente*. Pentru o coordonare eficientă, trebuie definit clar pragul de escaladare. **Remedierea acțiunii 1.3.1:** Se impune ca noul cadru normativ elaborat (Acțiunea 1.3.1) să includă, ca o condiție esențială, stabilirea explicită a criteriilor de clasificare (pragul de escaladare) care transformă un *incident cibernetic major* în criză de nivel național, declanșând mandatul de coordonare al CNMC.	**Precizare.** În procesul elaborării proiectului actului normativ privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare, se va lua în considerație propunerea expusă.
		3.	**Punctul problemei în proiect:** Capitolul VII, punctul 95.2, privind monitorizarea anuală **Analiza în baza Legii nr. 248/2025:** CNMC reprezintă autoritatea națională responsabilă de coordonarea activităților de prevenire, pregătire, răspuns și recuperare la situații de criză. Având în vedere ca incidentele și crizele cibernetice sunt subsumate situațiilor de criză, este necesar ca CNMC să fie informat cu privire la stadiul	**Nu se acceptă.** Raportul anual de progres privind implementarea Programului și a planului de acțiuni se va publica pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării.

			consolidării măsurilor de securitate cibernetică la nivel național, în vederea includerii acestora în raportul anual prevăzut la art. 45, litera i) privind întocmirea evaluării naționale privind stadiul de pregătire a autorităților și instituțiilor publice pentru managementul crizelor. **Remedierea Capitolului VII, punctul 95.2, privind monitorizarea anuală:** Introducerea obligației transmiterii Raportului anual de progres privind implementarea Programului și a planului de acțiuni spre examinare și evaluare inclusiv către CNMC.	Totodată, Agenția pentru Securitate Cibernetică va realiza obligațiile care revin în baza Legii nr. 248/2025 și cadrul normativ conex.
		4.	Totodată, pentru a asigura o terminologie unitară și pentru a evita confuzia, propunem includerea următoarelor noțiuni în Program, în conformitate cu Legea nr. 248/2025: **Noțiunea propusă:** Incident cibernetic major **Definiția în contextul securității cibernetice:** Un incident cibernetic cu o amploare și intensitate care afectează continuitatea sau calitatea serviciilor esențiale și a funcțiilor societale vitale, dar care poate fi încă gestionat de resursele extinse ale autorității competente (Agenția pentru Securitate Cibernetică) (Legea nr. 48/2023) și ale instituțiilor sectoriale. **Temeiul Legal implicit (Legea nr. 248/2025):** Reprezintă stadiul incipient al unei Situații de criză (art. 3 pct. 5). **Noțiunea propusă:** Criză cibernetică de nivel național **Definiția în contextul securității cibernetice:** O criză majoră (art. 3 pct. 4), generată de un pericol artificial (atac cibernetic), ale cărei consecințe pun în pericol economia națională sau funcțiile de bază ale statului și care depășește capacitatea de gestionare a autorității	**Nu se acceptă.** Noțiunile propuse constituie subiectul unui alt proiect. Totodată, în textul programului se operează cu terminologia Legii nr. 48/2023 privind securitatea cibernetică.

			competentă în sensul Legii nr. 48/2023 (Agenția pentru Securitate Cibernetică), necesitând decizii și coordonare interinstituțională la cel mai înalt nivel (CNMC). **Temeiul Legal implicit (Legea nr. 248/2025):** Criză / Criză majoră (art. 3 pct. 3, 4). **Noțiunea propusă:** Pragul de escaladare **Definiția în contextul securității cibernetice:** Setul de criterii calitative și cantitative care, odată atinse de un incident cibernetic major, impun transformarea acestuia în criză cibernetică de nivel național și transferă coordonarea strategică către CNMC. **Temeiul Legal implicit (Legea nr. 248/2025):** Asigură distincția procedurală dintre incident și criză (art. 3 pct. 5). Avizul este favorabil, sub condiția adoptării propunerilor de remediere, în special cele privind integrarea procedurală (renunțarea la crearea unui mecanism paralel) și definirea pragului de escaladare. Aceste măsuri vor asigura că Programul Național de Securitate Cibernetică este pe deplin integrat și compatibil cu Cadrul Național de Management al Situațiilor de Criză.	

Expertizare și notificare

Nr.	Autorii obiecțiilor și propunerilor	Nr.	Obiecțiile și propunerile	Argumentarea autorului proiectului
1.	**Ministerul Justiției** *(nr. 04/1-12345 din 16.12.2025)*	1.	Sub aspectul intenției de reglementare proiectul de act normativ a fost elaborat în temeiul art. 6 alin.(3) din Legea nr. 48/2023 privind securitatea cibernetică. Potrivit art. 6 alin. (3) din Legea nr. 48/2023,	**Precizare.** Urmare a consultării cu Cancelaria de Stat a inițierii

			Strategia națională de securitate cibernetică este un document de politici care definește obiectivele strategice, măsurile de politică și cele de reglementare, având ca scop atingerea și menținerea unui nivel sporit de securitate cibernetică. **Strategia națională de securitate cibernetică se aprobă de către Parlament, la propunerea Guvernului.** Din denumirea proiectului de act normativ prezentat spre examinare rezidă aprobarea **Programului național de securitate cibernetică pentru anii 2026-2030**. În conformitate cu pct. 16 din Hotărârea Guvernului nr. 386/2020 cu privire la planificarea strategică, Programul este un document de politici publice pe termen mediu (3-5 ani), **elaborat pentru implementarea strategiilor**, care detaliază și concretizează politicile ce urmează a fi realizate în domeniile acoperite de strategii. Mai mult, potrivit art. 23 alin. (2) lit. d) din Legea nr. 48/2023, Guvernul în termen de 12 luni de la data intrării în vigoare a Legii nr. 48/2023 (01 ianuarie 2025), va elabora, va aproba și va prezenta Parlamentului spre examinare Strategia națională în domeniul securității cibernetice. În contextul celor menționate, se va revedea oportunitatea elaborării unui Program național de securitate cibernetică pentru anii 2026-2030 în lipsa Strategiei naționale în domeniul securității cibernetice. Totodată, potrivit autorului, elaborarea proiectului de hotărâre, rezidă în necesitatea realizării obiectivelor și direcțiilor prioritare stabilite în documentele de politici publice, în special în Strategia națională de securitate a Republicii Moldova, Strategia de transformare digitală 2023–2030, precum și în alte documente strategice și de planificare, cum ar fi Strategia de dezvoltare „Educație 2030” și Programul de implementare a acesteia pentru anii 2023–2025, Strategia de dezvoltare a domeniului afacerilor interne 2022–2030, Strategia națională de apărare a Republicii Moldova pentru anii 2024–2034, Programul național de prevenire și de combatere a criminalității pentru anii 2026–2030 și Programul	elaborării Strategiei Naționale pentru Securitate Cibernetică, Cancelaria de Stat a considerat că obiectivul strategic de securitate cibernetică este deja integrat în cadrul Strategiei de transformare digitală 2023–2030, care a fost aprobată prin Hotărârea Guvernului nr. 650/2023. Totodată, Strategia securității naționale a Republicii Moldova (Hotărârea Parlamentului nr. 391/2023) descrie explicit direcțiile de acțiune pentru securitatea și reziliența cibernetică. Având în vedere această situație, Cancelaria de Stat a exprimat o opinie rezervată cu privire la elaborarea unei noi Strategii în domeniul securității cibernetice. Or, adoptarea unei astfel de inițiative ar implica modificarea strategiilor existente, în sensul reducerii redundanțelor din documentele de politici publice și asigurării unui cadru strategic coerent. Prin urmare, în baza pct. 16 din Hotărârea de Guvern nr. 386/2020 cu privire la planificarea strategică, Cancelaria de Stat a recomandat elaborarea de către

			național de aderare a Republicii Moldova la Uniunea Europeană pentru anii 2025–2029. Astfel, prin implementarea acestui Program național de securitate cibernetică pentru anii 2026-2030, Guvernul urmărește consolidarea rezilienței cibernetice, reducerea criminalității informatice, creșterea educației digitale și intensificarea cooperării internaționale, precum și alinierea la standardele Uniunii Europene.	Ministerul Dezvoltării Economice și Digitalizării a unui Program care să detalieze și să concretizeze politica securității cibernetice, asigurând implementarea Obiectivului general 5, cu referință la securitatea cibernetică din Strategia de transformare digitală 2023–2030 și a direcțiilor de acțiune din Strategia securității naționale.
		2.	În continuare, la forma actuală a proiectului se înaintează unele propuneri de îmbunătățire a calității proiectului de act normativ: ***La proiectul hotărârii Parlamentului:*** În clauza de adoptare, referințele actului normativ se va completa cu sursa de publicare a acestuia.	**Se acceptă.** S-a completat cu următorul text: „(Monitorul Oficial al Republicii Moldova, 2023, nr. 151-153, art. 225)”.
		3.	La **art. 1**, pentru corectitudinea redactării, cuvintele „prevăzut în anexă” se va substitui cu textul „(se anexează)”, potrivit uzanțelor de tehnică legislativă.	**Se acceptă.**
		4.	La **art. 3**, menționăm că, în conformitate cu prevederile art.76 din *Constituție*, legea se publică în Monitorul Oficial al Republicii Moldova şi intră în vigoare la data publicării sau la data prevăzută în textul ei. Potrivit art. 56 alin. (1) din *Legea nr. 100/2017 cu privire la actele normative*, actele normative intră în vigoare peste o lună de la data publicării în Monitorul Oficial al Republicii Moldova sau la data indicată în textul actului normativ, care nu poate fi anterioară datei publicării.	**Se acceptă.** A fost expus după cum urmează: „Prezenta hotărâre intră în vigoare la data publicării.”
		5.	La proiectul Programului național de securitate cibernetică pentru anii 2026-2030: Parafa de aprobare se va expune în felul următor: „Aprobat prin Hotărârea Parlamentului nr. /2025”.	**Se acceptă.**

		6.	Cu titlu preliminar, subliniem că, în conformitate cu pct. 7 din Regulamentul cu privire la planificarea strategică, aprobat prin *Hotărârea Guvernului nr. 386/2020*, la fundamentarea, elaborarea, avizarea, consultarea și aprobarea documentelor de planificare și a documentelor de politici publice care se aprobă prin hotărâri ale Guvernului, acestora li se aplică regulile și cerințele înaintate față de actele normative, în conformitate cu Legea nr. 100/2017 cu privire la actele normative. Astfel, prevederile cuprinse la art. 24 alin. (2) din *Legea nr. 100/2017*, stabilesc că la fundamentarea, elaborarea, avizarea, consultarea şi aprobarea documentelor de politici se aplică regulile şi cerinţele înaintate faţă de actele normative. În acest context, conținutul Programului ar fi necesar de revizuit prin prisma normelor de tehnică legislativă, ținând cont de cele expuse în continuare: Notele de subsol situate în marginile inferioare ale paginilor nu reprezintă elemente de structură ale actului normativ, fapt pentru care urmează a fi excluse, iar textul acestora se va integra în puncte separate.	**Se acceptă.**
		7.	La **pct. 20**, cu referire la abrevierea „IBM” se notează că potrivit art. 54 alin. (1) lit. i) din Legea nr. 100/2017, exprimarea prin abrevieri a unor denumiri sau termeni se poate face numai după explicarea acestora în text la prima folosire (observație valabilă pentru toate cazurile identice).	**Se acceptă**
		8.	La **pct. 84**, cuvintele „tabelul de mai jos” se vor substitui cu cuvântul „Tabelul” care urmează a fi succedat de abrevierea „nr.” și numerotarea corespunzătoare. Observația este valabilă pentru toate cazurile similare din proiect. Totodată, este de menționat faptul că tabelele trebuie să aibă un temei-cadru în textul actului și să se refere exclusiv la obiectul determinat prin norma de trimitere, astfel, se va revizui acest aspect prin operarea redactărilor necesare, inclusiv la tabelul nr. 3. Subsidiar, se constată lipsa figurii 5.	**Se acceptă.**

		9.	Proiectul **Planului de acțiuni** se va completa cu parafă după următoarea formulă: „Anexa la Programul național de securitate cibernetică pentru anii 2026-2030”	**Se acceptă.**
2.	**Centrul pentru Comunicare Strategică și Contracarare a Dezinformării** *(nr. 308/25 din 15.12.2025)*	1.	Potrivit avizului nr. 300/25 din 04.12.2025 Centrul a înaintat obiecțiile și propunerile de rigoare reieșind din domeniul de competență. Reieșind din tabelul de sinteză a obiecțiilor și propunerilor/recomandărilor la proiectul hotărârii Guvernului sus menționat, majoritatea obiecțiilor și propunerilor înaintate de Centru au fost acceptate. Așadar, în context, reiterăm că la Acțiunea 4.2.1. *„Elaborarea politicilor de comunicare strategică internă și conectarea 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”*, considerăm întemeiat reformularea acțiunii, și expunerea în redacția *„Elaborarea și integrarea în documentele de politici a modelelor operaționale și a instrumentelor standardizate pentru gestionarea intersectorială a comunicării strategice și de criză la nivel național și cooperarea cu platformele de comunicare strategică internaționale ale structurilor sistemului de securitate, apărare și ordine publică pentru asigurarea securității spațiului informațional și promovarea intereselor naționale sau obiectivelor naționale de securitate ale Republicii Moldova”*. Or, Centrul pentru Comunicare Strategică și Contracarare a Dezinformării a elaborat pe parcursul anului 2024 *modele şi instrumente de lucru destinate autorităților publice în gestionarea intersectorială a comunicării strategice şi de criză, inclusiv desfășurarea de instruiri*, iar autoritățile urmează de a le integra în documentele de planificare și documentele de politici publice.	**Precizare.** În contextul elaborării și aplicării instrumentelor metodologice dezvoltate de Centrul pentru Comunicare Strategică și Contracarare a Dezinformării s-a constatat că scopul urmărit prin indicatorul aferent acțiunii 4.2.1 este deja acoperit prin cadrul operațional existent. În acest sens, pentru a evita suprapuneri și pentru a menține coerența Programului cu arhitectura instituțională și funcțională deja instituită, indicatorul privind aprobarea politicilor de comunicare strategică a fost exclus.

			În context, în conformitate cu prevederile art.8 a Legii nr.242/2023, la îndeplinirea funcțiilor stabilite, Centrul exercită următoarele atribuții: - *oferă instruire, elaborează materiale metodologice, inclusiv pentru scenarii de criză, şi dezvoltă alte măsuri pentru a consolida capacităţile statului de comunicare strategică şi de contracarare a acţiunilor de manipulare a informaţiilor şi ingerinţelor străine;* - *la necesitate, acordă sprijin în procesul de comunicare strategică în situaţii de criză.* Prin scrisoarea înregistrată cu nr.249 din 02.10.2024, Centrul, în conformitate cu art.7 şi art.8 din Legea cadru nr. 242/2023, a elaborat și înaintat (către Cancelaria de Stat, Consiliului Suprem de Securitate, Unității responsabile pentru instituirea Centrului Unic de Gestionare a Crizei), spre informare, studiere şi aplicare, modele şi instrumente de lucru destinate autorităților publice, instituțiilor, agenţiilor şi organizaţiilor guvernamentale necesare în gestionarea intersectorială a comunicării strategice şi de criză. Astfel, documentele (toate cu regim strict confidențial), după cum urmează: *I. Procedură operațională standard pentru comunicare strategică în situații de criză care pot afecta securitatea Republicii Moldova, la nivel interinstituțional;* *II. Model pentru Registrul riscurilor şi evaluarea lor în procesele care ar putea afecta securitatea națională a Republicii Moldova;* *III. Model pentru Protocoale de comunicare strategică şi echipele de comunicare pentru diminuarea efectelor şi contracararea riscurilor.* Aceste materiale reprezintă elemente de plecare în stabilirea riscurilor la nivel instituțional, interinstituțional şi național, care pot afecta securitatea națională pe cei 5 Piloni de bază, în scopul îmbunătățirii şi consolidării activităților de planificare şi gestionare a comunicării strategice, comunicării de criză şi de contracarare a dezinformării, manipulării informaționale și ingerințelor străine,	

			integrată la nivel național pentru diminuarea efectelor nocive produse de posibile crize. De asemenea, Centrul a susținut un curs sistemic pe subiectul **managementul riscurilor şi crizelor de comunicare cu prezentarea modelului registrului riscurilor**. În acest sens, la data de 27 mai 2024 a avut loc o întâlnire de lucru la nivel înalt "Instrumente necesare pentru îmbunătățirea controlului managerial, ca obligație în procesul de aderare la UE (managementul crizei)" destinat conducătorilor structurilor Guvernului. Întrevederea a avut scopul de a informa și prezenta modalități de diminuare a efectelor generate de crize în sistemul guvernamental. Finalmente, autorul urmează a se conforma principiilor activității de legiferare, potrivit cărora actul normativ trebuie să se integreze organic în cadrul normativ în vigoare, scop în care proiectul actului normativ trebuie corelat cu prevederile actelor normative de nivel superior sau de același nivel cu care se află în conexiune. Subsidiar, învederăm că autorul proiectului urmează a se conforma prevederilor art.54 a Legii cu privire la actele normative, și a expune conținutul proiectului într-un limbaj simplu, clar și concis, pentru a se exclude orice echivoc, cu respectarea strictă a regulilor gramaticale, de ortografie și de punctuație.	
3.	**Comisia Electorală Centrală** *(nr. CEC-8/9742 din 16 decembrie 2025)*	1.	Referitor la adresa dumneavoastră, înregistrată la Comisie sub nr. CEC-7/24839 din 11 decembrie 2025, prin care transmiteți pentru informare proiectul definitivat de Hotărâre a Guvernului cu privire la aprobarea proiectului Hotărârii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 (număr unic 905/MDED/2025, autor – Ministerul Dezvoltării Economice și Digitalizării), propunem completarea obiectivului specific 3.3 „Consolidarea cooperării interne între autoritățile și instituțiile publice, precum și mass-media pentru a lupta eficient împotriva manipulărilor electorale și a atacurilor cibernetice” din Programul național de securitate cibernetică pentru anii 2026-2030 cu subpunctele 3.3.2, 3.3.3 și 3.3.4 având următorul conținut.	**Nu se acceptă.** Obiectivele Programului național de securitate cibernetică pentru anii 2026–2030 sunt orientate către consolidarea capacităților și rezilienței cibernetice la nivel național, având un caracter transversal și intersectorial. În acest sens, Programul nu dezvoltă obiective sectoriale specifice, acestea fiind în responsabilitatea documentelor de politici publice

			Nr. d/o	**Acțiuni unice identificabile**	**Indicatori de monitorizare**	**Termenul limită (trimestru/an)**	**Instituție responsabilă**	sectoriale, inclusiv cele din domeniul electoral.
			Obiectivul 3.3 Consolidarea cooperării interne între autoritățile și instituțiile publice, precum și mass-media pentru a lupta eficient împotriva manipulărilor electorale și a atacurilor cibernetice					
			3.3.2	Standardizare și audit de securitate pentru SI electorale	Auditul de securitate cibernetică la Comisia Electorală Centrală elaborat și exerciții pentru testarea rezilienței infrastructurii electorale efectuate:	2026-2030	Comisia Electorală Centrală Agenția pentru Securitate Cibernetică Serviciul Tehnologia Informației și Securitate Cibernetică	

				- înainte de fiecare ciclu electoral; - după fiecare scrutin național.		Serviciul de Informații și Securitate	
			3.3.3	Elaborarea unui Plan de răspuns la incidente cibernetice electorale	Planul de răspuns la incidente cibernetice electorale elaborat	2026-2030	Comisia Electorală Centrală Agenția pentru Securitate Cibernetică Serviciul Tehnologia Informației și Securitate Cibernetică Serviciul de Informații și Securitate
			3.3.4	Asigurarea protecției împotriva DDoS asupra site-urilor CEC și monitorizarea 24/7	Soluțiile avansate anti-DDoS pentru: - site-urile electorale, - API-urile critice elaborate.	2026-2030	Comisia Electorală Centrală Serviciul Tehnologia Informației și Securitate Cibernetică
4.	**Agenția de Guvernare Electronică** *(nr. 3007-246 din 16.12.2025)*		Agenția de Guvernare Electronică reiterează obiecția cu privire la necesitatea excluderii AGE din coloana aferentă instituțiilor responsabile pentru realizarea acțiunii 3.1.7 de la Obiectivul specific 3.1, formulată prin scrisoarea nr. 3007-230 din 25.11.2025.				**Se acceptă.** Acțiunea a fost exclusă.

			Suplimentar, atragem atenția, că obiecția dată a fost acceptată de către autor, mențiune care de altfel se regăsește în Sinteza obiecțiilor și propunerilor la proiect.	
5.	**Agenția pentru Securitate Cibernetică** *(nr. 09-735 din 17.12.2025)*	1.	La obiectivul specific 2.1. Consolidarea competențelor și abilităților ale entităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice şi infracţiunilor în domeniul comunicaţiilor electronice, sugerăm excluderea subpct. 2.1.3. Această propunere derivă din faptul că acțiunea din subpct. respectiv se regăsește deja ca sarcină pentru Agenție la obiectul general 1 Consolidarea capacităților operaționale.	**Se acceptă.**
		2.	La pct. 1.1.2 care presupune "stabilirea unui sistem centralizat integrat pentru schimbul de informații între furnizorii de servicii din sectoarele critice.", pentru claritate și evidențierea faptului că acest mecanism este unul distinct față de cel stabilit la subpct. 1.1.1 și subpct. 1.2.9, propunem următoarea redacție a acestuia: „1.1.2 Crearea unui mecanism centralizat pentru schimbul de informații cu furnizorii de servicii în sectoarele critice". Specificăm că acest mecanism va fi realizat după modelul de schimb de informații ISAC.	**Se acceptă.**
6.	**Ministerul Afacerilor Interne** *(nr. 38/4444 din 17.12.2025)*	1.	Astfel, conform **pct. 17** din Regulamentul cu privire la planificarea strategică, Programul se constituie din partea descriptivă și partea operațională (planul de acțiuni), iar **pct. 18** descrie detaliat structura părții descriptive al Programului. Prin urmare, se va lua în considerare următoarele obiecții: 1. Completarea Capitolului I „Introducere", cu informații privind părțile implicate în elaborarea programului *(pct. 18.1 din Regulamentul cu privire la planificarea strategică, aprobat prin HG nr. 386/2020)*, de altfel se creează impresia că MDED a elaborat unilateral acest proiect.	**Se acceptă.** Capitolului I „Introducere" a fost completat cu următorul text: „*La elaborarea Programului, autoritățile și instituțiile publice indicate la capitolul VII au contribuit, în limita competențelor, la procesul de elaborare și consultare inițiat de Ministerul Dezvoltării Economice și Digitalizării. Aceste autorități au furnizat perspective sectoriale esențiale pentru consolidarea rezilienței cibernetice, în special în*

				sectoarele care gestionează infrastructura critică națională.”
		2.	Divizarea Capitolului III „Obiective generale și specifice” în două capitole separate – „Obiective generale” și „Obiective specifice” și vor fi completate cu informații relevante, în corespundere cu cerințele *pct. 8, subpct. 18.3 și 18.4 din Regulamentul cu privire la planificarea strategică*.	**Nu se acceptă.** Hotărârea Guvernului nr. 386/2020 cu privire la planificarea strategică nu stabilește obligativitatea divizării în capitole distincte a obiectivelor generale de cele specifice. În același timp, acestea respectă cerințele stabilite de pct. 18 subpunctele 18.3 și 18.4 din Regulamentul cu privire la planificarea strategică.
		3.	Crearea unui Capitol separat „Indicatori de monitorizare”, care va fi completat corespunzător cerințelor *subpct. 18.5 din Regulamentul enunțat*.	**Precizare.** Indicatorii de monitorizare sunt integrați în mod corespunzător în structura Programului: indicatorii de rezultat sunt prezentați pentru fiecare obiectiv specific în Capitolul III, iar indicatorii de impact, corelați cu obiectivele generale, sunt incluși în Capitolul IV. Această abordare respectă cerințele metodologice prevăzute la subpunctul 18.5 din Regulamentul aprobat prin HG nr. 386/2020, fără a impune necesitatea creării unui capitol separat dedicat indicatorilor.
		4.	Descrierea Capitolului VII „Monitorizare, evaluare și raportare”, conform prevederilor HG nr. 386/2020, în special completarea	**Nu se acceptă.**

			acestuia cu informații privind modalitatea de evaluare intermediară, precum și referitor la conținutul rapoartelor de evaluare.	Capitolului VII „Monitorizare, evaluare și raportare” întrunește toate elementele stabilite de Hotărârea Guvernului 386/2020 cu privire la planificarea strategică și cadrul metodologic aferent.
		5.	La pct. 38 din Capitolul II al Programului se va utiliza denumirea corectă a subdiviziunii, ca urmare a reorganizării Inspectoratului național de investigații, și anume „Centrul pentru combaterea crimelor cibernetice al Inspectoratului național de investigații al Inspectoratului General al Poliției”.	**Se acceptă.**
			La Obiectivul specific 2.1 din Planul de acțiuni pentru implementarea Programului menționat:	
		6.	2.1. Coroborând prevederile acțiunilor 2.1.1 și 2.1.3 se denotă că acestea se referă la aceeași acțiune specifică și indicator de monitorizare, însă expus cu text diferit. De asemenea, se relevă că textul „instituirea unui mecanism de coordonare și cooperare interinstituțională” din acțiunea 2.1.1 este echivoc și interpretabil. Prin urmare, în ordinea celor expuse supra se optează pentru excluderea acțiunii 2.1.1.	**Se acceptă parțial.** Acțiunea 2.1.3 a fost exclusă.
		7.	La acțiunea 2.1.2, în vederea indicării corespunzătoare a tipului de instruire ce urmează să fie efectuate se propune substituirea textului „securitate cibernetică” cu textul „prevenirea și combaterea criminalității informatice”.	**Se acceptă.** Textul a fost revizuit, după cum urmează: „*Cel puțin 20 de profesioniști instruiți în prevenirea și combaterea criminalității informatice și/sau certificați în domeniul criminalisticii digitale.”*
		8.	La acțiunea 2.1.4, se propune modificarea termenului-limită de realizare, prin substituirea textului „T1 2026” cu textul „T4 2026”, având în vedere necesitatea informării prealabile a populației cu	**Se acceptă.**

			privire la operaționalizarea instrumentului/platformei online de raportare a infracțiunilor informatice. Corelativ, se subliniază că termenul de realizare al acțiunii 2.1.5 corelativă acțiunii 2.1.4. este T4 2026.	
		9.	La obiectivul specific 2.2., acțiunea 2.2.1, se constată că acțiunea privind reacreditarea Laboratorului de expertiză criminalistică în domeniul cibernetic este practic realizată. În aceste condiții, se impune reevaluarea oportunității includerii acesteia ca acțiune distinctă în cadrul obiectivului, urmând să fie exclusă sau se va indica termenul de realizare al acesteia T1 2026.	**Se acceptă parțial.** Termenul a fost revăzut în T 1 2027. În situația realizării anticipate, acest fapt va constitui un avantaj pentru implementarea Programului și pentru consolidarea capacităților naționale în domeniu.
		10.	Totodată, reieșind din faptul că Ministerul Afacerilor Interne va asigura implementarea Planului menționat prin intermediul Inspectoratului General al Poliției, se consideră judicios ca la compartimentul „Cod program/ Subprogram bugetar, denumirea sursei de finanțare” să fie specificat codul subprogramului bugetar al Inspectoratului General (în speță „3502”) pentru toate acțiunile unde figurează ca instituție responsabilă ministerul.	**Precizare.** Codul programului/ subprogramului bugetar este indicat exclusiv pentru acele acțiuni pentru care există acoperire bugetară identificată și care sunt planificate și reflectate în cadrul Cadrului Bugetar pe Termen Mediu.
7.	**Institutul de Standardizare din Moldova** *(nr. 01-02/564 din 7.12.2025)*		ISM a examinat proiectul de hotărâre și, în urma analizei efectuate a dispozițiilor acestuia, constată că, observațiile și obiecțiile formulate anterior rămân pe deplin valabile. În consecință, ISM își menține poziția exprimată asupra necesității de a lua în considerare obiecțiile prezentate în scrisoarea nr. 04-03/545 din 28.11.2025 (a se vedea în Anexă), care a fost transmisă Ministerului Dezvoltării Economice și Digitalizării, în vederea revizuirii corespunzătoare a proiectului menționat supra.	**Precizare.** Ministerul Dezvoltării Economice și Digitalizării a luat în considerație propunerile expuse în scrisoarea nr. 04-03/545 din 28.11.2025 a Institutului de Standardizare din Moldova (ISM). A acceptat din start includerea ISM în calitate de instituție coresponsabilă la acțiunea 1.2.2 (a se vedea

				versiunea proiectului expediată spre notificare). Totodată, Ministerul a prezentat în sinteză clarificări privind modul de calculare a costurilor estimative expuse la acț. 1.2.1. Estimarea costurilor pentru acțiunea 1.2.1 a fost realizată, pentru 1 standard, în conformitate cu Manualul privind estimarea costurilor documentelor de politici publice din Republica Moldova, instrument metodologic recomandat de Cancelaria de Stat și Ministerul Finanțelor pentru toate documentele de politici. Costurile au fost calculate pentru 1 standard aprobat anual, întrucît la această etapă este prematur de a estima numărul exact al standardelor ce va fi necesar a fi aprobate și actualizate în următorii ani, reieșind din faptul că urmează a fi transpuse noi acte UE ce posibil vor necesita aprobarea standardelor noi.
8.	**Ministerul Finanțelor**		La Planul de acțiuni pentru implementarea Programului Național de Securitate Cibernetică pentru anii 2026-2030, din Obiectivul specific 1.2. Acțiunea 1.2.9 ,,Crearea unei platforme centralizate de raportare și gestionare a vulnerabilităților cibernetice” urmează a fi exclus. Evidențiem că conform proiectului de hotărâre cu privire la aprobarea Regulamentului privind divulgarea coordonată a	**Se acceptă.** Acțiunea a fost exclusă.

			vulnerabilității în domeniul securității cibernetice (număr unic 714/MDED/2025) prezentat de MDED (demers nr.13/2-3431 din 03.12.2025) cu titlu de informare către Ministerul Finanțelor, autorul menționează în Sinteza obiecțiilor și propunerilor la proiectul de hotărâre de Guvern că în scopul eficientizării cheltuielilor, datele și documentația aferente procesului de divulgare coordonată a vulnerabilităților vor fi luate la evidență în Registrul de stat al incidentelor cibernetice. Prin urmare, ca rezultat va fi creat doar Registrul de stat al incidentelor cibernetice. Totodată, urmează a fi revizuit Capitolul V „Costuri” și pct. 4.2 din Nota de fundamentare privind impactul financiar.	
9.	**Cancelaria de Stat** *(nr. 21/1-69-12857 din 16.12.2025)*		Prin prezenta, Cancelaria de Stat a examinat repetat proiectul de hotărâre cu privire la aprobarea proiectului hotărârii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030 (număr unic 905/MDED/2025), și în conformitate cu competențele funcționale, comunică susținerea acestuia. Totodată, având în vedere că obiectivele strategice în domeniul securității cibernetice au fost integrate în Strategia securității naționale a Republicii Moldova (aprobată prin Hotărârea Parlamentului nr. 391/2023), iar proiectul Programului național de securitate cibernetică pentru anii 2026–2030 asigură și realizarea acestora la nivel operațional, se propune aprobarea acestuia prin hotărâre de Guvern.	**Se acceptă.**

Secretar de stat **Michelle ILIEV**