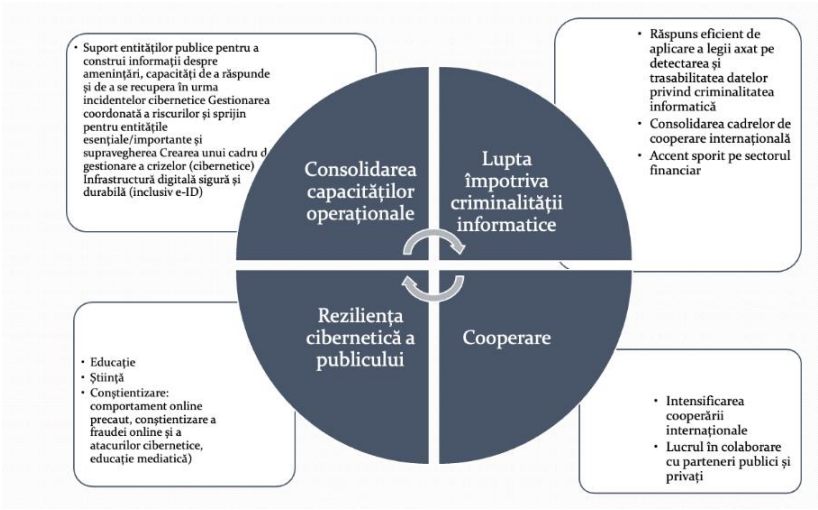
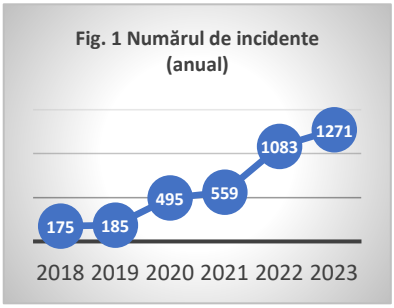
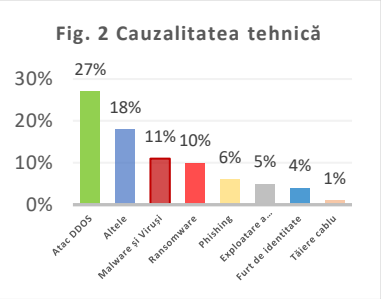
Conceptul

Programului național de securitate cibernetică pentru 2026-2030

Prezentul Concept este elaborat de Ministerul Dezvoltării Economice și Digitalizării în conformitate cu prevederile art. 6 alin. (3) din Legea nr. 48/2023 privind securitatea cibernetică și punctul 16 din Hotărârea Guvernului nr. 386/2020 privind planificarea strategică.

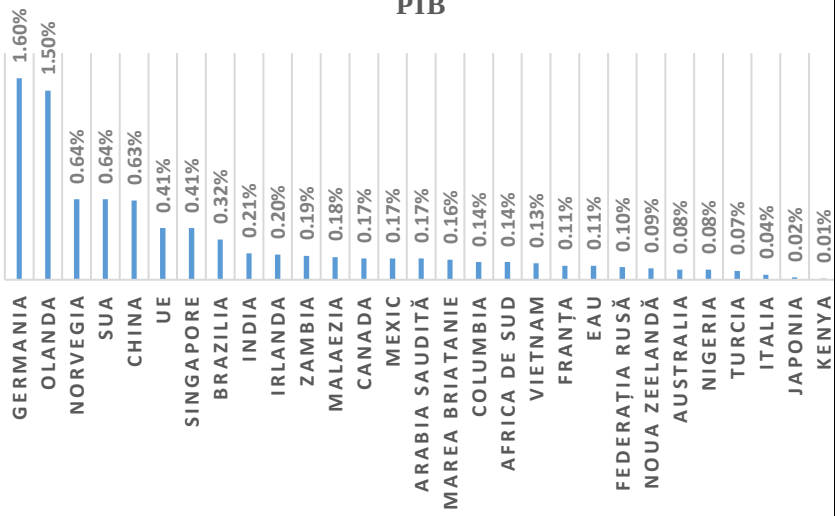
Structura și informația despre noul document de politici publice propus	
1. Denumirea documentului	Programului național de securitate cibernetică pentru anii 2026-2030
2. Tipul documentului de politici publice care se propune a fi elaborat și perioada planificată de implementare	Documentul de politici publice propus spre elaborare constituie un Program, care derivă din Strategia securității naționale a Republicii Moldova și Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030. Acest document de politici urmează a fi corelat cu Strategia de dezvoltare a domeniului afacerilor interne pentru anii 2022-2030. Atât Programul, cât și Planul de acțiuni, ca parte componentă a acestui program, urmează a fi elaborate în conformitate cu prevederile Legii nr.48/2023 privind securitatea cibernetică, ale Legii nr.100/2017 privind actele normative și ale Hotărârii Guvernului nr. 386/2020 privind planificarea strategică. Domeniile principale de intervenție: 1. Consolidarea capacităților operaționale; 2. Lupta împotriva criminalității informatice; 3. Reziliența cibernetică a societății; 4. Cooperarea internațională și națională.  Luând în considerare opinia Cancelariei de Stat, comunicată prin scrisoarea nr. 21/1-78-13196 din 02.12.2024, corelată cu cadrul normativ național privind planificarea strategică, aprobat prin

	Hotărârea Guvernului nr. 386/2020, documentul de politici publice urmează să fie aprobat de Parlament, la propunerea Guvernului.
3. Problemele din domeniu/subdomeniu care vor fi abordate în documentul de politici publice	În perioada 2018-2024, statele membre ale Uniunii Europene au raportat un total de 3251 de incidente cibernetice cu impact semnificativ[1], conform criteriilor stabilite de Directiva NIS1, Codul european al comunicațiilor electronice și Regulamentul eIDAS. Dintre acestea, 29% au fost considerate acțiuni rău intenționate. Cel mai afectat sector a fost cel privat, în special domeniile comunicațiilor, bancar, sănătate, servicii de încredere, transport și energie. În plus, datele indică o tendință generală de creștere a numărului de incidente cu impact semnificativ, conform ilustrării din *Figura 1*. Din cele 1230 de incidente rău intenționate raportate, majoritatea au fost clasificate drept infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în *Figura 2*.   Conform raportului *IBM Cost of a Data Breach*[2] actualizat pentru anul 2024, impactul financiar al încălcării datelor este și mai mare pentru entitățile critice. Raportul indică faptul că, în 2024, costul mediu global al unei încălcări de date a atins un nivel record de 4,88 milioane de dolari americani, marcând o creștere de 10% față de 2023.

[1] https://ciras.enisa.europa.eu/ciras-consolidated-reporting
[2] https://www.ibm.com/reports/data-breach

De asemenea, sunt importante constatările studiului global realizat de compania McAfee[3], care a evaluat pierderile economice cauzate de criminalitatea cibernetică. Acest studiu, intitulat *Net Losses: Estimating the Global Cost of Cybercrime*,

Fig. 3. Criminalitatea informatică ca procent din PIB



furnizează o estimare a impactului economic al infracțiunilor informatice pentru diferite țări, exprimate ca procent din PIB. Graficul prezentat în *Figura 3* evidențiază țările cel mai grav afectate în funcție de proporția prejudiciului monetizat în raport cu PIB-ul lor. În medie, pierderile cauzate de infracțiunile cibernetice reprezintă aproximativ 0,3% din PIB. Extrapolând aceste date pentru Republica Moldova, având în vedere că produsul intern brut al acesteia a fost de aproximativ 16,5 miliarde de dolari SUA în 2023, se poate estima un prejudiciu potențial anual de aproximativ 49 de milioane de dolari, bazat pe media de 0,3% din PIB.

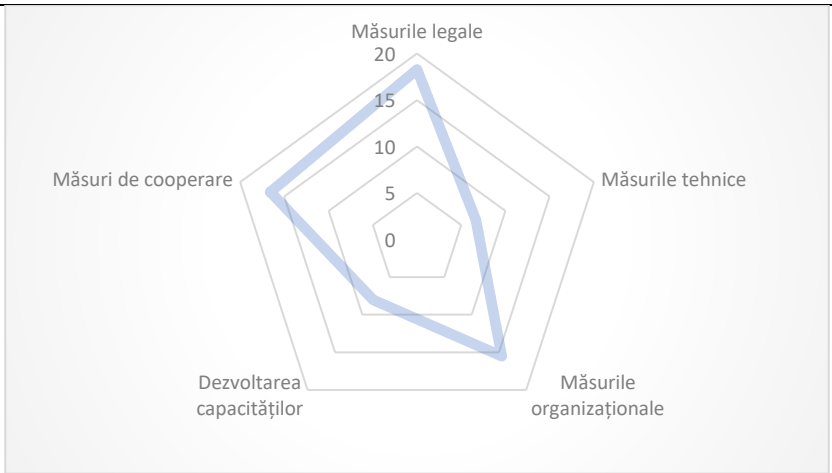
Potrivit Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030[4], sectorul TIC a devenit principalul motor al digitalizării și inovării în Republica Moldova și este în creștere rapidă. În 2023, industria IT a atins o pondere de peste 5,3% din produsul intern brut, depășind 15 mlrd. lei vânzări, ponderea sectorului TIC fiind de peste 8,3 % din PIB, cu peste 25 mlrd. lei vânzări în anul 2023, realizate de circa 3 200 de companii cu peste 35 000 de angajați.

În același timp, Strategia securității naționale a Republicii Moldova scoate în evidență riscurile cibernetice la care este expusă Republica Moldova, în principal fiind evidențiate atacurile cinetice sau cibernetice lansate de către actori statali

[3] https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis
[4] https://www.legis.md/cautare/getResults?doc_id=139408&lang=ro

	externi asupra infrastructurii critice naționale și regionale, atacurile cibernetice lansate asupra instituțiilor publice sau private de către structuri specializate în crime cibernetice, precum și riscurile asociate evoluțiilor din domeniul tehnologiilor informaționale și de comunicații, cum ar fi tehnologia blockchain și criptomoneda, inteligența artificială, învățarea automată, internetul obiectelor, tehnologia 5G, big data, tehnologiile cuantice, internetul ascuns. Conform Indicelui Global de Securitate Cibernetică (GCI) al Uniunii Internaționale a Telecomunicațiilor (ITU) pentru anul 2024, scorul general al Republicii Moldova este de 65,09, iar performanța țării este descrisă ca Nivelul 3 – Stabilirea, care reprezintă țările care au obținut un scor general de cel puțin 55/100 prin demonstrarea unui angajament de bază în materie de securitate cibernetică față de acțiunile guvernamentale care cuprind evaluarea, stabilirea sau implementarea anumitor măsuri de securitate cibernetică general acceptate într-un cadru moderat al numărului de piloni sau indicatori[5]. Potrivit raportului ITU privind Echipa Națională de Răspuns la Incidente Cibernetice, performanța Republicii Moldova pentru anul 2024 comparativ cu anul 2020 a înregistrat o creștere a măsurilor juridice, organizatorice și de cooperare, însă o scădere notabilă a măsurilor tehnice și de dezvoltare a capacităților. Această scădere însă poate fi atribuită parțial ajustărilor metodologice și ponderilor CGI, precum și modificării aduse întrebărilor. Graficul de mai jos (*Figura 4*) relevă performanța Republicii Moldova în CGI pentru anul 2024, evidențiind că măsurile tehnice și consolidarea capacităților sunt cele mai slabe puncte ale Republicii Moldova în acest domeniu. Cu toate acestea, acest indice poate fi îmbunătățit prin punerea în aplicare corespunzătoare a legislației naționale armonizate cu legislația UE. *Fig. 4 Performanța Republicii Moldova în GCI pentru anul 2024*

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



Republica Moldova nu are în prezent un cadru clar de gestionare a crizelor în domeniul securității cibernetice. Pe măsură ce situația amenințărilor 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 are un impact semnificativ asupra a cel puțin două state membre. Un astfel de incident, în funcție de cauza și de impactul său, poate escalada și se poate transforma în crize complexe, care afectează buna funcționare a pieței interne sau prezintă riscuri grave pentru securitatea și siguranța publică, pentru entități sau cetățeni din mai multe state membre sau din Uniune în ansamblu. UE a inițiat recent și recomandarea Consiliului pentru a îmbunătăți capacitățile de gestionare a crizelor cibernetice în UE[6].

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

Reieșind din cele descrise mai sus, precum și de întregul cadru

[6] https://digital-strategy.ec.europa.eu/en/library/cyber-blueprint-draft-council-recommendation

	strategic național, putem conchide că Republica Moldova se confruntă cu multiple provocări în domeniul securității cibernetice, printre care: • **Creșterea numărului de atacuri cibernetice** – Atacurile asupra instituțiilor publice și private s-au intensificat, punând în pericol infrastructurile critice și datele cetățenilor. • **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. • **Capacitate instituțională limitată** – Autoritățile responsabile cu securitatea cibernetică au resurse și expertiză insuficiente pentru a face față amenințărilor emergente. • **Lipsa conștientizării și educației în securitate cibernetică** – Atât sectorul public, cât și cel privat, dar și populația în general, au nevoie de instruire și conștientizare sporită privind riscurile și măsurile de protecție. • **Lipsa unui ecosistem de colaborare public-privat** – Sectorul privat nu este pe deplin integrat în mecanismele naționale de securitate cibernetică, iar cooperarea între instituțiile guvernamentale și companiile de tehnologie a informației și comunicațiilor este insuficientă. • **Nivelul scăzut de securitate cibernetică a infrastructurilor critice** – Sistemele energetice, financiare și de transport necesită măsuri urgente de protecție împotriva amenințărilor cibernetice sofisticate. • **Cooperare internațională insuficientă** – Deși Republica Moldova a început procesul de integrare în inițiative internaționale de securitate cibernetică, nivelul de colaborare cu partenerii externi trebuie extins și consolidat. Partajarea informațiilor, alinierea la standardele internaționale și participarea activă în platformele de securitate cibernetică sunt esențiale pentru creșterea capacității naționale de protecție. • **Creșterea criminalității informatice** – Infracțiunile cibernetice, inclusiv fraudele online, atacurile de tip ransomware și furturile de identitate s-au intensificat. Grupările infracționale utilizează metode din ce în ce mai sofisticate pentru a exploata vulnerabilitățile digitale, afectând atât instituțiile, cât și cetățenii. Obiectivele viitorului Program și acțiunile planificate urmează să

	sprijine obiectivul Republicii Moldova de integrare europeană și, implicit, armonizarea reglementărilor naționale ale Republicii Moldova cu legislația Uniunii Europene. Aprobarea Programului național de securitate cibernetică pentru 2026-2030 ar urma să genereze un impact semnificativ asupra securității cibernetice a Republicii Moldova. Printre beneficiile preconizate se pot număra: • **Îmbunătățirea protecției infrastructurilor critice** – Implementarea unor măsuri avansate de securitate va reduce vulnerabilitățile și riscul atacurilor cibernetice. • **Consolidarea capacității instituționale** – Crearea unor mecanisme eficiente de coordonare și creșterea resurselor umane calificate în domeniul securității cibernetice. • **Creșterea rezilienței cibernetice a societății** – Prin educație și conștientizare, populația și mediul de afaceri vor fi mai bine pregătite să prevină și să răspundă la incidente cibernetice. • **Creșterea încrederii în serviciile digitale** – Un mediu cibernetic mai sigur va contribui la adoptarea mai largă a tehnologiilor digitale, sprijinind dezvoltarea economică și inovația. • **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. • **Creșterea capacităților de combatere a criminalității informatice** – Consolidarea capacității de prevenire, detectare și investigare a infracțiunilor cibernetice prin îmbunătățirea cooperării între autorități, a cooperării internaționale și dezvoltarea unor mecanisme eficiente de sancționare a atacatorilor. Suplimentar, urmează a fi remarcat că digitalizarea accelerată a economiei moldovenești a adus oportunități, dar și riscuri pe măsură. Sectorul IT reprezintă unul dintre motoarele principale de creștere economică, 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. Totuși, un nivel scăzut de securitate cibernetică poate descuraja investițiile străine și poate afecta încrederea populației în serviciile digitale. În acest context, adoptarea **Programului național de securitate cibernetică pe anii 2026-2030** este esențială pentru asigurarea unui ecosistem digital sigur și

	rezilient, care să sprijine dezvoltarea economică și modernizarea Republicii Moldova. **Programul** va viza o gamă largă de actori care sunt direct sau indirect expuși riscurilor cibernetice și care vor beneficia de măsurile de protecție implementate. Printre aceștia se numără: 1. **Autoritățile și instituțiile publice** – responsabile de protejarea infrastructurilor digitale ale statului și de asigurarea continuității serviciilor esențiale prestate de către acestea. 2. **Infrastructura critică** – reprezentată de operatorii din sectoare cu o importanță critică ridicată, precum energie, transport, sănătate și telecomunicații, a căror securitate cibernetică este vitală pentru stabilitatea națională. 3. **Sectorul privat** - alții decât operatorii critici care depind de tehnologii digitale. 4. **Organizațiile necomerciale** – inclusiv ONG-urile și mediul academic, care joacă un rol important în promovarea rezilienței cibernetice și educației digitale. 5. **Cetățenii** – beneficiarii finali ai unui ecosistem digital sigur, care trebuie să fie informați și protejați împotriva amenințărilor online. În concluzie, pentru a răspunde acestor provocări, este necesară elaborarea unor intervenții bine direcționate, menite să asigure un ecosistem de **securitate cibernetică rezilient la amenințări externe și sustenabil pe termen lung**.
4. Scopul elaborării documentului de politici publice	După cum se menționează în Strategia de transformare digitală 2023-2030, *„la nivel național, securitatea cibernetică este o responsabilitate comună care necesită o acțiune coordonată prin intermediul unui Consiliu de coordonare pentru prevenirea, pregătirea, răspunsul și recuperarea incidentelor din partea autorităților guvernamentale, a sectorului privat și a societății civile.”* Pentru a asigura un șir de măsuri digitale sigure, securizate și reziliente, este necesar un document de politici publice cuprinzător în domeniu securității cibernetice, care să fie dezvoltat, implementat și executat folosind o abordare multilaterală. Stabilirea unei viziuni strategice, a unor obiective și priorități permite Republicii Moldova să privească securitatea cibernetică în mod holistic în ecosistemul digital național, în loc să se concentreze pe un anumit sector, obiectiv sau risc[7]. Domeniile principale de intervenție pentru Programul național

[7] https://mded.gov.md/wp-content/uploads/2023/11/STD_EN.pdf

	de securitate cibernetică pentru 2026-2030 sunt următoarele: **1. Consolidarea capacităților operaționale** În ultimii ani, Republica Moldova a elaborat un cadru normativ și organizațional privind modul de stimulare a rezilienței cibernetice. Următorul pas este consolidarea capacităților operaționale ale țării pentru a putea implementa cadrul creat. La nivel practic, implementarea acțiunilor din viitorul program va permite reducerea riscurilor și va stabili măsuri practice pentru a preveni incidentele cibernetice și, în cazul în care apar incidente cibernetice, vor exista suficiente capacități de a minimiza daunele și de a facilita recuperarea. Grupul de măsuri necesare urmează a fi dezvoltat în Program, acesta preponderent urmând să cuprindă: • Sprijinirea autorităților responsabile de securitatea cibernetică pentru înțelegerea, monitorizarea și evaluarea amenințărilor cibernetice. Practica de a învăța din incidentele din spațiul cibernetic este încă în curs de dezvoltare. Prin urmare trebuie sprijinite capacitățile acestor organizații de a răspunde, de a se recupera și de a învăța din incidentele și crizele cibernetice rapid și eficient. Guvernul va investi în oameni și sisteme care oferă o imagine mai clară a originii amenințărilor și spre cine sau ce sunt îndreptate acestea. • Gestionarea coordonată și integrată a riscurilor la nivel organizațional, sectorial și național. Riscurile cibernetice nu au primit încă un loc clar în gestionarea riscurilor la nivel național. Managementul riscurilor nu este încă clarificat, chiar dacă în Legea nr. 48/2023 privind securitatea cibernetică este stabilită o abordare bazată pe riscuri și ar trebui să joace un rol important în determinarea și atingerea nivelului dorit de reziliență. Autoritățile naționale cu funcții de supraveghere trebuie să furnizeze materiale metodice fără caracter obligatoriu pentru a ajuta furnizorii de servicii, esențiali sau importanți, să înțeleagă și să implementeze corect cadrul legal, iar măsurile de securitate ar trebui să constituie un scop al implementării acțiunilor din viitorul program. Echipa de răspuns la incidente cibernetice (CSIRT) și autoritățile de supraveghere vor face schimb de informații în mod eficient, la nivel național și internațional, atât cu privire la amenințări, incidente, cât și cu privire la modul de punere în aplicare a măsurilor de securitate. • Lipsa unui mecanism integrat de gestionare a crizelor și

	dezvoltarea unui mecanism național de gestionare integrată a crizelor oferă o bună oportunitate de a dezvolta un mecanism robust și eficient de gestionare a crizelor cibernetice. Este necesară stabilirea unui mecanism de gestionare a crizelor cibernetice, integrat în sistemul național de gestionare a crizelor, gata să fie integrat în cadrul UE de gestionare a crizelor. Exercițiile periodice de gestionare a crizelor cibernetice la nivel național și participarea activă la exercițiile UE și internaționale reprezintă un instrument în acest sens. • Identificarea digitală. Ca țară care a stabilit transformarea digitală ca prioritate strategică, este necesar de a se depune eforturi coordonate atât din partea sectorului public, cât și a celui privat, pentru a oferi infrastructuri digitale sigure și durabile. Identificarea digitală este una dintre elementele fundamentale, deoarece fără capacitatea de a se identifica în siguranță și de a tranzacționa online, nu sunt posibile interacțiuni complexe la distanță și, pe cale de consecință, orice efort ulterior de transformare digitală va fi viciat și incomplet. Principiile unificate pentru dezvoltarea serviciilor electronice, precum și reutilizarea datelor și utilizarea datelor între diferite resurse informaționale și sectoare sunt importante de a fi luate în considerare. În urma implementării Programului, în acest domeniu urmează să fie atinse următoarele obiective: o *Consolidarea capacităților operaționale de securitate cibernetică ale Republicii Moldova pentru a preveni, detecta și răspunde eficient amenințărilor cibernetice.* o *Îmbunătățirea gestionării riscurilor cibernetice și a răspunsului la crize prin integrarea securității cibernetice în cadrele naționale și desfășurarea de exerciții periodice.* o *Consolidarea capacității instituționale prin sprijinirea organismelor guvernamentale, echipelor de răspuns la incidente cibernetice (CSIRT) și autorităților de supraveghere în monitorizarea, evaluarea și schimbul de informații despre amenințări.* **2. Lupta împotriva criminalității informatice.** Criminalitatea 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 în general. Combinat cu operațiunile de criminalitate cibernetică sponsorizate, aceasta este o amenințare în creștere care necesită o intervenție din ce în ce mai decisivă și la scară largă a statului și o cooperare internațională în majoritatea țărilor. Criminalitatea cibernetică, inițiată atât de grupuri criminale organizate și organizații criminale, cât și de actori criminali sponsorizați, poate reprezenta o amenințare iminentă nu numai pentru sentimentul de securitate a societății și a cetățenilor, ci și pentru securitatea națională[8]. Strategia securității naționale menționează atacurile cibernetice lansate de actori statali străini asupra infrastructurii critice naționale și regionale și atacurile cibernetice asupra instituțiilor publice sau private de către structurile specializate în criminalitate informatică ca o amenințare la adresa securității Republicii Moldova. Pentru a îmbunătăți lupta împotriva criminalității informatice, este necesar de stabilit un răspuns mai eficient, axat pe detectarea și trasabilitatea datelor privind criminalitatea informatică și urmărirea penală a infractorilor cibernetici[9]. În urma implementării Programului în acest domeniu, urmează să fie atinse următoarele obiective: ○ *Consolidarea cooperării internaționale prin integrarea Republicii Moldova în cadrele de cooperare în materie de aplicare a legii și securitate cibernetică la nivelul UE.* ○ *Îmbunătățirea cooperării și coordonării între autoritățile publice în detectarea, investigarea și urmărirea penală a criminalității informatice și implicarea sectorului privat în prevenirea criminalității informatice.* **3. Reziliența cibernetică a societății** Acest domeniu de intervenție se concentrează pe oamenii din spatele tehnologiei și pe reziliența cibernetică a societății. 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 organizațiilor mici și a publicului a necesității de a se proteja împotriva amenințărilor cibernetice este încă limitată în Republica Moldova. În mod similar, nu există

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

[9] https://data.consilium.europa.eu/doc/document/ST-15129-2024-INIT/en/pdf

	cunoștințe științifice în materie de securitate cibernetică, prin urmare accentul va fi pus pe consolidarea capacităților și pe proiectarea viitoarelor programe de educație și formare pentru a aborda deficitul de personal specializat în securitate cibernetică. În urma implementării Programului, la acest capitol urmează să fie atinse următoarele obiective: o *Dezvoltarea unei forțe de muncă calificate în domeniul securității cibernetice prin extinderea oportunităților educaționale, prin stabilirea de burse pentru studenții dedicați carierei în sectorul public după absolvire.* o *Integrarea securității cibernetice în sistemul național de învățământ prin dezvoltarea unui curriculum specializat pentru elevii de gimnaziu.* o *Îmbunătățirea expertizei în domeniul securității cibernetice în instituțiile guvernamentale prin furnizarea de programe de formare dedicate securității cibernetice pentru cei angajații responsabili de ordinea publică, vamă și justiție.* o *Consolidarea rezilienței publice împotriva amenințărilor cibernetice prin campanii de conștientizare privind cele mai bune practici de siguranță și securitate cibernetică online.* **4. Cooperarea internațională și națională** Unul dintre principalele mijloace de asigurare a securității cibernetice este intensificarea cooperării naționale și internaționale și desfășurarea unor acțiuni mai active în cadrul organizațiilor și inițiativelor internaționale. Acest lucru va contribui nu doar la creșterea vizibilității Republicii Moldova ca partener internațional de încredere și la creșterea eficienței cooperării, dar va crește semnificativ și eficacitatea luptei împotriva criminalității informatice. Incidentele cibernetice nu se opresc la granițele naționale, astfel încât Guvernul trebuie să folosească în mod pro-activ toate oportunitățile oferite de cooperarea în interiorul și în afara Uniunii Europene. Guvernul Republicii Moldova își propune să contribuie la un mediu digital sigur, iar aceasta servește la abordarea riscurilor cibernetice transfrontaliere și permite un răspuns coordonat la incidente și crize cibernetice majore. Republica Moldova va face parte din eforturile depuse prin mijloace diplomatice – inclusiv consolidarea capacităților – pentru a consolida și extinde coaliția internațională care

	promovează comportamentul responsabil al statului în spațiul cibernetic. Pentru a asigura utilizarea cât mai eficientă a capacităților sale cibernetice limitate, autoritățile publice urmează să se angajeze în creșterea eficienței cooperării și îmbunătățirea mecanismelor de colaborare. Scopul este ca nu doar sectorul public, ci și sectorul privat și mediul academic să colaboreze și să coopereze îndeaproape pentru a asigura utilizarea eficientă a expertizei în securitate cibernetică, astfel încât reziliența cibernetică a țării să fie asigurată într-un mod cât mai eficient. În urma implementării Programului în acest domeniu, urmează să fie atinse următoarele obiective: o *Consolidarea cooperării internaționale prin participarea activă la organizații și inițiative internaționale;* o *Promovarea colaborării intersectoriale între autoritățile publice, sectorul privat și mediul academic pentru a îmbunătăți reziliența cibernetică și a optimiza utilizarea expertizei în securitate cibernetică.*
5. Concordanța cu documentele de politici publice, de planificare și angajamentele internaționale	Programul este elaborat în conformitate cu obiectivele de dezvoltare durabilă (ODD) și răspunde în mod indirect la fiecare dintre acestea. Totodată, acest document va contribui în special la următoarele ODD și țintele acestora adaptate la nivel național și reflectate în **Hotărârea Guvernului nr. 953/2022 cu privire la aprobarea cadrului național de monitorizare a implementării Agendei de Dezvoltare Durabilă 2030**: • **ODD 9:** Construirea unor infrastructuri reziliente, promovarea industrializării durabile și încurajarea inovației. o Creșterea semnificativă a accesului la tehnologia informației și comunicațiilor și promovarea accesului universal la internet până în 2030 (ținta 9.c). • **ODD 4:** Garantarea unei educații de calitate și promovarea oportunităților de învățare de-a lungul vieții pentru toți. o 4.b. Extinderea substanțială, până în anul 2030, a numărului de burse disponibile pentru înscrierea în învățământul superior, inclusiv formare profesională și tehnologia informației și comunicațiilor, programe tehnice, inginerești și științifice.

	• **ODD 17:** Consolidarea mijloacelor de implementare și revitalizare a parteneriatului global pentru dezvoltare durabilă. o 17.8. Operaționalizarea completă a băncii de tehnologii, mecanismului de consolidare a capacităților în știință, tehnologie și inovare, inclusiv sporirea utilizării tehnologiei generice, în special a tehnologiei informației și comunicațiilor. Programul va avea efect nu doar pentru protecția infrastructurii digitale a Republicii Moldova, ci va contribui și la dezvoltarea durabilă prin consolidarea economiei digitale, protecția drepturilor cetățenilor și promovarea colaborării internaționale, în conformitate cu obiectivele stabilite în Agenda de Dezvoltare Durabilă 2030. În același timp, programul răspunde la obiectivul privind prevenirea și combaterea amenințărilor hibride pe palierul securității cibernetice și informaționale stabilit în **Programul de activitate al Guvernului „Moldova prosperă, sigură, europeană”,** aprobat prin Hotărârea Parlamentului nr. 28/2023. Suplimentar, Programul se aliniază cu **Acordul de Asociere**, care trasează un șir de priorități ce vizează prevenirea și combaterea criminalității, inclusiv combaterea criminalității informatice. De asemenea, Programul va contribui la implementarea următoarei direcții prioritare din **Strategia Națională de Dezvoltare „Moldova Europeană 2030”,** aprobată prin Legea nr. 315/2022: • **5.3. Transformarea electronică a guvernării, societății și economiei**: o Consolidarea infrastructurii de securitate cibernetică, de securitate a infrastructurii critice a datelor și asigurarea confidențialității datelor personale; o Consolidarea și ajustarea programelor de studii avansate în domeniul securității cibernetice și investigării crimelor cibernetice pentru instruirea specialiștilor. Cât privește corelarea cu strategiile sectoriale și alte documente de politici în vigoare, Programul se aliniază cu următoarele documente: **Strategia securității naționale a Republicii Moldova, aprobată**

	<u>prin Hotărârea Parlamentului nr. 391/2023</u> **Direcția de acțiune: securitatea și reziliența cibernetică:** o dezvoltarea formelor de cooperare public-privată pentru asigurarea securității cibernetice; o îmbunătățirea sistemelor de comunicații securizate de stat; o modernizarea bazei tehnice IT a instituțiilor publice, introducerea sistemului de verificare biometrică a identității în conformitate cu standardele europene și implementarea proceselor de protecție și de securizare a datelor; o dezvoltarea planurilor de securitate și apărare cibernetică a infrastructurii și entităților critice; o organizarea, la scară națională, a programului de educație privind igiena cibernetică în rândul funcționarilor publici, al studenților și al elevilor; o organizarea și participarea la exerciții de securitate și apărare cibernetică; o consolidarea dialogului și a cooperării în domeniul cibernetic cu UE; o participarea și/sau alinierea la normele UE în domeniul reglementării tehnologiilor transformative. **<u>Strategia de transformare digitală a Republicii Moldova pentru anii 2023-2030, aprobată prin Hotărârea Guvernului nr. 650/2023</u>** **Obiectivul general nr.5: Crearea unui mediu digital accesibil, sigur și incluziv**: Realizarea acestui obiectiv general se va asigura prin următoarele direcții prioritare: o Instituirea unei autorități competente în domeniul securității cibernetice la nivel național; o Implementarea cadrului general strategic și operațional de coordonare și cooperare; o Implementarea măsurilor de securitate cibernetică și mecanismului obligatoriu de raportare a incidentelor cibernetice; o Consolidarea rezilienței infrastructurilor digitale ale furnizorilor de servicii critice; o Asigurarea aplicării cerințelor (standardelor) de securitate cibernetică în cadrul dezvoltării și/sau procurării software și hardware; o Dezvoltarea capacităților resurselor umane în domeniul

	securității cibernetice. **<u>Strategia de apărare națională a Republicii Moldova pentru 2024–2034, aprobată prin Hotărârea Guvernului nr. 319/2024</u>** **Direcția de acțiune 29.7: Consolidarea protecției spațiului cibernetic:** Obiectivul este asigurarea rezilienței și securității cibernetice a entităților publice și private care gestionează infrastructuri critice și servicii esențiale. Forțele Armate vor consolida capacitățile de securitate cibernetică prin îmbunătățirea sistemelor informatice, sporirea capacităților de răspuns la atacuri cibernetice și creșterea nivelului de conștientizare a securității în rândul personalului. Cooperarea cu parteneri naționali și internaționali va juca un rol crucial în susținerea acestor obiective. **<u>Strategia de dezvoltare a afacerilor interne pentru 2022-2030, aprobată prin Hotărârea Guvernului nr. 658/2022</u>** **Obiectivul general 6.6: Consolidarea sistemelor de gestionare a serviciilor TIC și a securității informaționale** **Obiectivul specific 2.1.3: Creșterea gradului de conștientizare în rândul cetățenilor (inclusiv al copiilor) privind pericolele din spațiul cibernetic/online** Totodată, acest program urmează să coreleze cu **<u>Programul de prevenire și combatere a criminalității pentru anii 2022-2025, aprobat prin Hotărârea Guvernului nr. 948/2022,</u>** care are: **Obiectiv general:** 1. Crearea și facilitarea accesului la instrumente și mecanisme adecvate privind combaterea și prevenirea criminalității informatice. **Obiective specifice:** 1.1. Dezvoltarea capacităților instituționale în domeniul criminalității cibernetice pentru asigurarea unei reacții de răspuns eficiente a instituțiilor responsabile; 1.2. Eficientizarea mecanismului privind colectarea datelor referitoare la incidentele de securitate cibernetică; 1.3. Sporirea gradului de sensibilizare a cetățenilor (inclusiv a copiilor) prin informarea acestora privind pericolele la care se pot expune accesând spațiul cibernetic/online. Programul răspunde și la acțiunile prevăzute în **<u>Planul național de reglementări pentru anul 2025</u>** (Hotărârea Guvernului nr. 841/2024) și proiectul **<u>Programului Național de Aderare a Republicii Moldova la UE 2025-2029</u>**, care stabilesc aprobarea

	până în noiembrie 2025 a documentului de politici publice în domeniul securității cibernetice.
	
	Corelarea cu cadrul bugetar pe termen mediu
	
	Implementarea programului va fi realizată prin cel puțin două 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"
	
	Costurile aferente Programului vor fi detaliate în Planul de acțiuni pentru implementare. Pe lângă resursele bugetare, vor fi identificate surse suplimentare de finanțare din partea partenerilor de dezvoltare pentru realizarea acțiunilor prevăzute în document. Estimarea costurilor pentru fiecare obiectiv și acțiune va fi realizată în baza programelor și subprogramelor bugetare pentru o alocare eficientă a resurselor financiare.

6. Perioada planificată pentru elaborarea documentului de politici publice	Programul va fi elaborat în perioada aprilie – septembrie 2025, iar implementarea acestuia este preconizată pentru anii 2026-2030.
7. Părțile implicate în elaborarea documentului de politici publice și mecanismele de asigurare a transparenței și a participativității	Procesul de cooperare pentru elaborarea și aprobarea Programului va fi efectuat într-o manieră participativă, cu implicarea părților interesate la nivel de ministere, alte autorități publice, sectorul privat și societatea civilă. Consultările publice vor fi efectuate în conformitate cu prevederile cadrului normativ, inclusiv conform prevederilor Legii nr. 239/2008 privind transparența în procesul decizional și Hotărârii Guvernului nr. 967/2016 privind mecanismul de consultare publică cu societatea civilă în procesul decizional. Principalii actori implicați în proces: - Ministerul Dezvoltării Economice și Digitalizării (autoritate principală); - Președenția Republicii Moldova; - Ministerul Energiei; - Ministerul Infrastructurii și Dezvoltării Regionale;

	- Ministerul Afacerilor Interne; - Ministerul Apărării; - Ministerul Mediului; - Ministerul Sănătății; - Ministerul Agriculturii și Industriei Alimentare; - Serviciul de Securitate și Informații; - Banca Națională a Moldovei; - Agenția pentru Securitate Cibernetică; - Agenția Națională de Reglementare în Comunicații Electronice și Tehnologia Informației (ANRCETI); - Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică"; - Instituția publică "Agenția de Guvernare Electronică"; - Instituția publică "Centrul Tehnologii Informaționale în Finanțe"; - Alte agenții relevante și instituții guvernamentale cu responsabilități de securitate cibernetică; - Sectorul privat (companii de telecomunicații și IT, instituții financiare, operatori de infrastructură critică, asociații de afaceri etc); - Societatea civilă (ONG-uri axate pe conștientizarea digitală și a securității cibernetice, mediul academic și de cercetare etc.); - Parteneri de dezvoltare (reprezentanți UE și proiecte care sprijină domeniul digital și de securitate cibernetică, organizații internaționale, parteneri bilaterali etc.); - Cetățeni (utilizatori individuali de servicii digitale și platforme online, reprezentanți ai grupurilor vulnerabile afectate de amenințări cibernetice etc.). Ministerul Dezvoltării Economice și Digitalizării va iniția consultarea publică a conceptului Programului în scopul informării și recepționării recomandărilor tuturor părților interesate și, în funcție de rezultatele consultărilor, va decide cu privire la extinderea numărului părților implicate, precum și al reprezentanților din partea autorităților delegatare. În baza recomandărilor și propunerilor parvenite în procesul de consultare, Ministerul Dezvoltării Economice și Digitalizării va asigura un proces participativ de consultare publică a

	Programului prin organizarea, după caz, a meselor rotunde, dezbaterilor publice, sondajelor, chestionarea grupurilor-țintă etc., asigurând respectarea principiului LNOB *(a nu lăsa pe nimeni în urmă)*.