Aprobat în ședința Guvernului din _____ 2025

Decizia protocolară nr._____/2025

Proiect

GUVERNUL

HOTĂRÂRE Nr. ___
din _____

cu privire la aprobarea proiectului hotărîrii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030

Guvernul HOTĂRĂŞTE:

Se aprobă şi se prezintă Parlamentului spre examinare proiectul hotărîrii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030.

PRIM-MINISTRU

PARLAMENTUL REPUBLICII MOLDOVA

HOTĂRÂRE

pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030

În temeiul art.6 alin.(3) lit.a) din Legea nr. 48/2023 privind securitatea cibernetică, Parlamentul adoptă prezenta hotărâre.

Art. 1 - Se aprobă Programul național de securitate cibernetică pentru anii 2026-2030, prevăzut în anexă.

Art. 2 - Autorităţile şi instituţiile publice responsabile vor realiza acţiunile prevăzute în anexa la Programul național de securitate cibernetică pentru anii 2026-2030.

Art. 3 - Prezenta hotărâre intră în vigoare la data adoptării.

PREȘEDINTELE PARLAMENTULUI

Anexă

Programul național de securitate cibernetică pentru anii 2026-2030

Capitolul I
INTRODUCERE

1. Programul național de securitate cibernetică pentru anii 2026–2030 (în continuare – *Programul*) 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, nu doar 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. Programul este elaborat în conformitate cu Obiectivele de Dezvoltare Durabilă (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 privind 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 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. Programul 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, Programul răspunde obiectivelor privind prevenirea și combaterea amenințărilor hibride în domeniul securității cibernetice și informaționale, stabilite în Programul de activitate al Guvernului "Moldova prosperă, sigură, europeană", aprobat prin Hotărârea Parlamentului nr. 28/2023.
5. Programul este aliniat cu Acordul de Asociere[1], care prevede priorități privind prevenirea și combaterea criminalității, inclusiv a criminalității informatice.
6. De asemenea, 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**:

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A22014A0830%2801%29.

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, Programul 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;

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 UE;

7.1.7. Alinierea la normele UE 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 de apărare națională 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. **Strategiei de dezvoltare "Educația 2030",** aprobată 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 de prevenire și combatere a criminalității pentru anii 2022–2025** (HG nr. 948/2022) **și Proiectul de Program de prevenire și combatere a criminalității pentru anii 2026–2030:**

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

7.8.1. Subcapitolul 10.5. Servicii de încredere și securitate cibernetică;

7.8.2. Subcapitolul 24.1.5. Prevenirea și combaterea criminalității informatice.

8. Nu în ultimul rând, Programul răspunde acțiunilor prevăzute 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 prevederile Legii nr. 48/2023 privind securitatea cibernetică, care prevede obligativitatea aprobării unui document de politici în domeniul securității cibernetice.
9. Suplimentar, la elaborarea 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”[2].
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, dintre care aproape o treime au fost acțiuni rău intenționate, cu un impact major asupra sectoarelor critice precum comunicațiile, sănătatea, energia și transporturile[3]. În acest context, și Republica Moldova, în pofida eforturilor recente de aliniere la standardele europene, rămâne vulnerabilă la atacuri cibernetice care pot afecta stabilitatea națională, infrastructurile critice și încrederea populației în serviciile digitale.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020JC0018

[3] https://ciras.enisa.europa.eu/ciras-consolidated-reporting

11. Transformarea digitală accelerată a economiei moldovenești, cu un sector IT care contribuie semnificativ la PIB și la exporturi, implică nu doar oportunități, ci și expuneri crescute la riscuri cibernetice. Estimările privind pierderile economice, cauzate de criminalitatea cibernetică, plasează prejudiciul anual pentru Republica Moldova la circa 49 milioane dolari SUA, o cifră semnificativă raportată la dimensiunea economiei naționale. În plus, indicele global al securității cibernetice (GCI[4]) al Uniunii Internaționale pentru Telecomunicații (UIT) evidențiază deficiențe importante 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 aproba Programul. Programul definește obiectivele strategice, măsurile de politică și cele de reglementare, cu scopul atingerii și menținerii unui nivel înalt de securitate a rețelelor și sistemelor informatice, precum 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, aflată în competența Ministerului Apărării și a entităților subordonate acestuia, Programul nu intervine direct asupra acestui segment, ci urmărește doar corelarea obiectivelor și acțiunilor propuse cu obiectivele Strategiei de apărare națională 2024–2034.
14. Prin acest 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 procesul de elaborare, în Program au fost reflectate contribuțiile autorităților administrației publice centrale, inclusiv ministere de resort și autorități autonome, cu atribuții relevante domeniului securității cibernetice sau conexe acestuia. Aceste autorități publice au oferit perspective sectoriale importante pentru consolidarea rezilienței cibernetice în domeniile pe care le gestionează, în special cele legate de infrastructura critică națională.

Capitolul II

ANALIZA SITUAȚIEI

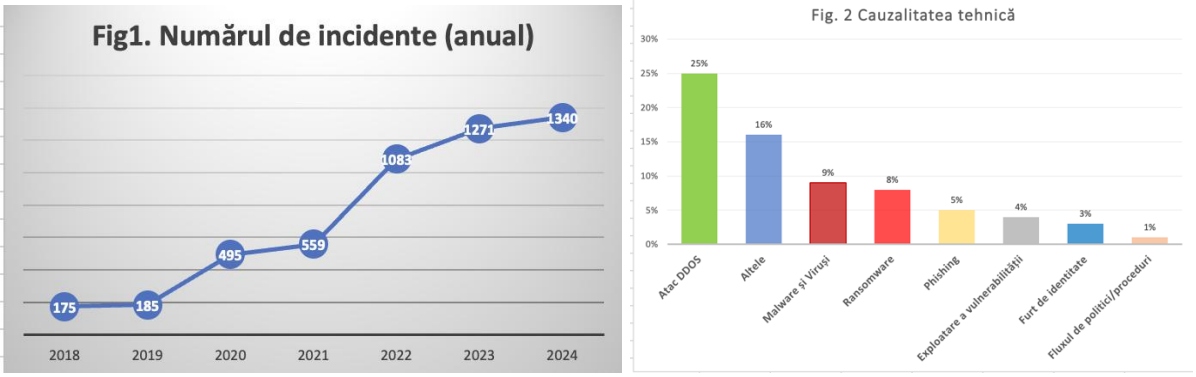
16. Digitalizarea a fost motorul dezvoltării economice în ultimele decenii. Ea a asigurat o interconectare globală tot mai mare și a redus barierele în relațiile dintre țări. În perioade de turbulențe geopolitice, această interdependență digitală poate duce la provocări majore. În plus, digitalizarea 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 continuă 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 3251 de incidente cibernetice cu impact semnificativ[5], conform criteriilor stabilite de Directiva

[4] Global Cybersecurity Index (Indicele global de securitate cibernetică)

[5] https://ciras.enisa.europa.eu/ciras-consolidated-reporting

NIS1[6], Codul european al comunicațiilor electronice[7] și Regulamentul eIDAS[8]. Dintre acestea, 29% au fost considerate acțiuni rău intenționate. Cel mai afectat sector a fost sectorul privat, în special domeniile comunicațiilor, 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 1402 de 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 (ENISA)

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 1340 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, 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 IBM privind costul unei încălcări a securității datelor în 2024*[9], 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[10], care a evaluat pierderile economice cauzate de criminalitatea informatică, intitulat *"Pierderi nete: estimarea costului global al*

[6] Directiva (UE) 2016/1148 a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016L1148

[7] Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11 decembrie 2018 de instituire a Codului european al comunicațiilor electronice: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02018L1972-20241018.

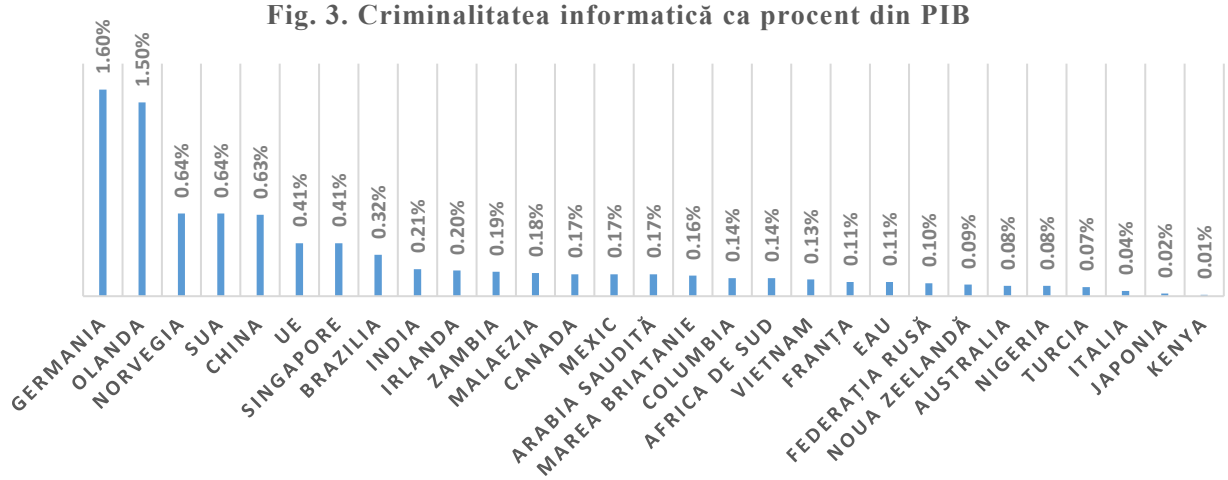
[8] Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:02014R0910-20241018.

[9] https://www.ibm.com/reports/data-breach

[10] https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis

criminalității informatice", oferă o estimare a impactului economic al criminalității

Fig. 3. Criminalitatea informatică ca procent din PIB



informatice pentru diferite țări, exprimat ca procent din PIB. Graficul prezentat în *figura 3* evidențiază țările cele 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 produsul intern brut al țării a fost de aproximativ 16,5 miliarde de dolari americani în 2023, se poate estima un prejudiciu anual potențial de aproximativ 49 de milioane de dolari, pe baza mediei de 0,3% din PIB.

Sursa: Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA)

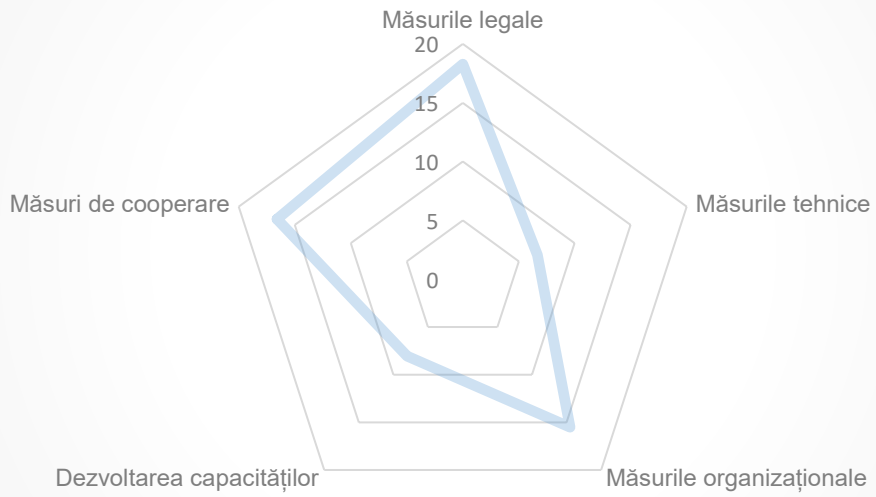
22. În Republica Moldova, fenomenul criminalității organizate a evoluat semnificativ în ultima perioadă, reflectând o tendință de adaptare și diversificare a activităților infracționale. Numărul infracțiunilor comise de grupuri criminale a crescut de peste patru ori, de la 201 cazuri în 2023 la 205 cazuri 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[11].
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. 77% 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 ceva mai scăzut, 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%).[12]
24. Conform Indicelui Global de Securitate Cibernetică (GCI) al UIT pentru 2024, Republica Moldova are un scor general de 65,09, iar performanța țării este descrisă ca fiind de nivel 3 (nivelul 3 reprezintă țările care au obținut un scor general de cel puțin 55/100),

[11] Ministerul Afacerilor Interne – Proiectul Programului pentru prevenirea și combaterea criminalității pentru perioada 2026-2030.

[12] *https://ega.ee/wp-content/uploads/2024/01/EGA-Online-safety-awareness_-results.pdf*

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.[13] Conform raportului UIT privind echipa națională de răspuns la incidente de securitate cibernetică, performanța Republicii Moldova pentru 2024, comparativ cu 2020, a înregistrat o creștere a măsurilor legale, organizaționale și de cooperare, însă o scădere notabilă a măsurilor tehnice și de dezvoltare a capacităților, dar acest lucru poate fi atribuit parțial ajustărilor metodologice și ponderilor GCI, precum și modificărilor aduse întrebărilor. Graficul de mai jos (*Figura 4*) evidențiază performanța Republicii Moldova în GCI pentru 2024, subliniind că măsurile tehnice și consolidarea capacităților sunt punctele slabe ale Republicii Moldova în acest domeniu. Cu toate acestea, acest indice poate fi îmbunătățit prin implementarea corespunzătoare a legislației naționale armonizate cu legislația UE.

Fig. 4 Performanța Republicii Moldova în GCI pentru 2024



Sursa: Uniunea Internațională a Telecomunicațiilor (UIT)

25. Industria IT în Republica Moldova se dezvoltă rapid. În 2023, industria IT a atins o pondere de peste 5,3% din produsul intern brut, 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 perioada 2025-2029 acordă prioritate punerii în aplicare a Legii 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

[13] https://www.itu.int/epublications/publication/global-cybersecurity-index-2024

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 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 UE 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, 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 UE 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 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, societatea informațională, tehnologia informației, economia digitală, securitatea cibernetică și guvernanța internetului. De asemenea, este autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul comunicațiilor electronice, inclusiv elaborarea, coordonarea și monitorizarea politicilor privind gestionarea domeniului de nivel superior .md, precum și 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 ține evidența furnizorilor de servicii din sectoarele și subsectoarele critice, de a supraveghea și 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" (STISC), în subordinea Cancelariei de Stat, 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 (PKI) a Guvernului, precum și administrează centrele de date din sectorul public. STISC exercită funcție de CERT-Gov, echipă de răspuns la incidente cibernetice (CSIRT) în sectorul public, adică o echipă responsabilă numai pentru rețele și sisteme informatice de stat.
35. Agenția de Guvernare Electronică (AGE) în subordinea Cancelariei de Stat este responsabilă pentru implementarea politicilor în domeniile de modernizare a serviciilor guvernamentale, și transformarea digitală a guvernării, gestionează platforme și servicii electronice guvernamentale (MConnect, MPass, MSign, MPay, etc). De asemenea, AGE are și responsabilități ce țin de asigurarea securității informației în autoritățile și instituțiile din sectorul public în procesul de e-Transformare a guvernării. AGE împreună cu partenerii săi ia măsuri juridice, organizatorice și tehnice complexe de garantare a securității informațiilor. Conform regulamentului său de activitate, principalele responsabilități ale AGE 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. Serviciul de Securitate și Informații (SIS) are un rol important în protejarea infrastructurii critice din țară, precum și a sistemelor speciale de telecomunicații. În calitate de serviciu de inteligență, SIS este responsabil pentru asigurarea securității naționale atît 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, cât și a activităților malițioase ale actorilor cibernetici statali. De asemenea, Serviciului de Informații și Securitate îi revine atribuția de autorizare a sistemelor informatice, care prelucrează informația atribuită la secret de stat. SIS realizează informări în adresa autorităților naționale privind amenințările cibernetice din spațiul cibernetic național și regional. .
37. Centrul pentru combaterea crimelor informatice al Inspectoratului Național de Investigații al Inspectoratului General de Poliție al Ministerului Afacerilor Interne este unitatea principală de investigare a criminalității informatice, însărcinată cu activități de investigație specială și de urmărire penală în materie de criminalitate informatică. Centrul este activ în furnizarea de asistență și îndrumare unităților de poliție locale în materie de criminalitate cibernetică și dovezi electronice. Centrul are un contract bilateral cu CERT-GOV pentru schimbul de informații privind incidentele cibernetice. Centrul cooperează, de asemenea, cu SIS și le oferă informații despre situația din spațiul cibernetic național.

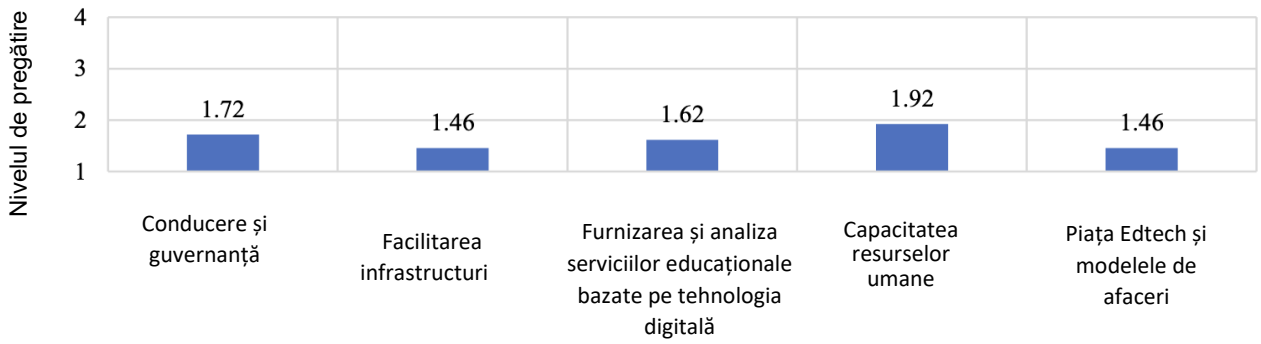
38. Procuratura Generală are o secție specializată - Secția combaterea crimelor cibernetice, însărcinată cu investigarea și urmărirea penală a cazurilor de criminalitate informatică, cu investigarea întregului spectru de infracțiuni prevăzute de articolul 2-10 din Convenția de la Budapesta, precum și a infracțiunilor conexe împotriva sau cu utilizarea sistemelor informatice și a datelor.
39. Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI) 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 ANRCETI este stabilit de Guvern. Cu toate acestea, această entitate este autonomă față de Guvern în activitatea sa de reglementare.
40. Ministerul Apărării și Armata Națională a Republicii Moldova are propriile capacități defensive și echipa sa de răspuns la incidente cibernetice (CERT militar) pentru a-și proteja propriile rețele.
41. Instituția 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 soluțiilor inovatoare pentru protecția infrastructurilor critice 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.
42. Centrul Național de Management al Crizelor, prevăzut în Legea Nr. 248/2025 privind managementul situațiilor de criză, 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.
43. 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 UE. 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 UE 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.[14]
44. 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 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. Datorită escaladării rapide și complexității lor, rezolvarea crizelor cibernetice necesită un mecanism bine pregătit și fiabil, care trebuie să fie bine integrat cu resursele generale de gestionare a

[14] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32017H1584

crizelor ale statului și să aibă, de asemenea, o capacitate foarte bună de cooperare internațională.

45. 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 "Educația 2030"[15], 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.
46. Dezvoltarea competențelor digitale reprezintă, de asemenea, o prioritate în cadrul Strategiei de dezvoltare "Educația 2030". În 2022, Banca Mondială a evaluat cinci domenii ale pregătirii digitale a sistemului de învățământ din Republica Moldova, concluzionând ca fiind la nivel "*emergent*", unde investițiile fundamentale au progresat, dar multe probleme rămân nerezolvate (*a se vedea figura 6*). În prezent, o parte integrantă a competențelor digitale o constituie cunoștințele în domeniul securității cibernetice. Lipsa generală de profesori și manageri calificați, bine pregătiți și motivați este una dintre provocările abordate în strategie, dar și 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 limitează 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.

Figura 6: Moldova – Evaluarea pregătirii pentru educația digitală 2021-2022 în Republica Moldova.



Sursa: Banca Mondială [16]

47. Conform sondajului privind conștientizarea siguranței online în Moldova, realizat în 2023[17], 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

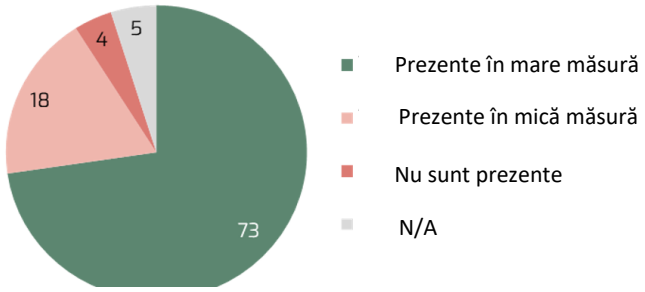
[15] https://www.legis.md/cautare/getResults?doc_id=136600&lang=ro

[16] Banca Mondială. Moldova – Evaluarea pregătirii pentru educația digitală 2021-2022, https://documents1.worldbank.org/curated/en/099120006252220689/pdf/P17773104ea6f2040a88e02bdf9bbd04f6.pdf

[17] *https://ega.ee/wp-content/uploads/2024/01/EGA-Online-safety-awareness_-results.pdfegov.md/ro/node/40718*

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 7: Răspunsuri la întrebările "În ce măsură credeți că manipularea, propaganda și dezinformarea sunt prezente în conținutul postat pe rețelele de socializare?"



Sursa: e-Governance Academy (Estonia) și Magenta Consulting

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

    47.1. **Creșterea numărului de atacuri cibernetice** – Atacurile asupra entităților publice și private s-au intensificat, punând în pericol infrastructurile critice și datele cetățenilor.

    47.2. **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.

    47.3. **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.

    47.4. **Capacitate instituțională limitată** – Autoritățile publice cu responsabilități în domeniul securității cibernetice nu dispun de resurse și expertiză suficiente pentru a face față amenințărilor emergente.

    47.5. **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.

    47.6. **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.

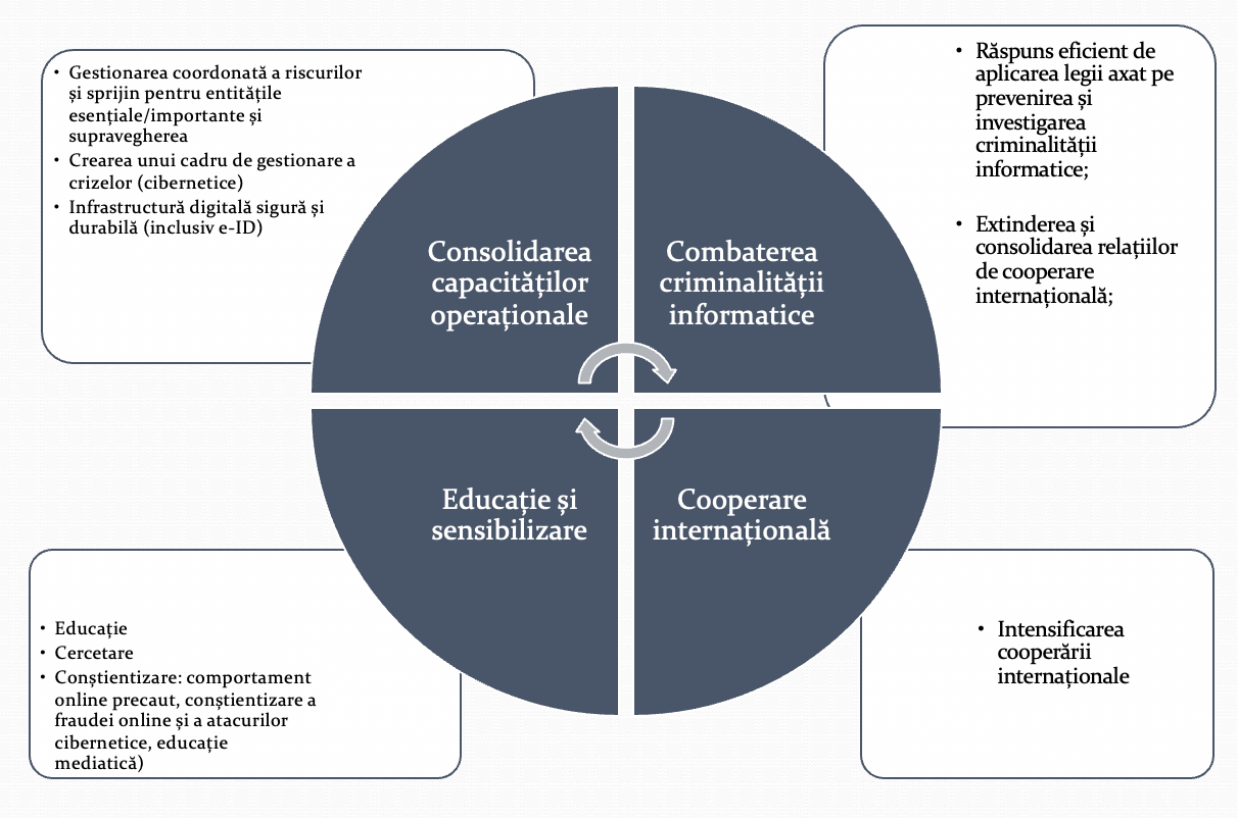
    47.7. **Securitatea cibernetică a infrastructurilor critice** – Sistemele energetice, financiare, sănătate și de transport necesită măsuri urgente de protecție împotriva amenințărilor cibernetice sofisticate.

    47.8. **Cooperare internațională insuficientă** – Deși Republica Moldova a început

procesul de integrare în inițiativele internaționale de securitate cibernetică, nivelul de colaborare cu partenerii externi trebuie 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.

47.9. **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.

49. Ca răspuns la aceste provocări, Programul prevede 4 domenii principale de intervenție:
    I. Consolidarea capacităților operaționale;
    II. Combaterea criminalității informatice;
    III. Educație și sensibilizare;
    IV. Cooperare internațională.



Domeniul de intervenție I – Consolidarea capacităților operaționale

50. 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. Următorul pas este consolidarea capacităților operaționale ale țării pentru implementarea cadrului creat. Programul 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.

51. Este necesară sprijinirea autorităților și 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, recupera și 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.
52. 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 2022 a fost aprobat conceptul registrului de stat al incidentelor de securitate cibernetică, iar Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică" (STISC) 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 menționat 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 Programului 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.
53. 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 Programului.
54. 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 Națională de Securitate, oferă o oportunitate bună de a crea un mecanism robust și eficient de gestionare a crizelor cibernetice. La data de 10 iulie 2025, Parlamentul a adoptat Legea nr. 248/2025 privind managementul situațiilor de criză. Legea stabilește cadrul juridic, organizatoric (funcțional și instituțional), operațional și de coordonare a gestionării crizelor în Republica Moldova. În acest context, un obiectiv în 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 UE. 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.
55. 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 a te identifica și interacționa online în siguranță, transformarea digitală nu poate fi completă. În 2024, serviciul de autentificare MPass a fost utilizat de

peste 20 de milioane de ori de aproximativ 200.000 de utilizatori, iar serviciul MSign a fost folosit pentru peste 53 de milioane de semnături electronice de 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 recunoașterii legale a identificării electronice și a serviciilor de încredere în întreaga UE, armonizarea cu Regulamentul eIDAS trebuie să fie o prioritate.

56. Obținerea unei imagini precise a situației securității cibernetice, inclusiv peisajul amenințărilor, incidentele și impactul acestora, este esențială. În acest scop, trebuie dezvoltată capacitatea de identificare și analiză a amenințărilor cibernetice, precum și capacitatea centralizată de raportare și gestionare a incidentelor la nivel național.
57. Printre problemele-cheie în acest domeniu se numără:
    - 56.1 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.
    - 56.2 Deficiențe în colectarea, raportarea, înregistrarea și analiza centralizată a incidentelor cibernetice împiedică obținerea unei imagini clare asupra situației naționale, atât la nivel operațional, cât și 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

58. 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. Combinat 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 a societății și a 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 peisajul amenințărilor de astăzi[18].
59. Strategia securității naționale 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[19]. 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[20].
60. În 2025, Moldova se confruntă cu mai multe provocări semnificative în combaterea criminalității cibernetice, influențată de tensiunile geopolitice, limitările infrastructurale

[18] RUSI. https://www.rusi.org/explore-our-research/publications/commentary/why-biasing-advanced-persistent-threats-over-cybercrime-security-risk

[19] Strategia Națională de Securitate a Republicii Moldova, Viziunea Președintelui Republicii Moldova

[20] Raportul pe 2024 al Republicii Moldova, DOCUMENT DE LUCRU AL SERVICIILOR COMISIEI, Bruxelles, 30.10.2024 SWD(2024) 698 final https://data.consilium.europa.eu/doc/document/ST-15129-2024-INIT/en/pdf

și evoluția amenințărilor digitale.

61. Conform studiului „World Cybercrime Index”[21], 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.
62. Principalele amenințări legate de criminalitatea cibernetică pentru Republica Moldova sunt:
    - 61.1 **Amenințări cibernetice sponsorizate de stat și atacuri hibride**. Republica Moldova a fost supusă unor atacuri cibernetice legate de actori străini, în special din Federația Rusă.[22] Aceste atacuri urmăresc să perturbe operațiunile guvernamentale și să erodeze încrederea publică, în special 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 UE, evidențiind vulnerabilitățile operațiunilor cibernetice motivate politic.
    - 61.2 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 legat de un atac ransomware de 4,5 milioane de euro asupra Organizației Olandeze pentru Cercetare Științifică, demonstrând rolul Republicii Moldova în investigațiile internaționale privind criminalitatea cibernetică. 23
    - 61.3 Atacuri cibernetice asupra infrastructurii critice. Infrastructura critică a Republicii Moldova, inclusiv sistemele de sănătate24 și de salarizare guvernamentale, a fost ținta unor atacuri cibernetice menite să submineze încrederea publicului în serviciile publicii 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.
    - 61.4 Insuficiența de profesioniști în securitatea cibernetică pe întregul ciclu de descoperire, constatare, 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 un fenomen de "exod de creiere" în care profesioniștii calificați caută oportunități în străinătate. Acest deficit împiedică dezvoltarea și implementarea unor strategii eficiente de apărare cibernetică.

---

[21] https://www.ox.ac.uk/news/2024-04-10-world-first-cybercrime-index-ranks-countries-cybercrime-threat-level#:~:text=Russia%20tops%20the%20list%2C%20followed,Right%3A%20Associate%20Professor%20Jonathan%20Lusthaus

[22] https://www.sis.md/sites/default/files/comunicate/fisiere/Raport_SIS_Public_Interferenta_in_procesul_electoral_0.pdf

[23] https://securityaffairs.com/177772/cyber-crime/moldovan-police-arrested-a-45-year-old-foreign-man-participating-in-ransomware-attacks-on-dutch-companies.html

[24] https://www.moldpres.md/eng/society/chisinaubased-hospital-victim-of-cyber-attack-

61.5 Provocări în materie de securitate cibernetică pentru IMM-uri. Întreprinderile mici și mijlocii (IMM-uri), care constituie peste 97% din companiile moldovenești25, sunt deosebit de vulnerabile la amenințările cibernetice. Resursele și conștientizarea limitate fac dificilă implementarea unor măsuri adecvate de securitate cibernetică, prezentând riscuri pentru ecosistemul economic mai larg.

63. 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 și în mai multe parteneriate internaționale, precum:

62.1 *Colaborarea cu Consiliul Europei:* 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.

62.2 *Sprijinul UE:* 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.

62.3 *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 inter-agenții și schimbul de cunoștințe.

64. De asemenea, autoritățile naționale au fost active în colaborarea internațională în domeniul aplicării legii, prin formatele Interpol și, de asemenea, 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.
65. Programul de prevenire și combatere a criminalității pentru anii 2022-2025[26] 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 UE și instituțiile relevante. Aceste probleme continuă a fi abordate și în proiectul Programului de prevenire și combatere a criminalității pentru anii 2026-2030, care vine cu o serie de măsuri pentru soluționarea acestora.

Domeniul de intervenție III - Educație și sensibilizare

66. 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[27]. În mod similar, există încă prea puține cunoștințe aprofundate de securitate cibernetică. Prin urmare, accentul necesită a fi pus pe consolidarea capacităților și proiectarea viitoarelor programe de educație și formare pentru a aborda deficitul de personal specializat în securitate cibernetică.

[25] https://old.eu4business.eu/moldova

[26] https://www.legis.md/cautare/getResults?doc_id=135455&lang=ro

[27] *https://ega.ee/wp-content/uploads/2024/01/EGA-Online-safety-awareness_-results.pdfegov.md/ro/node/40718*

67. Scopul Strategiei Naționale de Dezvoltare "Moldova Europa 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 non-formale și informale.[28] 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.
68. Strategia de transformare digitală 2023-2030[29] 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 unor resurse 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.
69. 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, este o problemă pe care părțile interesate din sectorul public și privat, organizații ale 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, dar este încă necesar un punct de contact comun, de preferință în sectorul public, prin care să poată fi organizată 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.
70. Din 2023, campania "*Siguranța Digitală*" este implementată de Academia de e-Guvernare (Estonia), în cooperare cu parteneri locali.[30] Campania face parte dintr-o misiune mai amplă de a crește gradul de conștientizare cu privire la siguranța online și de a oferi abilități printr-un curs online. Cu toate acestea, aceste inițiative 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

[28] https://moldova.unfpa.org/sites/default/files/pub-pdf/raport_de_progres_odd_2023_vf_07_08_2023_en_final.pdf

[29] Strategia de transformare digitală 2023-2030 - ttps://www.legis.md/cautare/getResults?doc_id=139408&lang=ro.

[30] Curs online oferit pe site-ul https://www.sigurantadigitala.md/

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 orice campanii de conștientizare.

71. Schimbarea gradului de conștientizare a subiectelor legate de siguranța online și securitatea cibernetică ar trebui evaluată în mod sistematic, inclusiv pentru a evalua impactul oricăror activități 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.
72. Unul dintre domeniile cele mai afectate care are mult de câștigat din cooperarea oportună și anticipată între părțile interesate din sectorul public și privat sunt alegerile. Pe de o parte, rezultatele votului 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.[31] 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.
73. Securitatea cibernetică și protecția datelor merg mână în mână și sunt doi aliați esențiali pentru protecția persoanelor și a drepturilor acestora. Tehnologiile de îmbunătățire a confidențialității sunt un bun exemplu în acest sens. Prin urmare, consolidarea cooperării și colaborării între agențiile de protecție a datelor și de securitate cibernetică permit 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

74. Unul dintre principalele mijloace de asigurare a securității cibernetice este intensificarea și îmbunătățirea cantitativă și calitativă a cooperării internaționale și a activităților mai active în cadrul organizațiilor și inițiativelor internaționale.
75. 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 rezervele de securitate cibernetică ale UE și la canalele internaționale de răspuns la incidente.
76. 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

[31]Sondaj privind conștientizarea siguranței online în Moldova, realizat în 2024 de Academia de e-Guvernare, Estonia și Agenția, Magenta Consulting, și finanțat de UE în cadrul proiectului de asistență rapidă în materie de securitate cibernetică din Moldova. și Academia de e-guvernare *https://ega.ee/wp-content/uploads/2024/01/EGA-Online-safety-awareness_-results.pdf*egov.md/ro/node/40718 *Sondaj privind conștientizarea siguranței online în Moldova, realizat în 2024 de Agenția de e-Guvernare, Magenta Consulting și Academia de Guvernare Electronică egov.md/ro/node/40718*

globale, gestionarea diplomației incidentelor transfrontaliere sau negocierea acordurilor internaționale privind securitatea digitală. Ministerul Afacerilor Externe al Republicii Moldova 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[32] al ONU sau dialogurile OSCE de consolidare a încrederii cibernetice.

77. Una dintre principalele provocări este armonizarea legislației naționale cu reglementările UE și integrarea în formatele și organizațiile de cooperare UE, urmând prioritățile naționale și liniile de acțiune pentru integrarea în Uniunea Europeană.
78. Al doilea factor foarte important în abordarea și alocarea resurselor pentru cooperarea internațională este natura globală a provocărilor în materie de securitate cibernetică. Majoritatea covârșitoare a incidentelor cibernetice și a infracțiunilor cibernetice sunt de natură transnațională, autorii, facilitatorii și victimele fiind localizați în 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, o reprezentare activă și participarea la forurile de cooperare internațională și o contribuție la activitatea lor.
79. 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.
80. Conform Legii nr. 48/2023 privind securitatea cibernetică, Agenția pentru Securitate Cibernetică în calitatea sa 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 sau entități internaționale înființate de acestea.

Capitolul III

OBIECTIVE GENERALE ȘI SPECIFICE

81. 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 și în Strategia de transformare digitală 2023–2030, precum și în alte documente strategice și de planificare, cum ar fi Strategia de dezvoltare „Educație 2030”, Strategia de dezvoltare a domeniului afacerilor interne 2022–2030, Strategia națională de apărare 2024–2034, Programul de prevenire și combatere a criminalității 2022–2025 (și proiectul pentru perioada 2026–2030) și Programul național

[32] Open-ended Working Group

de aderare a Republicii Moldova la UE 2025–2029.

82. 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.
83. 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 obiective specifice

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 reziliență 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	Creșterea numărului de cauze cu privire la infracțiunile informatice și infracţiunile în domeniul comunicaţiilor electronice remise în judecată	N/A	Creșterea cu 15%	Creșterea cu 30%

Obiectiv general	Obiectiv specific	Indicator	Valoarea de referință (2025)	Țintă (2028)	Țintă (2030)
		Sursa: Ministerul Afacerilor Interne			
	2.2. Crearea de instrumente tehnologice eficace și avansate pentru prevenirea, detectarea și investigarea eficientă a criminalității informatice	Dotarea cu instrumente și soluții inteligente de investigare *Sursa: Ministerul Afacerilor Interne*	8 instrumente (2024)	minim 9 instrumente	Creștere cu 25% (minim 10 soluții)
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[33] în rezerva totală de absolvenți de studii universitare *Sursa: Ministerul Educației și Cercetării, Biroul Național de Statistică*	13,7 % (2022)	15 %	16%

[33] STEAM: Science, Technology, Engineering, Arts, and Mathematics (Știință, Tehnologie, Inginerie, Artă și Matematică).

Obiectiv general	Obiectiv specific	Indicator	Valoarea de referință (2025)	Țintă (2028)	Țintă (2030)
	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, 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	4.1 Consolidarea cooperării	Creșterea scorului de țară la capitolul	15,51	16,5	18,5

Obiectiv general	Obiectiv specific	Indicator	Valoarea de referință (2025)	Țintă (2028)	Țintă (2030)
pentru a deveni 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	"măsuri de cooperare" *Sursa: Indicele global de securitate cibernetică al ITU*	(2024)		
	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

Capitolul IV

IMPACT

84. Pe lângă contribuția la realizarea obiectivelor și direcțiilor prioritare stabilite în documentele de politici publice de nivel superior, Programul și planul de acțiuni pentru implementarea acestuia sprijină obiectivele Republicii Moldova în ceea ce privește aderarea la Uniunea Europeană și armonizarea reglementărilor naționale ale Republicii Moldova cu legislația Uniunii Europene.
85. Implementarea Programului național de securitate cibernetică pentru anii 2026-2030 este de așteptat să genereze un impact semnificativ asupra securității cibernetice a Republicii Moldova. Dintre beneficiile așteptate trebuie relevate următoarele:
    84.1 **Îmbunătățirea protecției infrastructurilor critice**. Implementarea unor măsuri avansate de securitate va reduce vulnerabilitățile și riscul de atacuri cibernetice.
    84.2 **Consolidarea capacității instituționale**. Crearea unor mecanisme eficiente de coordonare și creșterea resurselor umane calificate în domeniul securității cibernetice.
    84.3 **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.
    84.4 **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.
    84.5 **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.
    84.6 **Combaterea criminalității informatice**. Consolidarea capacității de prevenire, detectare și investigare a criminalității informatice prin îmbunătățirea cooperării între autorități, cooperarea internațională și dezvoltarea unor mecanisme eficiente de sancționare a atacatorilor.
86. Trebuie remarcat faptul că digitalizarea accelerată a economiei moldovenești 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.
87. Cu toate acestea, un nivel scăzut de securitate cibernetică poate descuraja investițiile străine și poate afecta încrederea publicului în serviciile digitale. În acest context, implementarea Programului este esențială pentru asigurarea unui ecosistem digital sigur și rezilient, care să susțină dezvoltarea economică și modernizarea Republicii Moldova.
88. Pentru a aborda în mod eficient aceste provocări, trebuie dezvoltate intervenții specifice pentru a stabili un ecosistem de securitate cibernetică care să fie atât rezilient la amenințările externe, cât și durabil pe termen lung.
89. Impactul implementării măsurilor propuse va fi reflectat prin îmbunătățirea poziției Republicii Moldova în Indicele global de securitate cibernetică (GCI) al Uniunii Internaționale a Telecomunicațiilor (UIT), prin creșterea de la locul 63 în anul 2024 la locul 55 în anul 2028 și locul 50 în anul 2030.

Capitolul V

COSTURI

90. Implementarea Programului 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

permise de legislație.

91. În urma evaluării costurilor, cheltuielile necesare pentru realizarea acțiunilor planificate sunt estimate la circa 79,9 milioane lei. Dezagregarea pe obiective specifice și ani este prezentată în *Tabelul 2. Costuri pentru implementarea Programului*.
92. Deși o parte considerabilă 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 demers va contribui la diminuarea presiunii asupra bugetului național.
93. 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”

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**
Obiectivul specific 1.1		**10347,27**	4756,6	2120,87	1156,6	1156,6	1156,6
Costuri acoperite în CBTM (mii lei)	**1504**	**1789,2**	**304,4**	**571,6**	**304,4**	**304,4**	**304,4**
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-
Costuri neacoperite (mii lei)		**8558,07**	**4452,2**	**1549,27**	**852,2**	**852,2**	**852,2**
Obiectivul specific 1.2		**43502,04**	**21354,37**	**15013,97**	**7000,1**	**66,8**	**66,8**

Costuri acoperite în CBTM (mii lei)	**1504**	**1128,14**	**514,27**	**613,87**	**-**	**-**	**-**
Costuri asistență externă (mii lei)		**8940**	**8940**	**-**	**-**	**-**	**-**
Costuri neacoperite (mii lei)		**33433,9**	**11900,1**	**14400,1**	**7000,1**	**66,8**	**66,8**
Obiectivul specific 1.3		**4917,29**	960	1077,29	960	960	960
Costuri acoperite în CBTM (mii lei)	**5001**	**117,29**	-	-	-	-	-
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-
Costuri neacoperite (mii lei)		**4800**	960	960	960	960	960
Obiectivul specific 2.1		**2053,74**	467,29	234,58	1117,29	117,29	117,29
Costuri acoperite în CBTM (mii lei)	**1504**	**117,29**	**-**	**117,29**	**-**	**-**	**-**
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-
Costuri neacoperite (mii lei)		**1936,45**	**467,29**	**117,29**	**1117,29**	**117,29**	**117,29**
Obiectivul specific 2.2		**189,0**	-	189,0	-	-	-
Costuri acoperite în CBTM (mii lei)		**-**	-	-	-	-	-
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-
Costuri neacoperite (mii lei)		**189**	-	189	-	-	-

Obiectivul specific 3.1		**4924,64**	967,7	1143,84	937,7	937,7	937,7
Costuri acoperite în CBTM (mii lei)		**-**	-	-	-	-	-
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-
Costuri neacoperite (mii lei)		**4924,64**	967,7	1143,84	937,7	937,7	937,7
Obiectivul specific 3.2		**2822,15**	566,8	520	735,35	500	500
Costuri acoperite în CBTM (mii lei)	**1504**	**86,8**	66,8	20	-	-	-
Costuri asistență 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 CBTM (mii lei)		**-**	-	-	-	-	-
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-
Costuri neacoperite (mii lei)		**1765,0**	353,0	353,0	353,0	353,0	353,0
Obiectivul specific 3.4		**1859,08**	523,08	334,0	334,0	334,0	334,0
Costuri acoperite în CBTM (mii lei)		**189,08**	189,08	-	-	-	-
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-

Costuri neacoperite (mii lei)		**1670**	334	334	334	334	334
Obiectivul specific 4.1		**560,0**	80,0	240	80,0	80,0	80,0
Costuri acoperite în CBTM (mii lei)		**-**	-	-	-	-	-
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-
Costuri neacoperite (mii lei)		**560,0**	80,0	240	80,0	80,0	80,0
Obiectivul specific 4.2		**4634,58**	1114,58	880	880	880	880
Costuri acoperite în CBTM (mii lei)		**234,85**	234,85	-	-	-	-
Costuri asistență 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 CBTM (mii lei)		**117,29**	-	-	-	-	-
Costuri asistență externă (mii lei)		**-**	-	-	-	-	-
Costuri neacoperite (mii lei)		**2247**	**1781,56**	**166,46**	**99,66**	**99,66**	**99,66**
TOTAL		**79939,08**	**33042,27**	**22273,01**	**13653,7**	**5485,05**	**5485,05**
Costuri acoperite în CBTM (mii lei)		**3779,67**	**1426,42**	**1440,05**	**304,4**	**304,4**	**304,4**

Costuri asistență externă (mii lei)		**8940**	**8940**				
Costuri neacoperite (mii lei)		**67219,41**	**22675,85**	**20832,96**	**13349,3**	**5180,65**	**5180,65**

Capitolul VI

RISCURI DE IMPLEMENTARE

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

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

Tabelul 3. Descrierea riscurilor și a măsurilor de atenuare

Riscul	Impactul	Probabilitatea	Măsurile de diminuare a riscurilor
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.

Riscul	Impactul	Probabilitatea	Măsurile de diminuare a riscurilor
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; • Includerea acțiunilor prioritare în Planul Național de Dezvoltare
Capacitate administrativă limitată a autorităților și instituțiilor publice responsabile	Mediu	Mare	• Instruirea personalului; • Alocarea de resurse pentru consolidarea echipelor responsabile; • Implicarea experților din sectorul privat.
Nivel scăzut de conștientizare publică privind securitatea cibernetică	Mare	Mediu	• Campanii de informare naționale recurente; • Revizuirea metodelor de instruire a tinerilor și adulților în domeniul securității cibernetice; • Desemnarea unei autorități responsabile de coordonarea părții educaționale a programului.
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.

Riscul	Impactul	Probabilitatea	Măsurile de diminuare a riscurilor
Lipsa de angajament și sprijin din partea factorilor de decizie și a funcționarilor publici în implementarea Programului, inclusiv schimbarea de priorități 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 un plan de comunicare detaliată referitor la realizarea Programului, inclusiv pentru a obține sprijinul și interesul publicului.
Dependența de furnizori externi de soluții tehnologice	Mediu	Mediu	• Promovarea dezvoltării soluțiilor naționale; • Diversificarea parteneriatelor tehnologice, în mod special cu cele din Uniunea Europeană.

Capitolul VII

AUTORITĂȚI ȘI INSTITUȚII RESPONSABILE

94. Autoritățile și instituțiile publice cu competențe în realizarea politicii statului în domeniul securității cibernetice și combaterea criminalității cibernetice sunt responsabile de punerea în aplicare a Programului:

94.1 Ministerul Dezvoltării Economice și Digitalizării;

94.2 Ministerul Afacerilor Externe;

94.3 Ministerul Afacerilor Interne;

94.4 Ministerul Educației și Cercetării;

94.5 Procuratura Generală;

94.6 Agenția pentru Securitate Cibernetică;

94.7 Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică";

94.8 Instituţia Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor");

94.9 Inspectoratul General de Poliție;

94.10 Comisia Electorală Centrală;

94.11 Centrul Național pentru Protecția Datelor cu Caracter Personal;

94.12 Ministerul Energiei;

94.13 Ministerul Infrastructurii și Dezvoltării Regionale;

94.14 Alte autorități și instituții relevante.

Capitolul VIII

PROCEDURI DE MONITORIZARE, EVALUARE ŞI RAPORTARE

95. 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 implementarea Planului de acțiuni, în vederea determinării gradului de realizare a acțiunilor și a conformității acestora cu cele planificate. Un alt aspect important este identificarea și evaluarea deficiențelor în realizarea acțiunilor, cu înaintarea unor propuneri de remediere.
96. În procesul de implementare a Programului vor fi realizate următoarele proceduri de monitorizare și evaluare:
    95.1 **Monitorizarea semestrială** – proces continuu, realizat la fiecare 6 luni, care implică colectarea, analiza și interpretarea datelor referitoare la progresul activităților Programului, având scopul de a asigura conformitatea cu planul de acțiuni 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 pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării.
    95.2 **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 de progres anual privind implementarea Programului și a planului de acțiuni se întocmește de Secretariatul responsabil de monitorizarea Programului și se publică pe pagina web oficială a 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 pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării.

95.3 **Evaluarea finală** – se realizează în termen de 6 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 Secretariatul responsabil de monitorizarea Programului. Raportul final se publică pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării.

97. 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 acțiunilor incluse în planul de acțiuni al 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 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.
98. 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 Ministerul 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 implementarea acțiunilor, solicitând date, informații și analize relevante pentru monitorizarea și evaluarea gradului de implementare a Programului.
99. 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 implementarea acțiunilor planificate de care sunt responsabile, conform termenelor stabilite în planul de acțiuni.
100. Raportul de evaluare se prezintă spre validare Consiliului coordonator în domeniul securității cibernetice și va fi publicat pe pagina web oficială a Ministerului Dezvoltării Economice și Digitalizării.
101. 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.

Planul de acțiuni pentru implementarea Programului Național de Securitate Cibernetică pentru anii 2026-2030

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
Obiectivul general 1. Consolidarea capacităților operaționale														
Obiectivul specific 1.1. Consolidarea capacităților de răspuns la incidentele cibernetice al Agenției pentru Securitate Cibernetică														
1.1.1	Dezvoltarea Registrului de stat al incidentelor cibernetice și a sistemului informatic care îl formează.	Sistemul centralizat de raportare și schimb de informații este funcțional.	3600			3600	1504	3600					T4 2026	Agenția pentru Securitate Cibernetică
		Protocoalele standardizate de raportare sunt testate prin cel puțin un exercițiu anual	468	468			1504	93,6	93,6	93,6	93,6	93,6	2026 – 2030	Agenția pentru Securitate Cibernetică
1.1.2	Stabilirea proceselor și a unui sistem centralizat integrat pentru schimbul de informații între furnizorii de servicii din sectoarele critice.	Sistemul centralizat de schimb de informații este funcțional.	847,07	150.0		697,07	1504		847,07				T2 2027	Agenția pentru Securitate Cibernetică
		Protocoale standardizate pentru schimbul de informații pentru autoritățile publice și pentru furnizorii de servicii din sectoarele critice sunt adoptate.	117,2	117,2			1504		117,2				T2 2027	Agenția pentru Securitate Cibernetică

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
		Protocoale standardizate pentru schimbul de informații pentru autoritățile publice și pentru furnizorii de servicii din sectoarele critice testate prin cel puțin un exercițiu anual.	468	468			1504	93,6	93,6	93,6	93,6	93,6	2026 – 2030	Agenția pentru Securitate Cibernetică
1.1.3	Dezvoltarea și furnizarea de programe de instruire specializate pentru furnizorii de servicii în sectoarele critice privind instrumentele de raportare a incidentelor și de schimb 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”)
1.1.4	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 două exerciții la nivel sectorial /intersectorial organizate anual	4000			4000	1504	800	800	800	800	800	2026 – 2030	Agenția pentru Securitate Cibernetică Instituția publică “Serviciul de Tehnologie a

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														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 rapoartelor privind situația din spațiul cibernetic național, care vor cuprinde inclusiv analize dezagregate pe marginea grupurilor ce mai expuse (ex. elevi, persoane vârstnice, femei, mediul rural).	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 de Tehnologie a Informației și Securitate Cibernetică” Ministerul Dezvoltării Economice și Digitalizării
Obiectiv specific 1.2. Consolidarea rezilienței furnizorilor de servicii în sectoarele critice împotriva amenințărilor cibernetice și a incidentelor cibernetice.														

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
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 sectoarele critice și promovarea implementării standardelor naționale în domeniul securității informației și securității cibernetice de către furnizorii de servicii în sectoarele critice.													
		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				T2 2027	Agenția pentru Securitate Cibernetică
1.2.2	Instruirea furnizorilor de servicii din sectoarele critice din domeniul public 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	Studiu privind necesitățile sectoriale de formare/dezvoltare profesională în domeniul securității cibernetice sunt sistematizate în baza solicitărilor Anul 2026 - 30% de funcționari instruiți Anul 2027 - 50% 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

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
		Anul 2028 - 90% de funcționari instruiți												Cibernetică „Cybercor”) Ministerul Dezvoltării Economice și Digitalizării
1.2.3	Identificarea necesităților și promovarea certificării specialiștilor în securitatea cibernetică prin organizații specializate pentru a respecta standardele internaționale și programele de certificare profesională (ISACA[34], SANS[35], PECB[36] etc)	Studiu privind necesitățile sectoriale de formare/dezvoltare profesională în domeniul securității cibernetice sunt sistematizate în baza solicitărilor	66,8	66.8			1504		66,8				T4 2027	Agenția pentru Securitate Cibernetică Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”) Instituția publică “Serviciul de Tehnologie a Informației și

[34] Asociatia de Audit si Control a Sistemelor Informatice (Information Systems Audit and Control Association).

[35] Administrator de sistem, Audit, Rețea, Securitate (SysAdmin, Audit, Network, Security).

[36] Consiliul de Evaluare și Certificare Profesională (Professional Evaluation and Certification Board).

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														Securitate Cibernetică” Ministerul Dezvoltării Economice și Digitalizării Alte autorități și instituții relevante
		Cel puțin 20 de specialiști în securitate cibernetică certificați prin cursuri oferite în parteneriat cu organizații specializate	1000			1000	1504		1000				T 4 2027	Agenția pentru Securitate Cibernetică Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”) Instituția publică “Serviciul de Tehnologie a Informației și Securitate Cibernetică”

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														Ministerul Dezvoltării Economice și Digitalizării Alte autorități și instituții relevante
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.	80 % din efectivul limită al Agenției pentru Securitate Cibernetică angajați.	400			400		400					T4 2026	Agenția pentru Securitate Cibernetică
1.2.5	Crearea cadrului normativ privind securitatea cibernetică a rețelelor 5G	Studiul de analiză a impactului și a riscurilor de implementare a setului de instrumente de securitate cibernetică 5G al UE elaborat	8940		8940		Acord de Grant cu Swedfund (Ordin MDED 32/2025)	8940					T 2 2026	Ministerul Dezvoltării Economice și Digitalizării
		Cadrul normativ privind securitatea cibernetică a rețelelor 5G adoptat	207,99	207,99			5001		207,99				T1 2027	Ministerul Dezvoltării Economice și Digitalizării

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
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					T 4 2026	Ministerul Dezvoltării Economice și Digitalizării
1.2.7	Identificarea și desemnarea autorității sau instituției publice care va exercita rolul de centrul național de coordonare de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică	Centrul național de coordonare de competențe în domeniul industrial, tehnologic și de cercetare în materie de securitate cibernetică desemnat	189,08	189,08			5001	189,08					T 4 2026	Ministerul Dezvoltării Economice și Digitalizării
1.2.8	Elaborarea proiectului de Hotărâre de Guvern cu privire la 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 de Guvern adoptat	117,2	117,2			5001	117,2					T2 2026	Ministerul Dezvoltării Economice și Digitalizării
1.2.9	O platformă informatică centralizată de raportare și gestionare a vulnerabilităților cibernetice, accesibilă	Platforma implementatăși funcțională, cu cel puțin 90% dintre furnizorii de servicii identificați conectați și utilizând platforma pentru	1800			1800	1504	1800					T4 2026	Agenția pentru Securitate Cibernetică

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
	furnizorilor de servicii din sectoarele critice	raportarea vulnerabilităților												
1.2.10	Integrarea furnizorilor de servicii din sectoarele critice în cadrul SOC-ului național pentru asigurarea monitorizării și răspunsului coordonat la incidentele cibernetice.	Cel puțin 50 furnizorii de servicii integrați pe platforma	1000			1000	1504		1000				T3 2027	Agenția pentru Securitate Cibernetică
1.2.11	Implementarea unei soluții de protectie DDOS si WAF pentru furnizorii de servicii din sectoarele critice	Cel puțin 50 furnizorii de servicii integrați pe platforma	5400			5400	1504		5400				T1 2027	Agenția pentru Securitate Cibernetică
1.2.12	Implementarea unei soluții integrate de tip EDR pentru asigurarea protecției cibernetice a furnizorilor de servicii din sectoarele critice	Cel puțin 800 dispozitive protejate	2700			2700	1504	2700					T3 2026	Agenția pentru Securitate Cibernetică
1.2.13	Elaborarea și promovarea cadrului normativ secundar în vederea evaluării conformității mijloacelor de protecție criptografică și a semnăturilor electronice și	Cadrul normativ aprobat	189,08	189,08					189,08				T2 2027	Serviciul de Informații și Securitate Ministerul Dezvoltării

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
	certificarea produselor criptografice în conformitate cu normele UE													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.[37]	Cadrul normativ aprobat	117,29	117,29			5001		117,29				T4 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 3 exerciții comune de răspuns la crize cibernetice desfășurate cu părțile interesate trans sectoriale anual	4000			4000		800	800	800	800	800	2026-2030	Centrul pentru Comunicare Strategică și Combatere a Dezinformării

[37] RECOMANDAREA (UE) 2017/1584 A COMISIEI din 13 septembrie 2017 privind răspunsul coordonat la incidentele și crizele de securitate cibernetică de mare amploare https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32017H1584&qid=1731591042578

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														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

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
		Cel puțin 2 instruiri în comunicarea strategică pentru gestionarea crizelor cibernetice și/sau atacurilor hibride	800			800		160	160	160	160	160	Anual	Centrul pentru Comunicare Strategică și Combatere 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

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														Ministerul Sănătății Alte autorități publice relevante
Obiectivul general 2. Consolidarea rezilienței țării împotriva criminalității informatice														
Obiectivul specific 2.1. Consolidarea competențelor și abilităților ale entităților de aplicare a legii în ceea ce privește investigarea infracțiunilor informatice și infracțiunilor în domeniul comunicațiilor electronice														
2.1.1	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.	Mecanism de schimb de informații și de coordonare între autoritățile publice instituit și funcțional	117,29	117,29			1504	117,29					T 4 2026	Ministerul Afacerilor Interne (Inspectoratul General de Poliție) Procuratura Generală Agenția pentru Securitate Cibernetică

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														Instituția publică "Serviciul de Tehnologie a Informației și Securitate Cibernetică"
2.1.2	Investiții continue în competențele și abilitățile digitale ale autorităților de aplicare a legii, inclusiv în capacitățile și competențele criminalistice digitale și în noi metode de investigare a criminalității informatice și a infracțiunilor conexe	Cel puțin 20 de profesioniști în securitate cibernetică certificați în domeniul aplicării legii și criminalisticii digitale	1000			1000				1000			T 4 2028	Ministerul Afacerilor Interne (Inspectoratul General de Poliție) Procuratura Generală
2.1.3	Promovarea și dezvoltarea formatelor de cooperare și colaborare între autoritățile și instituțiile publice și sectorul privat pentru schimbul eficient de informații, inclusiv prin stabilirea de parteneriate, în particular prin consolidarea interacțiunii cu sectorul telecomunicațiilor, cu furnizorii de servicii de internet și cu operatorii obiectivelor de infrastructură critică pentru	Stabilirea a cel puțin 2 parteneriate anual	586,45			586,45		117,29	117,29	117,29	117,29	117,29	2026-2030	Ministerul Afacerilor Interne (Inspectoratul General de Poliție)

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
	a îmbunătăți detectarea și raportarea amenințărilor și incidentelor cibernetice și a vulnerabilităților serviciilor și produselor de tehnologie a informației.													
2.1.4	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 2 acțiuni/campanii de informare a populației	250			250		250					T 1 2026	Ministerul Afacerilor Interne (Inspectoratul General de Poliție)
2.1.5	Informarea populației cu privire la operaționalizarea instrumentului/platformei online de raportare a infracțiunilor informatice	Cel puțin o campanie de informare realizată	100			100		100					T 4 2026	Ministerul Afacerilor Interne (Inspectoratul General de Poliție)
Obiectivul specific 2.2. Crearea de instrumente tehnologice eficace și avansate pentru prevenirea, detectarea și investigarea eficientă a criminalității informatice														
2.2.1	Reacreditarea Laboratorului de expertiză criminalistică în domeniul cibernetic	Laboratorul de expertiză criminalistică în domeniul cibernetic reacreditat	189			189			189				T 4 2027	Ministerul Afacerilor Interne (Inspectoratul General al Poliției);

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
Obiectivul general 3. Dezvoltarea competențelor și a culturii de securitate cibernetică în societate														
Obiectivul specific 3.1. Dezvoltarea unei forțe 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 programe de recalificare și perfecționare 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 femeilor pentru a încuraja participarea lor la industria digitală și la cursuri de formare.	Program de formare continuă elaborate și disponibile pentru diferite grupuri țintă	20,0			20,0		20,0					T 4 2026	Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”) Ministerul Educației și Cercetării Instituția publică “Agenția de Guvernare Electronică”
		Cel puțin 100 persoane instruite, dintre care cel puțin 45 de sex feminin anual	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”)

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
3.1.2	Diversificarea mecanismelor de finanțare a învățării și educației adulților în domeniul securității cibernetice.	Cel puțin 2 granturi acordate anual OSC-urilor/ONG-urilor 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 autoritățile responsabile de aplicarea legii (inclusiv sectorul vamal și judiciar).	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 (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	Mecanism de certificare a calificărilor elaborate	117,29			117,29			117,29				T 1 2027	Ministerul Educației și Cercetării Instituția Publică Universitatea

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
	comunicațiilor și dezvoltarea de programe complexe de formare a profesorilor și oportunități de burse pentru îmbunătățirea și diversificarea abilităților de predare.													Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”)
		Program de formare a cadrelor didactice stabilite, inclusiv prin metode participative, instrumente digitale etc elaborate.	20,0			20,0			20,0				T 1 2027	Ministerul Educației și Cercetării
		Cel puțin 10 formatori au încheiat cursurile de formare a formatorilor și fac parte din grupul de formatori	48,85			48,85			48,85				T 3 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 pentru elevii STEAM este actualizat	10,0			10,0		10,0					T 3 2026	Ministerul Educației și Cercetării Instituția Publică Universitatea Tehnică a Moldovei (Institutul Național de

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														Inovații în Securitatea Cibernetică „Cybercor”)
3.1.6	Dezvoltarea pedagogiei digitale și a materialelor didactice relevante și inovatoare pentru a promova și stimula dobândirea și practicarea competențelor STEAM	Materiale didactice inovatoare dezvoltate	20,0			20,0			20,0				T 2 2027	Ministerul Educației și Cercetării
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.	Cel puțin 3 campanii de conștientizare a publicului organizate anual	2 504			2504		500,8	500,8	500,8	500,8	500,8	2026-2030	Serviciul de Informații și Securitate Instituția publică “Agenția de Guvernare Electronică” Instituția publică “Serviciul de Tehnologie a Informației și Securitate Cibernetică” Ministerul Dezvoltării Economice și Digitalizării

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
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 de către persoanele fizice și întreprinderi	Sondaje anual efectuate	2500			2500		500	500	500	500	500	2026-2030	Agenția pentru Securitate Cibernetică Ministerul Dezvoltării Economice și Digitalizării 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.	Nevoile sectoriale de formare sunt definite și coordonate	66,8	66,8			1504	66,8					T 3 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				T 1 2027	Agenția pentru

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														Securitate Cibernetică Instituția Publică Universitatea Tehnică a Moldovei (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	50 de formatori au încheiat cursurile de formare a formatorilor și fac parte din grupul de formatori	235,35			235,35				235,35			T 2 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 radiodifuzori, distribuitori de servicii media, formatori de opinie	Cel puțin 3 instruiri desfășurate și ghiduri distribuite radiodifuzorilor, distribuitorilor de servicii media, formatori de opinie	1765			1765		353	353	353	353	353	2026-2030	Centrul pentru Comunicare Strategică și

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
	publică, jurnaliști și organizații neguvernamentale privind tehnicile de dezinformare și/sau manipulare a informațiilor utilizate pentru a afecta securitatea informațională a statului	publică, jurnaliști și organizații neguvernamentale anual												Combatere a Dezinformării Serviciul de Informații și Securitate Consiliul Audiovizualului
Obiectivul specific 3.4. Protejarea drepturilor și libertăților persoanelor atunci când datele lor cu caracter personal sunt prelucrate														
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, inclusiv datele cu caracter personal.	Aprobarea de acte administrative comune pentru reglementarea procedurilor operaționale de cooperare	189,08	189,08			1504	189,08					T 4 2026	Agenția pentru Securitate Cibernetică Centrul Național pentru Protecția Datelor 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 2 campanii comune de promovare a conștientizării igienei cibernetice, a confidențialității și a protecției datelor desfășurate organizate anual	1 670,0			1670		334	334	334	334	334	2026-2030	Agenția pentru Securitate Cibernetică Centrul Național pentru Protecția Datelor cu Caracter Personal

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
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 UE														
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 (ENISA) și cu autoritățile competente în domeniul securității cibernetice din țările învecinate și din țările din afara Uniunii Europene	Cel puțin 2 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 de Poliție) Agenția pentru Securitate Cibernetică Instituția publică "Serviciul de Tehnologie a Informației și Securitate Cibernetică"
4.1.2	Integrarea cu rețeaua echipelor de răspuns la incidente de securitate informatică (CSIRT) a UE, echipele de răspuns la situații de urgență cibernetică (CERT) și sistemele de alertă timpurie.	Cel puțin 2 participări la grupuri operative comune și alte formate de cooperare	160			160			160				T4 2027	Agenția de Securitate Cibernetică
Obiectivul specific 4.2 Dezvoltarea platformelor de comunicare strategică externă pentru asigurarea securității informaționale și promovarea intereselor naționale ale Republicii Moldova														

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
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	Planul național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice aprobat	117,29	117,29			1504	117,29					T 2 2026	Agenția de Securitate Cibernetică
		Politici de comunicare strategică aprobate	117,29	117,29			1504	117,29					T 4 2026	Ministerul Afacerilor Interne (Inspectoratul General de Poliție) Centrul pentru Comunicare Strategică și Combatere a Dezinformării Ministerul Apărării Serviciul de Informații și Securitate
4.2.2	Îmbunătățirea răspunsului la crizele cibernetice prin asigurarea unei abordări coordonate	Cel puțin 2 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

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
														"Serviciul de Tehnologie a 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					T2 2026	Ministerul Afacerilor Externe
		Personalul unității de diplomație cibernetică angajat	1 681,9			1 681,9		1 681,9					T4 2026	Ministerul Afacerilor Externe
4.3.2	Oferirea de instruire specializată în diplomație cibernetică pentru personalul Ministerului Afacerilor	Cel puțin o instruire a personalului relevant al Ministerului Afacerilor Externe, al ambasadelor și	231,1			231,1		46,22	46,22	46,22	46,22	46,22	2026-2030	Ministerul Afacerilor Externe

N/o	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 repatizate pe ani (mii lei)					Termenul limită (trimestru/an)	Instituție responsabilă
				Buget de stat	Asistență externă	Costuri neacoperite		2026	2027	2028	2029	2030		
	Externe, ambasadelor și misiunilor permanente	al misiunilor permanente organizată anual												
4.3.3	Participarea la setul de instrumente pentru diplomație cibernetică al UE	Republica Moldova are acordat statutul de asociat sau observator în setul de instrumente pentru diplomație cibernetică al UE	66,8			66,8			66,8				T3 2027	Ministerul Afacerilor Externe
4.3.4	Negocierea acordurilor bilaterale sau regionale de cooperare cibernetică cu aliații strategici	Cel puțin 1 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	Ministerul Afacerilor Externe

NOTA DE FUNDAMENTARE

la proiectul Hotărîrii Guvernului cu privire la aprobarea proiectului Hotărîrii Parlamentului pentru 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 proiectului Hotărîrii Parlamentului pentru 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 proiectului Hotărîrii Parlamentului pentru 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 implemntarea 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 de apărare națională 2024–2034, aprobată prin Hotărârea Parlamentului nr. 319/2024;
- Strategia de dezvoltare "Educația 2030", 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.

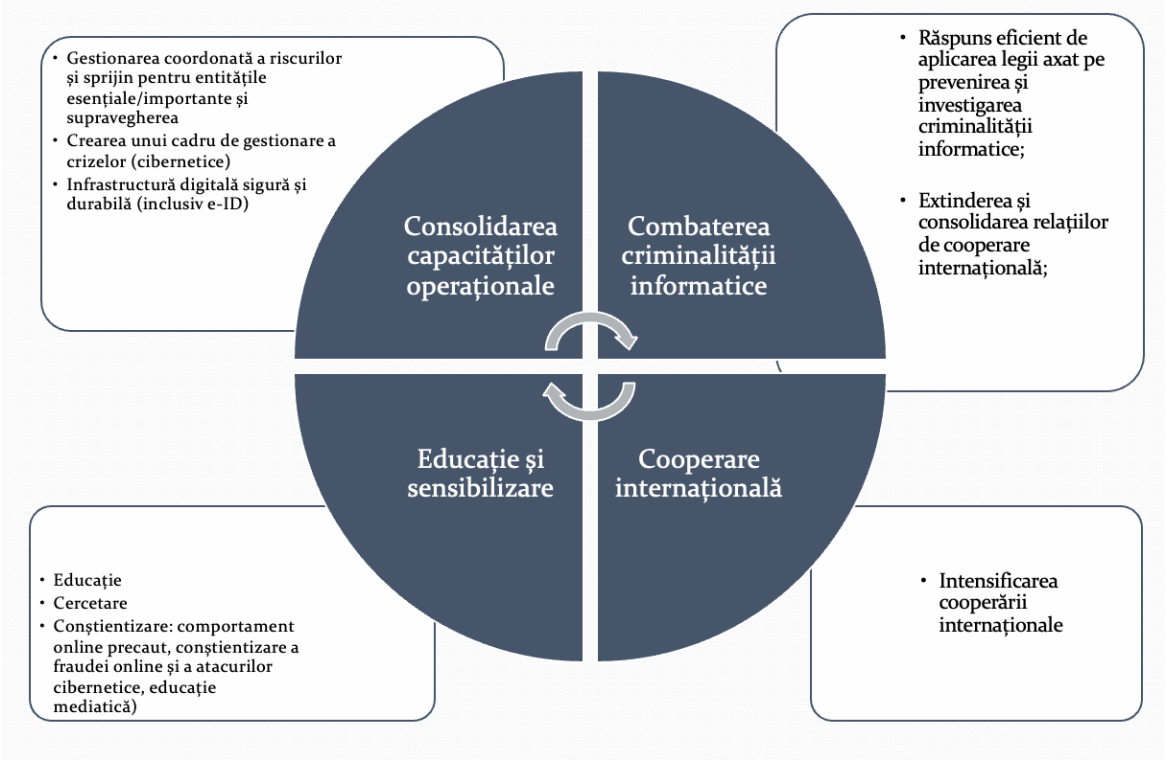
Sectorul TIC contribuie semnificativ la PIB, însă lipsa cadrelor calificate și investițiile reduse în cercetare și educație au impact asupra rezilienței digitale. Totodată, Strategia de securitate națională subliniază vulnerabilitatea țării la atacuri cibernetice și riscuri hibride, inclusiv dezinformare. 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”, Strategia de dezvoltare a domeniului afacerilor interne 2022–2030, Strategia națională de apărare 2024–2034, Programul de prevenire și combatere a criminalității 2022–2025 (și proiectul pentru perioada 2026–2030) și Programul național de aderare a Republicii Moldova la UE 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	Creșterea numărului de cauze cu privire la infracțiunile informatice şi infracțiunile în domeniul comunicaţiilor electronice remise în judecată *Sursa: Ministerul Afacerilor Interne*	N/A	Creșterea cu 15%	Creșterea cu 30%
	2.2. Crearea de instrumente tehnologice eficace și avansate pentru prevenirea, detectarea și investigarea eficientă a criminalității informatice	Dotarea cu instrumente și soluții inteligente de investigare *Sursa: Ministerul Afacerilor Interne*	8 instrumente (2024)	Minim 9 instrumente	Creștere cu 25% (minim 10 soluții)

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 un partener de încredere în	4.1 Consolidarea cooperării internaționale prin integrarea Republicii	Creșterea scorului de țară la capitolul "măsuri de cooperare"	15,51 (2024)	16,5	18,5

comunitatea internațională de aplicare a legii și securitate cibernetică	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 și 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 79,9 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".

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 calității și a conformității de către Cancelaria de Stat și Ministerul Finanțelor. 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.

7. Concluziile expertizelor

Proiectul va fi 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 **Natalia SELEVESTRU**

SINTEZA

obiecțiilor și propunerilor/recomandărilor la proiectul hotărârii Guvernului cu privire la aprobarea proiectului hotărîrii Parlamentului pentru 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 şi 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 şedinţei 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.**

Secretar de stat **Michelle ILIEV**

PROCESUL-VERBAL nr. 22

al ședinței Consiliului pentru coordonarea dezvoltării durabile din 10.11.2025

online, ora 15:00

Au participat:

Președinte al Consiliului	dna	Lilia DABIJA, secretar general adjunct al Guvernului
Membri ai Consiliului	dna	Angela Țurcanu, secretar general al Ministerului Infrastructurii și Dezvoltării Regionale
	dna	Dina Roșca, secretar general al Ministerului Finanțelor
	dl	Andrei Grițco, secretar general al Ministerului Energiei
	dna	Lilia Gantea, secretar general al Ministerului Sănătății
	dna	Viorica Grecu, secretar general al Ministerul Justiției
	dna	Galina Rusu, secretar general al Ministerului Educației și Cercetării
	dl	Petru Tătaru, secretar general al Ministerului Mediului
	dl	Sergiu Gherciu, secretar general al Ministerului Agriculturii și Industriei Alimentare
	dna	Ana Varzari, secretar general al Ministerului Culturii
	dl	Igor Cutie, secretar general al Ministerului Apărării
	dna	Ina Voicu, secretar general al Ministerului Dezvoltării Economice și Digitalizării
	dl	Andrei Cecoltan, secretar general adjunct al Ministerului Afacerilor Interne
	dl	Iurie Mocanu, director general adjunct al Biroului Național de Statistică
Invitați	dna	Carolina Novac, secretar de stat al Ministerului Energiei
	dl	Ion Gumene, secretar de stat al Ministerului Finanțelor
	dl	Viorel Pană, șef al Direcției investiții publice și finanțe în sectorul economic, Ministerul Finanțelor
	dl	Nicolae Olari, șef al Direcției eficiență energetică, Ministerul Energiei
	dl	Ivan Danii, director general, Agenția Geodezie, Cartografie și Cadastru
	dna	Irina Alexe, expert al Uniunii Europene în planificare strategică, Cabinetul Prim-ministrului
	dl	Dragoș Ciuparu, consilier de nivel înalt al Uniunii Europene, Cabinetul Prim-ministrului
	dna	Olesea Luchian, șef al Direcției administrație publică centrală
	dna	Rodica Nicoara, șef al Direcției planificare strategică, șef adjunct al Direcției generale planificare strategică și

coordonarea politicilor, Cancelaria de Stat

dna Doina Rusnac, consultant principal în Direcția planificare strategică din cadrul Direcției generale planificare strategică și coordonarea politicilor, Cancelaria de Stat

dna Marina Botea, consultant principal în Direcția planificare strategică din cadrul Direcției generale planificare strategică și coordonarea politicilor, Cancelaria de Stat

dna Natalia Pulbere, consultant principal în Direcția coordonarea asistenței externe și fonduri europene, Cancelaria de Stat

Ședința a fost prezidată de dna Lilia DABIJA, secretar general adjunct al Guvernului, președinte al Consiliului pentru coordonarea dezvoltării durabile.

Se acceptă propunerea Ministerului Energiei de a completa ordinea de zi cu subiectul „Referitor la examinarea propunerii de restructurare a proiectului „Eficiența energetică în Republica Moldova (MEEP)"".

Ordinea de zi:

1. Referitor la validarea conceptului Programului național privind învățarea limbii române pentru anii 2026-2029.

Raportor: Galina Rusu – secretar general al Ministerului Educației și Cercetării

2. Referitor la validarea conceptului Programului de implementare a Strategiei naționale pentru cultură și patrimoniu pentru anii 2025-2030.

Raportor: Ana Varzari – secretar general al Ministerului Culturii

3. Referitor la examinarea proiectului Programului național de dezvoltare a turismului „Turism 2028".

Raportor: Ana Varzari – secretar general al Ministerului Culturii

4. Referitor la validarea conceptului Programului de dezvoltare a sectorului serviciilor energetice pentru perioada 2026-2030.

Raportor: Carolina Novac – secretar de stat al Ministerului Energiei

5. Referitor la examinarea proiectului Programului național de securitate cibernetică pentru anii 2026-2030.

Raportor: Ina Voicu – secretar general al Ministerului Dezvoltării Economice și Digitalizării

6. Referitor la examinarea proiectului Programului de dezvoltare a infrastructurii naționale de date spațiale pentru perioada 2026-2030.

Raportor: Ivan Danii – director general al Agenției Geodezie, Cartografie și Cadastru

7. Referitor la Raportul de monitorizare privind progresul în realizarea Planului național de reglementări pentru anul 2025.

Raportor: Lilia Dabija – secretar general adjunct al Guvernului

8. Referitor la examinarea propunerii de restructurare a proiectului „Eficiența energetică în Republica Moldova (MEEP)".

Raportor: Carolina Novac – secretar de stat al Ministerului Energiei

Ca urmare a discuțiilor, s-a decis:

1. Referitor la validarea conceptului Programului național privind învățarea limbii române pentru anii 2026-2029:

i. Se validează conceptul Programului național privind învățarea limbii române pentru anii 2026-2029.

ii. La elaborarea proiectului Programului, Ministerul Educației și Cercetării va respecta prevederile Regulamentului cu privire la planificarea strategică, aprobat prin Hotărârea Guvernului nr. 386/2020.

2. Referitor la validarea conceptului Programului de implementare a Strategiei naționale pentru cultură și patrimoniu pentru anii 2025-2030:

i. Se validează conceptul Programului de implementare a Strategiei naționale pentru cultură și patrimoniu pentru anii 2025-2030.

ii. Conform solicitării Ministerului Agriculturii și Industriei Alimentare, Ministerul Culturii va remite dosarul conceptului Programului.

iii. La elaborarea proiectului Programului, Ministerul Culturii va respecta prevederile Regulamentului cu privire la planificarea strategică, aprobat prin Hotărârea Guvernului nr. 386/2020.

3. Referitor la examinarea proiectului Programului național de dezvoltare a turismului „Turism 2028":

i. Se validează proiectul Programului național de dezvoltare a turismului „Turism 2028".

ii. Până la prezentarea proiectului pentru înregistrare și examinare în cadrul

ședinței secretarilor generali ai ministerelor, Ministerul Culturii va asigura:

- definitivarea proiectului în conformitate cu obiecțiile și recomandările din Raportul de evaluare a calității și conformității transmis de Cancelaria de Stat, precum și prin prisma avizului Ministerului Finanțelor;
- obținerea avizului privind evaluarea strategică de mediu de la Ministerul Mediului în conformitate cu cadrul normativ în vigoare.

iii. Ministerul Culturii va promova proiectul în strictă conformitate cu prevederile Hotărârii Guvernului nr. 386/2020 cu privire la planificarea strategică și ale Legii nr. 100/2017 cu privire la actele normative.

4. Referitor la validarea conceptului Programului de dezvoltare a sectorului serviciilor energetice pentru perioada 2026-2030:

i. Se validează conceptul Programului de dezvoltare a sectorului serviciilor energetice pentru perioada 2026-2030.

ii. Ministerul Energiei va ține cont de toate recomandările incluse în Raportul de evaluare a proiectului conceptului elaborat de Cancelaria de Stat, urmând ca versiunea revizuită a conceptului să fie plasată pe pagina web oficială a instituției, în conformitate cu cadrul normativ în vigoare.

iii. La elaborarea proiectului Programului, Ministerul Energiei va respecta prevederile Regulamentului cu privire la planificarea strategică, aprobat prin Hotărârea Guvernului nr. 386/2020.

5. Referitor la examinarea proiectului Programului național de securitate cibernetică pentru anii 2026-2030:

i. Se validează proiectul Programului național de securitate cibernetică pentru anii 2026-2030.

ii. Până la prezentarea proiectului pentru înregistrare și examinare în cadrul ședinței secretarilor generali ai ministerelor, Ministerul Dezvoltării Economice și Digitalizării:

- 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”*;
- 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;

- va include Ministerul Energiei în lista autorităților și instituțiilor responsabile la punctul 94 al proiectului Programului, conform solicitării acestuia.

iii. Ministerul Dezvoltării Economice și Digitalizării va asigura promovarea proiectului în strictă conformitate cu prevederile Hotărârii Guvernului nr. 386/2020 cu privire la planificarea strategică și ale Legii nr. 100/2017 cu privire la actele normative.

6. Referitor la examinarea proiectului Programului de dezvoltare a infrastructurii naționale de date spațiale pentru perioada 2026-2030:

i. Se validează proiectul Programului de dezvoltare a infrastructurii naționale de date spațiale pentru perioada 2026-2030.

ii. Agenția Geodezie, Cartografie și Cadastru va asigura promovarea proiectului în strictă conformitate cu prevederile Hotărârii Guvernului nr. 386/2020 cu privire la planificarea strategică și ale Legii nr. 100/2017 cu privire la actele normative

7. Referitor la Raportul de monitorizare privind progresul în realizarea Planului național de reglementări pentru anul 2025:

i. Se validează Raportul de monitorizare privind progresul în realizarea Planului național de reglementări pentru anul 2025 (PNR 2025), aferent situației din 4 noiembrie 2025;

ii. Autoritățile publice centrale vor asigura monitorizarea continuă a PNR 2025 și vor depune toate eforturile necesare pentru a crește gradul de realizare a acțiunilor planificate.

8. Referitor la examinarea propunerii de restructurare a proiectului „Eficiența energetică în Republica Moldova (MEEP)”:

Se acceptă prezentarea propunerii de restructurare a proiectului „Eficiența energetică în Republica Moldova (MEEP)” spre examinare în următoarea ședință a Comitetului interministerial pentru planificare strategică.

Secretar general adjunct al Guvernului /semnat electronic/ **Lilia DABIJA**

Ministerul Dezvoltării
Economice și Digitalizării
al Republicii Moldova

Nr. 13/2-3211 din 12.11.2025

Cancelaria de Stat

În temeiul pct. 63.16 al Regulamentului cu privire planificarea strategică, aprobat prin Hotărârea Guvernului nr. 386/2020 cu privire la planificarea strategică, remitem pentru înregistrare și examinare în cadrul ședinței secretarilor generali ai ministerelor *proiectul Hotărîrii Guvernului cu privire la aprobarea proiectului Hotărîrii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030*.

Totodată, avînd în vedere că proiectul menționat este inclus în documentele strategice ale Republicii Moldova, și anume *Agenda de reforme aferente Planului de creștere al Republicii Moldova pentru anii 2025–2027* (aprobat prin Hotărârea Guvernului nr. 260/2025) și *Foaia de parcurs privind „Statul de drept”,* care constituie un criteriu de referință în procesul de aderare a Republicii Moldova la Uniunea Europeană (aprobată prin Hotărârea Guvernului nr. 275/2025), având termen de realizare anul 2025, solicităm respectuos includerea a acestuia, în regim de urgență, pe agenda **ședinței secretarilor generali**.

În acest sens, în temeiul prevederilor pct. 38 și 185 din Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, se transmite cererea privind înregistrarea în lista proiectelor care urmează a fi examinate în cadrul ședinței secretarilor generali a proiectului sus-menționat.

CERERE

privind înregistrarea de către Cancelaria de Stat
a proiectelor de acte ale Guvernului

Nr. crt.	Criterii de înregistrare	Nota autorului
1.	Categoria și denumirea proiectului	Proiectul hotărârii Guvernului cu privire la aprobarea proiectului Hotărîrii Parlamentului pentru aprobarea Programului național de securitate cibernetică pentru anii 2026-2030.
2.	Autoritatea care a elaborat proiectul	Proiectul este elaborat de către Ministerul Dezvoltării Economiei și Digitalizării cu suportul partenerilor de dezvoltare.

3.	Justificarea depunerii cererii	Proiectul este elaborat în conformitate cu prevederile art. 6 alin. (3) al Legii nr. 48/2023 privind securitatea cibernetică și își propune să contribuie la realizarea obiectivelor și direcțiilor prioritare stabilite în documentele de politici publice de nivel superior.
4.	Referința la documentul de planificare care prevede elaborarea proiectului *(PNA, PND, PNR, alte documente de planificare sectoriale)*	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”.
5.	Lista autorităților și instituțiilor a căror avizare este necesară	1. Cancelaria de Stat 2. Ministerul Afacerilor Externe 3. Ministerul Afacerilor Interne 4. Ministerul Educației și Cercetării 5. Ministerul Apărării 6. Ministerul Sănătății 7. Ministerul Finanțelor 8. Ministerul Justiției 9. Ministerul Energiei 10. Ministerul Infrastructurii și Dezvoltării Regionale 11. Procuratura Generală 12. Agenția pentru Securitate Cibernetică 13. Aparatul Președintelui Republicii Moldova 14. Centrul Național de Management al Crizelor 15. Serviciul Tehnologia Informației și Securitate Cibernetică 16. Instituţia Publică Universitatea Tehnică a Moldovei (Institutul Național de Inovații în Securitatea Cibernetică „Cybercor”) 17. Comisia Electorală Centrală 18. Serviciul de Informații și Securitate 19. Centrul Național pentru Protecția Datelor cu Caracter Personal

		20. Institutul de Standardizare din Moldova 21. Centrul pentru Comunicare Strategică și Combatere a Dezinformării 22. Agenția de Guvernare Electronică 23. Biroul Național de Statistică 24. Consiliul Audiovizualului 25. Centrul Național Anticorupție – *expertiza anticorupție*
6.	Termenul-limită pentru depunerea avizelor/expertizelor	5 zile lucrătoare
7.	Persoana responsabilă de promovarea proiectului	Veronica Duda, consultant principal al Secției politici în domeniul securității cibernetice, Direcția politici în domeniul tehnologiei informației și digitalizării tel.: 022 250-557 e-mail: veronica.duda@mded.gov.md
8.	Anexe	1. Proiectul de Hotărâre 2. Nota de Fundamentare 3. Sinteza obiecțiilor și propunerilor/recomandărilor ale examinării prealabile de către Cancelaria de Stat și Ministerul Finanțelor, precum și urmare a examinării CCDD.
9.	Data și ora depunerii cererii	
10.	Semnătura	

Secretar de stat **Natalia SELEVESTRU**