Analiză de impact

la proiectul Hotărârii Guvernului cu privire la constituirea, organizarea și funcționarea Agenției Naționale pentru Securitate Cibernetică

Titlul analizei impactului (poate conține titlul propunerii de act normativ):	Proiectul Hotărârii Guvernului cu privire la constituirea, organizarea și funcționarea Agenției Naționale pentru Securitate Cibernetică
Data:	07.07.2023
Autoritatea administrației publice (autor):	Ministerul Dezvoltării Economice și Digitalizării
Subdiviziunea:	Secția politici în domeniul securității cibernetice
Persoana responsabilă și datele de contact:	Dl Sergiu Florea, sergiu.florea@mded.gov.md

Compartimentele analizei impactului

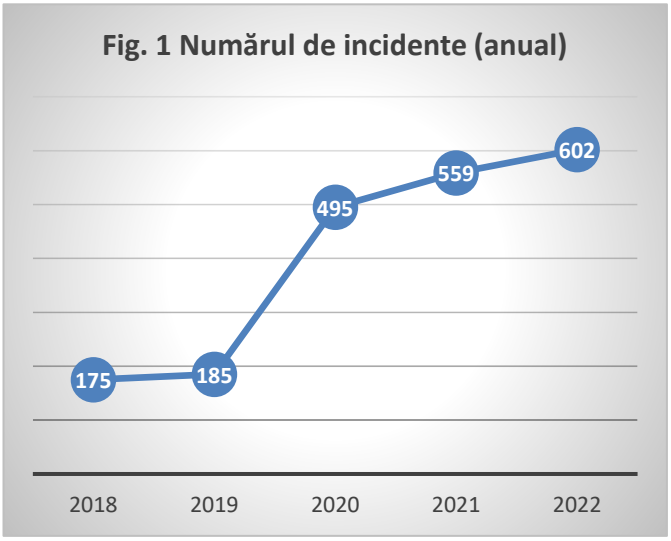
1. Definirea problemei

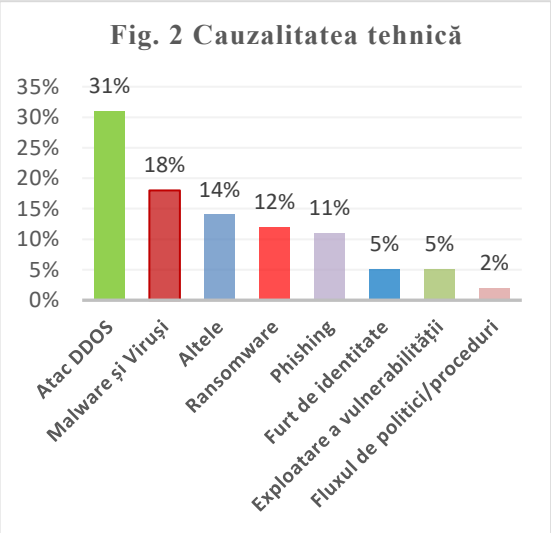
a) Determinați clar și concis problema și/sau problemele care urmează să fie soluționate

Protecție insuficientă în sectorul public și sectorul privat împotriva incidentelor, riscurilor și amenințărilor legate de securitatea rețelelor și a sistemelor informatice.

b) Descrieți problema, persoanele/entitățile afectate și cele care contribuie la apariția problemei, cu justificarea necesității schimbării situației curente și viitoare, în baza dovezilor și datelor colectate și examinate

Potrivit datelor statistice, la nivelul Uniunii Europene, în perioada 2018-2022, statele membre au raportat un număr de 2016 incidente cibernetice cu impact semnificativ conform criteriilor stabilite de Directiva NIS1, Codul european al comunicațiilor electronice și Regulamentul eIDAS. Dintre acestea, 24% au fost clasificate ca acțiuni rău intenționate (malicious actions). Sectorul privat a fost cel mai afectat, în special sectorul bancar, cel de comunicații, cel al sănătății și cel al serviciilor de încredere. Tendința generală a incidentelor cu impact semnificativ este în creștere, iar explozia din 2020 poate fi legată de creșterea utilizării mediului digital ca urmare a pandemiei COVID 19 (*Fig. 1*). Din cele 490 de incidente rău intenționate raportate, majoritatea sunt clasificate ca infracțiuni cibernetice, conform graficului de cauzalitate tehnică prezentat în *Fig. 2*. Aceste date indică necesitatea unei abordări mai riguroase și mai bine coordonate la nivel european pentru a preveni și gestiona incidentele cibernetice cu impact semnificativ.



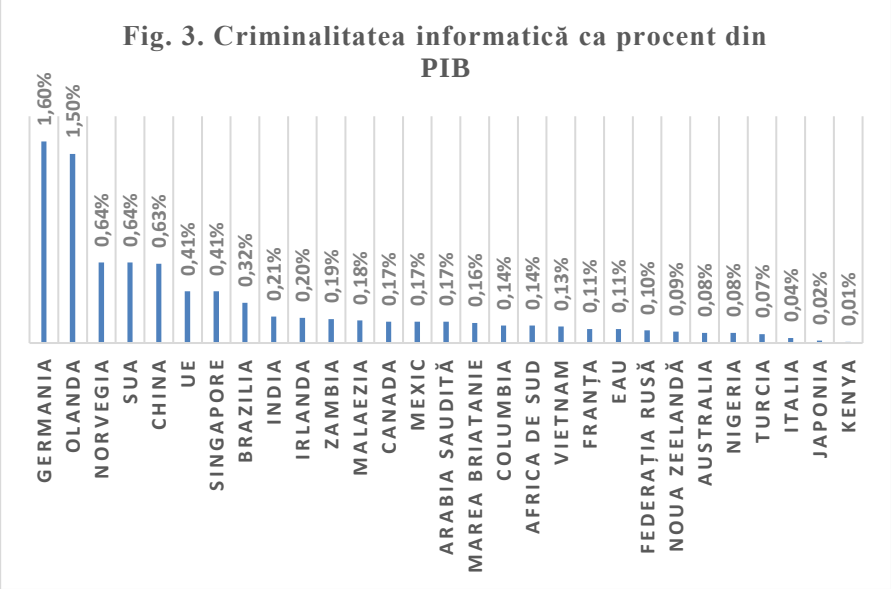


Potrivit raportului IBM *Cost of a Data Breach*[1], impactul financiar al unei încălcări a datelor este semnificativ pentru entitățile critice. Raportul IBM arată că în 2022, costul mediu global al unei încălcări a datelor a atins un nivel istoric de 4,35 milioane de dolari americani, reprezentând o creștere cu 2,6% față de anul precedent și o creștere cu 12,7% față de 2020.

Raportul subliniază factorii care influențează costurile încălcării datelor și prezintă soluții pentru minimizarea riscurilor. De exemplu, utilizarea de instrumente de inteligență artificială și automatizare poate reduce costurile cu 3,05 milioane de dolari americani, în timp ce organizarea unei echipe CSIRT și testarea regulată a planului de răspuns la incidente poate economisi în medie 2,66 milioane de dolari americani. Implementarea unei arhitecturi de încredere zero poate reduce costurile cu aproximativ 1 milion de dolari americani, în timp ce tehnologiile XDR au redus în medie cu 29 de zile timpul de răspuns la încălcări.

Raportul IBM mai menționează și alți factori care influențează costurile de încălcare a datelor, cum ar fi costul mai mare pentru organizațiile cu infrastructură critică și costurile diferite pentru atacurile de phishing, ransomware sau acreditări compromise. În plus, raportul subliniază o creștere bruscă a costurilor primelor de asigurare cibernetică și a plăților considerabile pentru ransomware. În ciuda acestor costuri, totuși, companiile sunt din ce în ce mai deschise să plătească răscumpărări.
Prin urmare, raportul IBM evidențiază importanța implementării de soluții de securitate pentru a minimiza riscurile de încălcare a datelor, întrucât costurile financiare asociate cu astfel de incidente pot fi semnificative pentru entitățile critice.

Suplimentar, urmează a fi menționat studiul global al companiei McAfee[2], care a estimat pierderile economice produse de criminalitatea cibernetică. Acest studiu intitulat "*Net Losses: Estimating the Global Cost of Cybercrime*" oferă o estimare a impactului economic al criminalității informatice pentru diferite țări, măsurat ca procent din PIB. În graficul prezentat în *Fig. 3* sunt afișate cele mai afectate state în funcție de monetizarea prejudiciului, în procent din PIB-ul acestora. În medie, prejudiciul produs de infracțiunile cibernetice reprezintă aproximativ 0,3% din PIB. Dacă să extrapolăm pe Republica Moldova, Produsul Intern Brut al acesteia a fost de 14,048 miliarde de dolari SUA în 2022. Astfel, putem deduce un potențial prejudiciu anual de circa 42 mil.de dolari, având în vedere media de 0,3% din PIB.



În 2018[3], costul criminalității cibernetice la nivel mondial a depășit 1 trilion de dolari, iar pierderile monetare produse de acest tip de infracțiune s-au ridicat la circa 945 de miliarde de dolari. Cheltuielile pentru securitatea cibernetică la nivel global se estimează că au depășit 145 de miliarde de dolari în 2020.

În prezent, economia globală suportă o povară de 1 trilion de dolari din cauza criminalității cibernetice. În 2018, s-a constatat că aceste infracțiuni au costat economia globală peste 600 de miliarde de dolari, iar o nouă estimare sugerează o creștere de peste 50% în doi ani. În acest context, devine din ce în ce

[1] https://www.ibm.com/downloads/cas/3R8N1DZJ
[2] https://www.enisa.europa.eu/publications/the-cost-of-incidents-affecting-ciis
[3] https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf

mai important să se instituie mecanisme de identificare a furnizorilor de servicii esențiale, ale căror perturbare ar putea cauza prejudicii semnificative nu numai acestor entități, ci și unui număr mare de beneficiari ai acestor servicii și intereselor statului. De asemenea, este necesară îmbunătățirea schimbului de informații între diferitele categorii de furnizori de servicii și asigurarea unui sistem adecvat de răspuns coordonat la eventualele amenințări, pe baza unor analize justificate de date statistice și monitorizări în timp real. În acest fel, se poate limita impactul economic al criminalității cibernetice și se poate proteja economia globală și interesele cetățenilor.

Conform proiectului Strategiei de transformare digitală pentru anii 2023-2030, sectorul tehnologiei informației și comunicațiilor (TIC) din Republica Moldova a înregistrat o creștere dinamică datorită cererii ridicate, concurenței și efortului consolidat al tuturor actorilor implicați, generând anual circa 7% din Produsul Intern Brut al țării, cu venituri totale de aproximativ 15 miliarde MDL sau 900 milioane USD. În ultimii cinci ani, piața de comunicații electronice a avut o perioadă de creștere agilă, consolidând poziția Moldovei ca destinație de top pentru internetul de mare viteză, accesibilitate și disponibilitate a internetului gigabit.

Sectorul tehnologiei informației (IT) a devenit motorul creșterii industriei TIC în perioada 2015-2020, depășind telecomunicațiile și contribuind la aproximativ 3,6% din PIB-ul țării în 2020, față de 0,8% în 2013, când sectorul IT a fost declarat prioritar. Această creștere a fost determinată de avantajele Moldovei ca destinație de externalizare a serviciilor IT, precum costurile reduse, locația și competențele, precum și de un regim fiscal și administrativ facilitat pentru rezidenții Virtual Moldova IT Park.

În ciuda acestor realizări, dezvoltarea rapidă a tehnologiei informației și comunicațiilor electronice și a proceselor de transformare digitală a dus la creșterea semnificativă și continuă a amenințărilor la adresa securității cibernetice. Pandemia COVID-19 a arătat cât de sensibile sunt serviciile electronice și economia digitală la astfel de provocări. Republica Moldova, la fel ca multe alte țări, se confruntă cu diferite tipuri de atacuri cibernetice care vizează nu numai entitățile guvernamentale, ci și sectorul privat și populația în general.

În august 2022, Serviciul Tehnologia Informației și Securitate Cibernetică (STISC) a reușit să contracareze mai multe tentative de atacuri cibernetice asupra sistemelor informaționale de importanță statală din Republica Moldova. Aceste atacuri vizau în jur de 80 de sisteme informaționale, platforme și portaluri publice, cu scopul de a cauza indisponibilitatea resurselor informaționale ale statului. Analiza preliminară a arătat că aceste atacuri aveau un caracter distribuit și erau efectuate din afara Republicii Moldova.

Această situație se înscrie într-un context mai larg de amenințări cibernetice în Republica Moldova. În general, țara este afectată de diferite tipuri de atacuri cibernetice, care vizează nu numai entitățile guvernamentale, ci și sectorul privat și populația în general. Raportul de evaluare efectuat de ITU[4] relevă că autoritățile specializate monitorizează și urmăresc peisajul amenințărilor cibernetice, însă lipsește o înțelegere holistică a acestora. Conform acestui raport, cele mai comune tipuri de incidente de securitate cibernetică sunt scams, phishing (inclusiv smishing și vishing), ransomware, web defacement și denial of service. Din 2015, Republica Moldova s-a confruntat cu patru tipuri de atacuri, inclusiv DDOS, phishing și atacuri de forță brută care au încercat să obțină acces la sistemele informatice guvernamentale și deturnarea paginilor web oficiale. Sectorul privat este la fel de vulnerabil la amenințările cibernetice, iar IMM-urile reprezintă cea mai vulnerabilă parte a acestuia. În 2019, IMM-urile reprezentau aproximativ 98,6% din numărul total de întreprinderi, iar circa 17% dintre acestea au integrat cu succes tehnologiile digitale în activitatea lor, ceea ce ridică îngrijorări deosebite.

În plus, cetățenii Republicii Moldova sunt, de asemenea, supuși atacurilor cibernetice, iar cele mai frecvente sunt vishingul și smishingul. Aceste tipuri de atacuri au succes datorită nivelului redus de

[4] https://moldova.un.org/sites/default/files/2023-01/CIRT-Assessment-Moldova-final.pdf

cultură digitală și igiena cibernetică. De exemplu, în 2021, una dintre grupurile criminale prinse pentru furt de bani din conturile bancare a utilizat Viber pentru a contacta cetățenii și a se prezenta ca angajați ai băncii, făcând peste 40 de retrageri din conturile bancare ale mai multor persoane fizice. Astfel, este esențial ca atât cetățenii, cât și întreprinderile și entitățile guvernamentale să adopte protocoale de securitate cibernetică.

În prezent, Republica Moldova nu dispune de mecanisme fiabile și eficiente pentru consolidarea datelor și informațiilor care să ofere o imagine de ansamblu asupra situației reale în domeniul securității cibernetice la nivel național. Această lipsă de date statistice suficiente îngreunează analiza situației și formularea unor concluzii pertinente cu privire la reziliența entităților care prestează servicii esențiale în acest domeniu. Întreprinderea măsurilor de asigurare a securității cibernetice și raportarea incidentelor semnificative sunt abordate într-un mod mai sistematizat doar în sectorul public, cu excepția autorităților administrației publice locale. În acest caz, CERT-Gov are rolul central în gestionarea incidentelor de orice tip care au loc în rețelele și sistemele informaționale ale statului. Cu toate acestea, criteriile aplicabile clasificării incidentelor cibernetice în acest sector nu sunt interoperabile cu cele aplicate la nivelul statelor europene, din perspectiva clasificării bazate pe criteriile stabilite de Directiva NIS (art. 14 alin. 4 și art. 16 alin. (4))[5].

Lipsa unei abordări sistemice la nivel național are ca efect indisponibilitatea în sectorul privat a informațiilor privind numărul incidentelor de securitate cibernetică, natura acestora și cauzalitatea tehnică. În plus, nu există informații despre distribuția acestor incidente în diferite sectoare de activitate.

Reieșind din faptul că această analiză este corelată cu intervențiile legislative de armonizare a legislației naționale cu legislația UE în domeniul securității cibernetice la nivel național, se poate anticipa tipologia persoanelor juridice de drept public și de drept privat care vor cădea sub incidența unor obligații de raportare și îndeplinire a anumitor cerințe de securitate. În primul rând, pentru acest scop este necesară determinarea sectoarelor critice, pe baza anexelor Directivei NIS2. Aceste sectoare și subsectoarele corespunzătoare sunt împărțite în două categorii: 11 sectoare cu o importanță critică ridicată și alte 7 sectoare de importanță critică.

În al doilea rând, conform Directivei NIS2, se aplică regula dimensiunii pentru a determina cercul de subiecți ai legii. În acest sens, urmează a fi calificați ca operatori de servicii esențiale/furnizori de servicii critice persoanele juridice de drept privat care se califică cel puțin ca întreprinderi mijlocii, care furnizează servicii în unul sau mai multe dintre sectoarele sau subsectoarele determinate ca fiind critice pentru Republica Moldova, precum și toate persoanele juridice de drept privat.

În cercul de subiecți care urmează să cadă sub incidența reglementărilor în domeniul securității cibernetice ar trebui incluși furnizorii de rețele publice de comunicații electronice sau de servicii de comunicații electronice accesibile publicului, prestatori de servicii de încredere, Registratorul național al domeniului de nivel superior .md, furnizorii de servicii de înregistrare a numelor de domenii, persoanele juridice care sunt singurul furnizor în Republica Moldova a unui serviciu care este esențial pentru susținerea unor activități societale și economice critice, furnizorul unui serviciu dependent de o rețea și/sau de un sistem informatic, persoanele juridice care sunt critice din cauza importanței lor specifice la nivel național sau regional pentru sectorul sau tipul de servicii respectiv sau pentru alte servicii, precum și autoritățile publice care administrează și gestionează infrastructurile de comunicații electronice, sistemele informatice sau alte servicii esențiale pentru societate etc.

În baza acestei tipologii, autoritatea competentă are responsabilitatea de a identifica fiecare furnizor de servicii asupra cărora ar trebui să se aplice obligațiile prevăzute de lege, ceea ce are un un impact direct asupra numărului de personal ce va trebui angajat în cadrul acestei autorități și a subdiviziunii de supraveghere și control. Odată ce acești subiecți sunt identificați, autoritatea competentă urmează să se asigure că aceștia respectă obligațiile legale în ceea ce privește măsurile de securitate și

[5] https://eur-lex.europa.eu/eli/dir/2016/1148/oj?locale=ro

notificările. Prin urmare, realizarea calitativă a acestor atribuții va implica angajarea unui număr mai mare de personal, în mod special pentru a asigura supravegherea și controlul adecvat al acestor furnizori de servicii. Este important de subliniat faptul că autoritatea competentă nu se va limita doar la funcția de funcția de echipă de răspuns la incidentele cibernetice la nivel național, ci va avea un număr mai larg de competențe. Aceasta implică o coordonare și colaborare amplă între diferitele autorități competente pentru a asigura implementarea eficientă a reglementărilor și protejarea infrastructurilor și serviciilor critice.

În prezent, Republica Moldova nu dispune de proceduri mature de colaborare și schimb de informații în timp real între autoritățile competente ale Guvernului și întreprinderile critice, în special în ceea ce privește identificarea operatorilor de servicii esențiale, riscurile și amenințările cibernetice și non-cibernetice, precum și măsurile de securitate cibernetică și fizică luate de aceste entități și rezultatele activităților de supraveghere.

În 2016, Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) a publicat un studiu[6] cu privire la diferitele abordări pe care statele membre urmează să le aplice pentru a-și proteja infrastructurile critice de informații. Sunt prezentate două modele – centralizat și descentralizat.

- **Modelul centralizat** se caracterizează prin:
  - existența unei autorități centrale pentru toate sectoarele;
  - legislație cuprinzătoare.

- **Modelul descentralizat** – multiple autorități sectoriale competente pentru sectoarele și serviciile specifice și se caracterizează prin:
  - principiul subsidiarității;
  - cooperare strânsă între agențiile publice;
  - legislație sectorială.

În august 2022, urmare a coordonării dintre echipa Proiectului de asistență rapidă în domeniul securității cibernetice în Moldova și beneficiarii proiectului au fost identificate pentru analiză modelele de guvernanță în șase țări membre UE, care au transpus Directiva NIS1 și au o organizare matură de securitate cibernetică, conform diferitelor măsurători de securitate cibernetică. Analiza echipei proiectului s-a bazat pe următoarele elemente:

- Cartografierea principalilor actori guvernamentali în domeniul securității cibernetice și cum aceștia și își îndeplinesc funcțiile și îndatoririle în special în următoarele domenii:
  - Elaborarea și aplicarea politicilor (inclusiv elaborarea și punerea în aplicare a strategiei naționale de securitate cibernetică);
  - Gestionarea incidentelor și a crizelor (în special, din punctul de vedere al CERT/CSIRT);
  - Coordonarea infrastructurii critice de informații și protecția serviciilor esențiale;
  - Standardele naționale în domeniul TIC și al securității cibernetice;
  - Apărarea cibernetică militară națională.
- Rolurile și funcțiile autorităților naționale din perspectiva strategiei naționale de securitate cibernetică.
- Cadrul normativ în domeniul securității cibernetice.
- Poziția în indicii internaționali de securitate cibernetică.

Astfel, în baza criteriilor de mai sus au fost analizate următoarele șase state membre UE, după cum urmează:

- În **Republica Cehă** autoritatea competentă este situată în subordinea Guvernului. Totodată, CERT-ul guvernamental este parte componentă a autorității competente. CERT-ul național este externalizat în baza unui contract public.

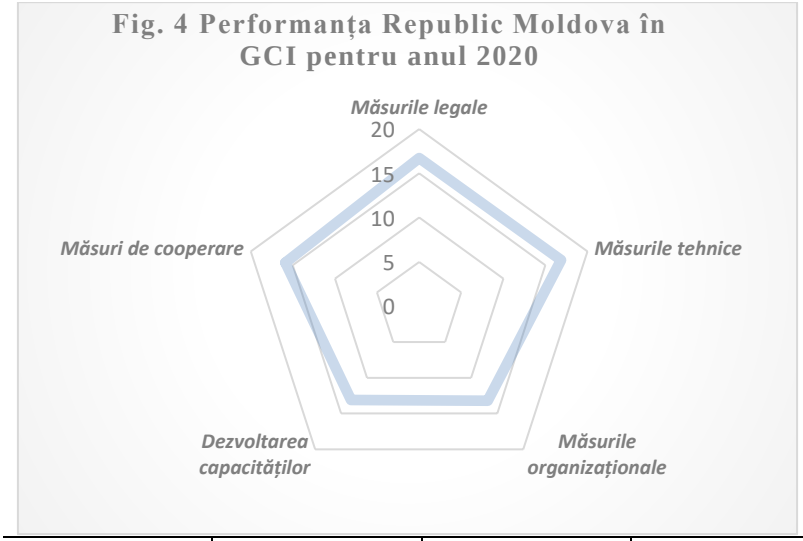
[6] https://www.enisa.europa.eu/publications/stocktaking-analysis-and-recommendations-on-the-protection-of-ciis

Chiar dacă autoritatea competentă are statut similar cu cel al unei autorități administrative centrale din Republica Moldova, totuși aceasta este o agenție de implementare, iar politicile în domeniul securității cibernetice sunt elaborate de Ministerul Afacerilor Interne.

- În **Estonia** autoritatea competentă este situată în subordinea Ministerul Economiei și Comunicațiilor. Totodată, CERT-ul național și CERT-ul guvernamental sunt parte componentă a autorității competente.
  Politicile în domeniul securității cibernetice sunt elaborate de Ministerul Economiei și Comunicațiilor la nivel de coordonare.
- În **Finlanda** se aplică un model descentralizat și nu are o autoritate responsabilă de gestionarea centralizată și coordonarea securității cibernetice la nivel național. Fiecare autoritate competentă este responsabilă în domeniul său, respectând legislația în domeniul securității cibernetice.
  Centrul Național de Securitate Cibernetică din cadrul Agenției finlandeze pentru transport și comunicații sigură funcționarea activităților socio-economice în caz de perturbări și situații de urgență în condiții normale (ex. asigurarea funcționării și securității informaționale a rețelelor și serviciilor publice de comunicații, precum și a altor rețele și servicii de comunicații conectate la acestea).
  CSIRT al Centrului Național de Securitate Cibernetică (NCSC-FI) participă la sarcinile agenției de prevenire, investigare și informare a breșelor de securitate, precum și la menținerea și partajarea conștientizării situației de securitate cibernetică.
  Pe lângă Centrul Național de Securitate Cibernetică, Finlanda are mai multe autorități naționale competente pentru operatorii de servicii esențiale în diferite sectoare definite în Directiva NIS 1, spre exemplu:
  - Energie - Autoritatea pentru Energie;
  - Transport - Agenția Finlandeză pentru Siguranța Transporturilor
  - Infrastructuri bancare și ale pieței financiare - Autoritatea de Supraveghere Financiară;
  - Sănătate - Autoritatea Națională de Supraveghere a Sectorului Sănătate.
- În **Grecia** autoritatea competentă este Direcția de securitate cibernetică din cadrul Secretariatului general pentru politică digitală din cadrul Ministerului Politicii Digitale, Telecomunicațiilor și Informaticii. CERT-ul național este în cadrul Marelui Stat Major, iar CERT-ul guvernamental este în subordinea Agenției Naționale de Informații.
  Politicile în domeniul securității cibernetice sunt elaborate de Ministerul Politicii Digitale, Telecomunicațiilor și Informaticii.
- În **Olanda** se aplică un model mixt, cu unele elemente din modelele de guvernanță care ar putea fi caracterizate ca fiind descentralizate în ce privește autoritățile competente. Model de guvernanță în Olanda este unul distribuit după cum urmează: din punctul de vedere al competenței de supraveghere și control, Ministerul Afacerilor Economice și Climei, Banca Națională, Ministerul Infrastructurii și Gestionarea Apelor și Ministerul Sănătății acoperă toate cele 7 sectoare din anexa nr. II la Directiva NIS1. Ministerul Justiției și Securității exercită funcția de punct unic de contact și are în subordinea sa Centrul Național de Securitate Cibernetică care exercită funcția de CSIRT național și guvernamental, a cărui constituență este alcătuită doar din Operatorii de Servicii Esențiale. Un CSIRT de dedicat exclusiv Furnizorilor de Servicii Digitale operează în subordinea Ministerului Afacerilor Economice și al Climei.
  Politicile în domeniul securității cibernetice sunt elaborate de Ministerul Justiției și Securității.
- În **România** modelul de guvernanță în domeniul securității cibernetice este unul mai degrabă centralizat din perspectiva elementelor definitorii pentru un astfel de model date de Directiva NIS1. Astfel funcțiile de autoritate competentă (identificare, evidență, supraveghere și control), CSIRT național și punct unic de contact sunt concentrate într-o singură autoritate Directoratul Național de Securitate Cibernetică, care este organ de specialitate al administrației publice centrale cu personalitate juridică, în coordonarea prim-ministrului.

Potrivit Indicelui Global de Securitate Cibernetică (GCI) al Uniunii Internaționale a Telecomunicațiilor (ITU) pentru anul 2020, Republica Moldova se situează pe locul 33 în Europa și pe locul 63 în lume. Acest indice evaluează angajamentul a 194 de țări în materie de securitate cibernetică, măsurând gradul de conștientizare a importanței și dimensiunilor problemelor de securitate cibernetică, precum și rezistența și fiabilitatea sectorului TIC al fiecărei țări. Potrivit raportului ITU privind echipa de răspuns la incidente de securitate cibernetică la nivel național, performanța Republicii Moldova în cadrul GCI pentru 2020 a scăzut, dar acest lucru poate fi atribuit eliminării și adăugării de noi întrebări și modificărilor metodologiei și ponderării GCI. Însă acest indice poate fi îmbunătățit în contextul armonizării legislației naționale la cea a UE și implementării corespunzătoare a legislației naționale, inclusiv stabilirii autorității competente responsabile de gestionarea acestui sector. Graficul de mai jos (*Fig. 4*) ilustrează performanța Republicii Moldova în GCI pentru anul 2020, atrăgând atenția că anume măsurile organizaționale și consolidarea capacităților sunt punctele cele mai slabe pe care le are Republica Moldova astăzi.

Fig. 4 Performanța Republic Moldova în GCI pentru anul 2020



Domenii relativ consolidate:
Măsurile legale și tehnice

Domenii cu potențial de creștere:
Măsurile organizaționale și dezvoltarea capacităților

Scorul total	Măsurile legale	Măsurile tehnice	Măsurile organizaționale	Dezvoltarea capacităților	Măsuri de cooperare
75,78	16,73	16,86	13,21	13,09	15,89

De asemenea, trebuie să evidențiem că Republica Moldova este evaluată și în ceea ce privește maturitatea în domeniul securității cibernetice prin intermediul Indicelui Național de Securitate Cibernetică (NCSI)[7]. Acest indice este global și în timp real, și măsoară pregătirea țărilor pentru a preveni amenințările cibernetice și a gestiona incidentele cibernetice. Potrivit acestuia, există restanțe semnificative în ceea ce privește dezvoltarea politicilor de securitate cibernetică, analiza amenințărilor cibernetice și a informațiilor, protecția serviciilor digitale, cooperarea militară în domeniul cibernetic, care au un nivel sub 30%, iar protecția serviciilor esențiale și managementul crizelor de securitate cibernetică au o valoare de 0%.

Prin urmare, poate fi concluzionat că asigurarea securități cibernetice este vitală și sunt necesare să se ia măsuri pentru asigurarea unei protecții corespunzătoare a sistemelor și rețelelor informatice de amenințările cibernetice în continuă creștere. În special, este necesară o consolidare a sectorului cibernetic și o dezvoltare a capacităților naționale în acest domeniu, inclusiv prin instituirea unei autorități competente în acest sector care să includă un CSIRT național. Aceasta ar îmbunătăți gestionarea incidentelor cibernetice la nivel național și ar permite o cooperare mai bună între diferitele entități implicate în domeniul securității cibernetice, inclusiv cu sectorul privat. În plus, este important să se investească în instruirea inițială și continuă a personalului, astfel încât acesta să dispună de calificările suficiente și necesară pentru a-l face capabil să răspundă corespunzător la amenințările cibernetice în evoluție.

c) Expuneți clar cauzele care au dus la apariția problemei

[7] https://ncsi.ega.ee

Cauzele care au dus la apariția problemei protecției insuficiente împotriva incidentelor, riscurilor și amenințărilor legate de securitatea rețelelor și a sistemelor informatice în Republica Moldova sunt următoarele:

- ***Capacități insuficiente în cadrul autorităților în materie de securitate cibernetică***. Acest lucru se datorează lipsei de specialiști și de resurse necesare pentru a construi o infrastructură adecvată pentru a preveni incidentele cibernetice și pentru a răspunde la acestea. În plus, autoritățile nu sunt întotdeauna pregătite să abordeze problemele de securitate cibernetică din cauza lipsei de cunoștințe și experiență în domeniu;
- ***Insuficiența unor mecanisme normative, instituționale și operaționale care să permită monitorizarea situației privind infrastructura informațională critică a sectorului privat***. Aceasta se datorează în mare măsură absenței unui cadru legal (unor obligații minime necesare pentru asigurarea securității cibernetice) și a unei politici clare pentru securitatea cibernetică, ceea ce face dificilă dezvoltarea și implementarea unor politici și măsuri adecvate pentru protejarea infrastructurii informaționale critice a sectorului privat;
- ***Cooperare insuficientă dintre actorii implicați în materie de securitate cibernetică***. Aceasta este cauzată de o lipsă de coordonare în ceea ce privește eforturile de protejare a rețelelor și sistemelor informatice împotriva incidentelor, riscurilor și amenințărilor cibernetice. În plus, cooperarea insuficientă între acești actori duce la o lipsă de informații și resurse pentru a aborda/reacționa la problemele din domeniul securității cibernetice;
- ***Schimb de informații insuficient în sectorul public***. Schimbul de informații între instituțiile publice în ceea ce privește incidentele, vulnerabilitățile, riscurile și amenințările cibernetice este insuficient. Aceasta se datorează lipsei unor canale de comunicare adecvate și a unui cadru legal care să prescrie/impună acest schimb de informații. De asemenea, lipsa de încredere între autoritățile/instituțiile publice poate face dificilă partajarea informațiilor și poate duce la o lipsă de coordonare în eforturile de asigurare a securității rețelelor și sistemelor informatice împotriva incidentelor cibernetice;
- ***Lipsa schimbului de informații obligatoriu la nivelul sectorului privat despre incidentele cibernetice cu impact semnificativ în rețelele și sistemele informatice utilizate în prestarea serviciilor esențiale pentru susținerea unor activități societale și economice critice.*** În sectorul privat din Republica Moldova nu există un mecanism obligatoriu de raportare a incidentelor cibernetice, ceea ce duce la lipsa informațiilor și analizelor despre evenimentele produse în spațiul cibernetic al Republicii Moldova. Aceasta la rândul său generează incapacitatea cronică de a reacționa prompt la acestea. În plus, lipsa de schimb de informații sau un schimb de informații nesistemic îngreunează procesul de coordinare dintre sectorul privat și cel public în prevenirea și răspunsul la incidentele cibernetice.

Aceste cauze la rândul lor sunt generate de ***lipsa unei autorități competente responsabile de interacțiune în domeniul securității cibernetice***. Astfel, nu există o entitate centrală care să se ocupe de supravegherea și coordonarea proceselor de securitate cibernetică la nivel național. În acest context, autoritățile și instituțiile publice și private sunt lăsate să-și asume responsabilitatea pentru propriile lor sisteme și rețele, dar fără o direcție clară și fără suportul necesar pentru a aborda amenințările cibernetice.

În plus, furnizorii de servicii esențiale pentru funcționarea economiei digitale ar trebui să se supună unor norme și reglementări specifice pentru a asigura protecția datelor, a rețelelor și a sistemelor lor informatice. În lipsa unei autorități responsabile, monitorizarea respectării acestor reguli devine o sarcină dificilă și costisitoare pentru fiecare organizație în parte.

Lipsa unei autorități competente generează o lipsă de coordonare a proceselor de asigurare a securității cibernetice, inclusiv prevenirea și soluționarea incidentelor cibernetice, controlul, monitorizarea și analiza amenințărilor și vulnerabilităților cibernetice la nivel național. Aceasta ar trebui să ofere, de asemenea, asistență furnizorilor de servicii în procesul de monitorizare a propriilor lor rețele și sisteme informatice, oferind îndrumări metodologice și suportul necesar pentru a se conforma cu cerințele legale și reglementările specifice.

În lipsa unei astfel de autorități, procesul de asigurare a securității cibernetice la nivel național este fragmentat, costisitor și mai puțin eficient.

d) Descrieți cum a evoluat problema și cum va evolua fără o intervenție

Asigurarea securității informaționale a țării a constituit una din preocupările majore de mai mult timp și aceasta se întâlnește tot mai frecvent, în contextul transformării digitale a țării. Această preocupare a fost reflectată în diferite documente de politici ca parte componentă a procesului de dezvoltare a societății informaționale în Republica Moldova, cum ar fi Strategia Națională de edificare a societății informaționale "Moldova electronică", Strategia națională de dezvoltare a societății informaționale "Moldova Digitală 2020" sau Programul de modernizare tehnologică a Guvernării.

Cu toate acestea, o atenție mai pronunțată față de domeniul securității cibernetice a fost acordată abia în 2017, prin adoptarea de către Parlament a Concepției securității informaționale a Republicii Moldova, unul din obiectivele de bază ale căreia este dezvoltarea capacităților de reziliență informațională și cibernetică. Acest document a fost însă precedat de adoptarea de către Guvern în anul 2015, a Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020. Obiectivul principal al acestuia a fost crearea unui sistem de management al securității cibernetice prin securizarea serviciilor societății informaționale, în vederea contribuirii la dezvoltarea unei economii bazate pe cunoaștere. Aceleași obiective au fost dezvoltate și în Strategia securității informaționale a Republicii Moldova 2019-2024.

Deși au fost întreprinse acțiuni în conformitate cu aceste documente de politici, nu s-a reușit determinarea la nivel național a unei autorități competente în domeniul securității cibernetice și crearea unei echipe de răspuns la incidente cibernetice la nivel național. Această situație limitează autoritățile publice responsabile în realizarea misiunii lor și expune sectorul public și privat, precum și societatea în general la riscuri majore în ceea ce privește amenințările de securitate cibernetică.

Totodată, lipsa unei intervenții de politici poate avea un impact negativ considerabil asupra economiei și securității naționale, afectând toți actorii din societate, inclusiv mediul de afaceri, cetățenii și entitățile critice.

În ceea ce privește sectorul economic, vulnerabilitatea la incidente de securitate cibernetică poate afecta afacerile prin pierderi financiare și daune reputaționale. Aceste probleme pot afecta în special afacerile mici și mijlocii, care pot fi mai puțin capabile să își permită să investească în securitatea cibernetică și pot fi mai vulnerabile la atacuri cibernetice.

În ceea ce privește sectorul securității naționale, vulnerabilitatea la incidente de securitate cibernetică poate afecta capacitățile de informații și infrastructurile critice ale unei țări. Atacurile cibernetice pot fi utilizate pentru spionaj, sabotaj sau chiar pentru a lansa atacuri împotriva infrastructurilor critice, cum ar fi rețelele de electricitate sau gaze. Aceste atacuri pot avea un impact semnificativ asupra securității și stabilității unei țări.

În cazul în care nu există un răspuns corespunzător la incidentele de securitate cibernetică, consecințele pot fi și mai grave. Acest lucru poate duce la o creștere a numărului și a gravității atacurilor cibernetice, precum și la o creștere a costurilor și a timpului necesar pentru a remedia problemele. În plus, lipsa unui răspuns corespunzător poate duce la pierderi de informații sensibile și la o creștere a riscului de fraude și infracțiuni.

În ceea ce privește entitățile critice, vulnerabilitățile acestora la incidentele cibernetice pot fi exploatate de amenințări care odată materializate ar putea afecta furnizarea unor servicii esențiale și, pe cale de consecință, producerea unor prejudicii considerabile asupra economiei și societății în general.

La rândul lor, toate aceste consecințe pot duce la o serie mai largă de efecte negative, care are putea consta în diminuarea încrederii în instituțiile statului și în sectorul economic. Lipsa încrederii în instituțiile statului și în stat pe arena internațională cauzată de incapacitatea acestora de a asigura securitatea cibernetică și de a proteja datele și infrastructurile critice împotriva atacurilor cibernetice poate duce la o imagine negativă a țării în ochii altor state și organizații internaționale, ceea ce poate submina relațiile diplomatice și comerciale. Iar subminarea încrederii în sectorul economic al Republicii Moldova cauzată de vulnerabilitatea la atacurile cibernetice și de incapacitatea companiilor de a-și proteja datele și infrastructurile critice poate duce la pierderea încrederii consumatorilor și a investitorilor, ceea ce poate afecta negativ afacerile și economia în general. Investițiile scăzute a sectorului privat și public în securitatea cibernetică, cauzată de lipsa de conștientizare și de prioritizare a securității cibernetice în țară, poate avea ca efect insuficiența resurselor necesare implementării măsurilor de asigurare a securității cibernetice și dezvoltării capacităților minime pentru a face față amenințărilor cibernetice.

Astfel, aceste consecințe pot avea un impact negativ semnificativ asupra dezvoltării economice și sociale a țării, precum și asupra relațiilor internaționale ale acesteia. Pentru a preveni aceste consecințe, este important ca statul să ia măsuri pentru a asigura securitatea cibernetică și pentru a încuraja investițiile în acest domeniu atât din partea sectorului privat, cât și din partea sectorului public.

e) Descrieți cadrul juridic actual aplicabil raporturilor analizate și identificați carențele prevederilor normative în vigoare, identificați documentele de politici și reglementările existente care condiționează intervenția statului

Cadrul de politici și cadrul normativ

Cadrul de politici de securitate cibernetică este oferit de un set de documente de politici publice adoptate de Parlament sau Guvern și care oferă viziunea strategică pentru țară cu privire la modul de înființare, consolidare și asigurare a rezilienței sistemului de securitate cibernetică pentru spațiul informațional al Republica Moldova.

Din perspectiva **cadrului strategic** următoarele documente de politici cuprind obiective ce condiționează intervenția statului:

Concepția securității informaționale[8], aprobată prin Legea nr. 299/2017

Concepția reprezintă o viziune de ansamblu asupra scopului, obiectivelor, principiilor și direcțiilor de bază ale activității de asigurare a unui nivel înalt al securității informaționale a Republicii Moldova, securitatea informațională fiind parte componentă a sistemului național de securitate. Potrivit acestei concepții măsurile de prevenire, depistare și contracarare a amenințărilor complexe și persistente la adresa securității informaționale pot fi întreprinse doar cu condiția existenței și funcționării unui cadru normativ corespunzător în domeniu, a unor instrumente și metode bine definite, a unor mecanisme de colaborare la nivel național și internațional. Concepția securității informaționale a Republicii Moldova este determinată de necesitatea protejării intereselor statului, ale societății și ale persoanei, a obiectivelor vitale și de importanță strategică pentru securitatea națională, de necesitatea asigurării protecției informației atribuite la secret de stat, precum și de necesitatea prevenirii și combaterii criminalității informatice.

Concepția constituie baza pentru elaborarea Strategiei securității informaționale a Republicii Moldova și a Planului de acțiuni pentru implementarea strategiei respective. În primul capitol Concepția descrie situația în domeniu și definește problemele din acest sector, stabilește obiectivele de bază, amenințările la adresa securității informaționale, realizarea cărora are ca scop asigurarea protecției, în spațiul informațional, a drepturilor și libertăților fundamentale, a democrației și a statului de drept. În partea a doua Concepția descrie instrumentele și căile de soluționare a problemelor identificate, inclusiv direcțiile strategice și tactice de asigurare a securității informaționale, principiile și principalele sarcini ale autorităților competente, metodele de asigurare a securității informaționale (juridice, tehnico-organizatorice, economice, contrainformative și de securitate), cooperarea internațională în acest

[8] https://www.legis.md/cautare/getResults?doc_id=105660&lang=ro

domeniu și organizarea sistemului de asigurare a securității informaționale. În ce privește aspectul organizării sistemului respectiv, concepția desemnează Serviciul de Informații și Securitate ca fiind, în limitele competenței atribuite prin lege autoritatea națională de coordonare a activității autorităților publice desfășurate în domeniul securității informaționale.

Strategia securității informaționale[9] a Republicii Moldova pentru anii 2019-2024 și Planul de acțiuni pentru implementarea acesteia, aprobate prin Hotărârea Parlamentului nr. 257/2018

După cum s-a menționat mai sus, Concepția securității informaționale reprezintă documentul de bază pentru elaborarea acestei Strategii și documentul de politici ce integrează domeniile centrale și asociate spațiului informațional, ce oferă noțiuni, definește principiile de organizare la nivel de stat, societate și persoană, precum și detaliază metodele juridice, tehnico-organizatorice, economice și contrainformative pentru asigurarea securității informaționale a Republicii Moldova. În acest context, **scopul principal** al Strategiei securitate informațională este de a lega și integra din punct de vedere juridic domeniile prioritare cu responsabilități și competențe de asigurare a securității informațiilor la nivel național, bazată inclusiv pe reziliența cibernetică. Scopul și obiectivele acestei Strategii se realizează în baza Planului de acțiuni pentru implementarea acesteia. Astfel, în contextul definirii problemelor și al descrierii situației la momentul adoptării strategiei, acest document evidențiază un spectru larg de probleme cu care se confruntă până acum Republica Moldova. Problemele abordate de Strategie se referă la cinci componente de bază ale securității cibernetice și investigației criminalității cibernetice, securitatea spațiului media, componenta de contrainformații și securitate, aspectele juridice și, în final, problemele de conștientizare a maselor. Dintre acestea, Strategia evidențiază problemele cele mai proeminente cum ar fi lipsa unui CERT național (Centrul de răspuns la incidente de securitate cibernetică), responsabil de prevenirea și răspunsul la incidente din domeniul securității cibernetice la scară largă la nivel național, lipsa unui sistem integrat de management al securității cibernetice și un mecanism viabil de audit al securității cibernetice, precum și lipsa de specialiști calificați, programe de formare specializată adresate angajaților organelor de drept, dotarea insuficientă cu echipamente și software, finanțare redusă pentru participarea specialiștilor la proiecte internaționale și evenimente pentru consolidarea capacităților și schimbul de bune practici etc. Strategia include mai multe cerințe fundamentale pentru a obține o mai bună guvernare a securității cibernetice la nivel național, precum și o listă de acțiuni propuse și indicatori de progres.

Diverse aspecte ale securității cibernetice sunt abordate și în ***alte documente de politici***, interconectate cu Strategia securității informaționale, cum sunt:

- Strategia de securitate națională, aprobată prin Hotărârea Parlamentului nr. 153/2011[10]
- Strategia Națională de Apărare și Planul de Acțiuni privind implementarea Strategiei Naționale de Apărare 2018–2022, aprobate prin Hotărârea Parlamentului nr. 134/2018[11]
- Planul individual de acțiuni de parteneriat Republica Moldova – NATO pentru anii 2022–2023, aprobat prin Hotărârea Guvernului nr. 26/2022[12].

Cadrul normativ

În domeniul administrației publice, potrivit art. 107 din **Constituția Republicii Moldova**, organele centrale de specialitate ale statului sunt ministerele, acestea au responsabilitatea de a conduce domeniile încredințate și sunt responsabile de activitatea lor. Totodată, în scopul conducerii, coordonării și exercitării controlului în domeniul organizării economiei și în alte domenii care nu intră nemijlocit în atribuțiile ministerelor, se înființează, în condițiile legii, și alte autorități administrative.

Legea nr. 98/2012 privind administrația publică centrală de specialitate stabilește sistemul instituțional al administrației publice centrale de specialitate și reglementează regimul general al activității acesteia, principiile fundamentale de organizare și funcționare a administrației publice

[9] https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro
[10] https://www.legis.md/cautare/getResults?doc_id=105346&lang=ro
[11] https://www.legis.md/cautare/getResults?doc_id=110013&lang=ro
[12] https://www.legis.md/cautare/getResults?doc_id=129865&lang=ro

centrale de specialitate, precum și raporturile juridice care decurg din activitatea ministerelor, a Cancelariei de Stat și a altor autorități administrative centrale.

Structura organizatorică a sistemului administrativ guvernamental este determinată de natura competenței, funcțiilor și atribuțiilor ce urmează a fi exercitate de către autoritățile publice constituite în subordinea Guvernului. Astfel, potrivit art. 3 și art. 14 din Legea respectivă, pentru asigurarea implementării politicii statului în anumite subdomenii sau sfere din domeniile de activitate care îi sunt încredințate unui minister, pot fi create autorități administrative în subordinea acestuia.

Potrivit art. 7 al **Legi nr. 136/2017 cu privire la Guvern**, acesta este împuternicit de a stabili modul de organizare și funcționare, domeniile de activitate, structura și efectivul-limită ale ministerelor, ale altor autorități administrative centrale subordonate Guvernului și ale structurilor organizaționale din sfera lor de competență, coordonează și controlează activitatea acestora, precum și înființează în subordinea sa alte autorități administrative centrale pentru realizarea politicii statului într-un domeniu de activitate care nu intră în competența nemijlocită a ministerelor, precum și în domenii de activitate în care competențele ministerelor se intersectează, precum și le reorganizează și dizolvă.

În domeniul securității cibernetice, la nivel național, **Legea nr. 48/2023 privind securitatea cibernetică** reprezintă cadrul normativ primar în domeniul securității cibernetice. Implementarea cerințelor, măsurilor și mecanismelor instituite în această lege are ca obiectiv să garanteze un nivel înalt de securitate a rețelelor și sistemelor informatice din Republica Moldova, oferind protecție pentru interesele vitale ale persoanelor fizice și juridice, ale societății și ale statului, precum și ale intereselor naționale ale Republicii Moldova.
În acest context, legea prevede:

- desemnarea de către Guvern a unei autorități competente în domeniul securității cibernetice cu funcții de identificare a persoanelor juridice care vor intra în cercul de subiecți asupra cărora se vor răsfrânge prevederile legale (furnizori de servicii) și menținerea în stare de actualitate a unei liste a furnizorilor de servicii și funcții de supraveghere și control a măsurilor de securitate pe care furnizorii de servicii trebuie să le implementeze pentru a asigura un nivel adecvat de securitate a rețelelor și sistemelor lor informatice, de stabilire a unor practici comune în gestionarea incidentelor cibernetice și de coordonare operațională a situațiilor de criză, de cooperare și interacțiune la nivel național și internațional și de schimb de experiență cu organizații, state sau alte entități relevante la nivel european în primul rând;
- instituirea în cadrul autorității competente, a unei echipe de răspuns la incidentele de securitate cibernetică (CSIRT) cu competențe la nivel național care să exercite atribuții de monitorizare și analiză a amenințărilor cibernetice, vulnerabilităților și incidentelor cibernetice, de răspuns la incidente cibernetice, de asigurare a schimbului de informații și coordonare a procesului de divulgare a vulnerabilităților;
- definirea cadrului general strategic și operațional de coordonare și cooperare dintre sectorul public și privat în domeniul securității cibernetice, inclusiv în ce privește gestionarea crizelor, și aprobarea unui plan național de răspuns care să asigure pregătirea capacității de reacție și a recuperării în caz de incidente cibernetice și/sau crize de securitate cibernetică. În același context, legea cuprinde norme juridice primare care vor avea ca efect aprobarea de către Guvern a Strategiei naționale privind securitatea cibernetică și instituirea Consiliului coordonator în domeniul securității cibernetice;
- instituirea obligațiilor de a implementa măsuri de securitate de către furnizorii de servicii esențiale, privați și publici, pentru funcționarea economiei și a societății, care să asigure atingerea unui nivel minim comun de securitate a rețelelor și sistemelor informaționale și reziliența serviciilor, ceea ce implicit va avea ca efect pozitiv asupra creșterii nivelului de pregătire și de răspuns la incidentele și amenințările cibernetice;
- implementarea unui mecanism obligatoriu de raportare a incidentelor cibernetice cu impact semnificativ de către furnizorii de servicii, și crearea unui regim de notificare voluntară a incidentelor cibernetice de către orice categorii de persoane;
- crearea și asigurarea funcționării adecvate a mecanismelor de cooperare eficiente la nivel național și internațional, prin difuzarea de către autoritatea competentă întregii societăți și în mod

deosebit entităților ce furnizează servicii în domenii critice, a informațiilor relevante, a avertizărilor și alertelor, precum și a celor mai bune practici internaționale;

- stabilirea unui mecanism de supraveghere și control de către autoritatea competentă a modului în care furnizorii de servicii implementează măsurile de securitate cibernetică și asigură raportarea incidentelor cibernetice cu impact semnificativ.

Legea privind securitatea cibernetică a fost adoptată de Parlament la data de 16 martie 2023 și publicată în Monitorul Oficial la data de 28 aprilie 2023. Odată cu publicarea legii a început curgerea termenelor de implementare a acesteia stabilite de art. 23. Astfel, până la data de 1 ianuarie 2025, data intrării în vigoare a legii, Guvernul urmează să realizeze un complex de măsuri organizatorice, normative și tehnice orientate spre punerea în aplicare a normelor legale, în mod special:

- aducerea legilor actuale în concordanță cu prevederile Legii privind securitatea cibernetică;
- adoptarea actelor normative subsidiare și aducerea în concordanță cu prevederile legii a cadrului normativ propriu;
- desemnarea/instituirea autorității competente, inclusiv a CSIRT național, asigurarea acesteia cu resurse, inclusiv financiare, etc.

Până la intrarea în vigoare a Legii privind securitatea cibernetică chestiunile privind asigurarea securității cibernetice sunt reglementate disparat în diverse legi și acte normative ale Guvernului.

Astfel, ***Legea nr. nr 467/2003***[13] ***cu privire la informatizare si resursele informaționale de stat*** (art.23) și **Legea nr. 71/2007**[14] **cu privire la registre** (art.24) reglementează, pe de o parte, responsabilitățile autorităților publice în asigurarea securității cibernetice a sistemelor și resurselor informaționale ale statului, iar pe de altă parte, responsabilitățile entităților, inclusiv private, în protecția informațiilor conținute de resursele și prelucrate de sistemele informaționale pe care le creează.

În același timp, cerințele de securitate pentru rețelele publice de comunicații electronice și serviciile de comunicații electronice accesibile publicului sunt prevăzute la articolele 21 și 22 din ***Legea comunicațiilor electronice nr. 241/2007***[15]. Această lege reglementează activitatea în domeniul comunicațiilor electronice civile a tuturor furnizorilor de rețele sau servicii de comunicații electronice, fie din sectorul public sau privat, și stabilește drepturile și obligațiile utilizatorilor. Legea nu se extinde la rețelele de comunicații speciale. Din punct de vedere al securității rețelelor și serviciilor de comunicații electronice, Agenția Națională pentru Reglementare în Comunicațiile Electronice și Tehnologia Informației este responsabilă de implementarea măsurilor minime de securitate pe care toți furnizorii ar trebui să le implementeze. Agenția poate verifica și evalua măsurile stabilite de furnizori pentru a garanta securitatea și integritatea rețelelor și serviciilor de comunicații electronice.

De asemenea, **Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate** are ca scop să faciliteze și să eficientizeze schimbul de date și interoperabilitatea în cadrul sectorului public, precum și între sectorul public și cel privat, în vederea creșterii calității serviciilor publice prestate, a creării noilor servicii publice electronice și a asigurării securității informaționale.

Pentru punerea în aplicare a acestor legi, Guvernul a aprobat:

- **Hotărârea Guvernului nr. 201/2017**[16] privind aprobarea cerințelor minime obligatorii de securitate cibernetică, care se adresează atât autorităților guvernamentale, cât și autorităților care nu intră în structura administrativă a Guvernului;
- **Hotărârea Guvernului nr. 482/2020** [17]privind aprobarea măsurilor necesare asigurării securității cibernetice la nivel guvernamental, care completează, în special, cu măsuri organizatorice

[13] https://www.legis.md/cautare/getResults?doc_id=132933&lang=ro
[14] https://www.legis.md/cautare/getResults?doc_id=131038&lang=ro
[15] https://www.legis.md/cautare/getResults?doc_id=133262&lang=ro
[16] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro
[17] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro

decizia sus-menționată, dar numai pentru autoritățile și instituțiile publice care fac parte din structura administrativă guvernamentală;

- **Hotărârea Guvernului nr. 388/2022**[18] privind aprobarea Concepției Sistemului Informațional „Registrul de Stat al Incidentelor de Securitate Cibernetică", este una dintre măsurile preliminare pentru stabilirea unei platforme informaționale pentru comunicarea strategică cu entitățile publice, precum și pentru asigurarea evidenței amenințărilor, vulnerabilităților în spațiul cibernetic. și incidente de securitate cibernetică identificate sau raportate.

Bineînțeles, actele normative menționate urmează să constituie obiectul unei analize aprofundate pentru relevarea normelor ce sunt în contradicție cu prevederile Legii nr. 48/2023 și, dacă e cazul, aducerea corespunzătoare a acestora în concordanță cu noul cadru legal în domeniul securității cibernetice.

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.

Consiliul Coordonator pentru Asigurarea Securității Informaționale a fost înființat prin Hotărârea Guvernului nr. 467/2022[19]. Acest organism colectiv, cu atribuții consultative și operaționale, a fost instituit pentru integrarea sistemică a entităților participante în spațiul informațional și susținerea unui nivel înalt de securitate informațională, inclusiv securitate cibernetică. Activitatea Consiliului se concentrează pe patru niveluri: cibernetic, operațional, mass-media și civic-privat. Consiliul monitorizează activitatea persoanelor juridice de drept public și privat responsabile cu implementarea Planului de acțiuni pentru implementarea Strategiei securității informaționale. Activitatea consultativă se desfășoară la nivelul Consiliului între membrii constitutivi în cadrul ședințelor ordinare sau extraordinare, pe teme axate pe asigurarea securității informaționale și cibernetice. Activitatea operațională constă în finalizarea de către Consiliu a complexului de măsuri de reacție la pericole, riscuri și amenințări ale securității informaționale și cibernetice, implementarea acțiunilor necesare de către persoane juridice, atât publice, cât și private, la nivelul departamentului, interinstituțional, sectorial, intersectorial sau național, conform cadrului normativ care reglementează activitatea componentelor societății informaționale. Secretariatul Consiliului este asigurat de Cancelaria de Stat.

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 echipamente de comunicații electronice.

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 implementează politica de securitate cibernetică.[20] În cadrul STISC funcționează **CERT-Gov**[21]. CERT-Gov[22] este un CSIRT guvernamental, adică o echipă responsabilă numai pentru sisteme și rețele informatice de stat. Activitatea acestei entități se concentrează pe coordonare, formare și alte funcții administrative. Activitățile lor de răspuns la incidente sunt limitate din cauza lipsei de oameni cu

[18] https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro
[19] https://www.legis.md/cautare/getResults?doc_id=132064&lang=ro
[20] https://www.legis.md/cautare/getResults?doc_id=128904&lang=ro
[21] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro
[22] https://stisc.gov.md/ro/cert-gov-md

cunoștințe tehnice de specialitate puternice, dar și din cauza insuficienței echipamentelor tehnice și a cadrului normativ deficitar. În principiu CERT-Gov acționează ca punct național de contact național „de facto", deoarece oficial la nivel juridico-normativ încă nu a fost stabilit un CERT național.

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 platforma 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 [23]. Conform regulamentului său de activitate, principalele responsabilități ale Agenției în domeniul securității cibernetice sunt auditul securității cibernetice în sectorul public, inclusiv monitorizarea implementării rezultatelor auditului securității cibernetice, cercetarea securității cibernetice, precum și supravegherea instituțiilor publice în ceea ce privește implementarea cerințelor minime de securitate.

Serviciul de Securitate și Informații (SIS) are un rol important în protejarea infrastructurii critice din țară, precum și a sistemelor speciale de telecomunicații [24]. Cu toate acestea, în prezent, SIS se concentrează pe securitatea fizică și mai puțin pe aspectele de securitate cibernetică. Responsabilitățile diferitelor instituții sunt în discuție, întrucât SIS așteaptă legislația de la Ministerul Dezvoltării Economice și Digitalizării privind protecția infrastructurii informaționale critice. Potrivit pct. 115 din Strategia securității informaționale a Republicii Moldova pentru anii 2019-2024, Serviciul de Securitate și Informații are rolul principal în procesul de monitorizare și coordonare a implementării Strategiei securității informaționale și a Planului de acțiuni al acesteia.

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.

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.

Agenția Națională pentru Reglementare în Comunicații Electronice și Tehnologia Informației[25] (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[26]. Cu toate acestea, această entitate este autonomă față de Guvern în activitatea sa de reglementare. Potrivit legii, Agenția aprobă regulile [27]de implementare a măsurilor minime de securitate și integritate a rețelelor publice de comunicații electronice și/sau a serviciilor de comunicații electronice accesibile publicului, precum și elaborează reglementări privind administrarea domeniului de nivel superior .md.[28]

[23] http://www.egov.md/en/about
[24] https://www.legis.md/cautare/getResults?doc_id=129284&lang=ro
[25] https://en.anrceti.md/informatie_sumara
[26] https://www.legis.md/cautare/getResults?doc_id=125209&lang=ro
[27] https://www.legis.md/cautare/getResults?doc_id=119924&lang=ro
[28] https://en.anrceti.md/node/35

Ministerul Apărării este implementatorul Strategiei Naționale de Apărare pentru anii 2018-2021. Strategia menționează și activități de apărare cibernetică. Armata moldovenească își dezvoltă însă doar propriile capacități defensive și CERT-ul său departamental pentru a-și proteja propriile rețele.

2. Stabilirea obiectivelor

a) Expuneți obiectivele (care trebuie să fie legate direct de problemă și cauzele acesteia, formulate cuantificat, măsurabil, fixat în timp și realist)

Obiectiv general:

Capacitățile de prevenire și răspuns la incidente și crize cibernetice la nivel național dezvoltate și cooperarea internațională în acest domeniu instituită și consolidată.

Obiective specifice:

1. Autoritatea competentă în domeniul securității cibernetice este deplin funcțională până la data de 27 ianuarie 2024;
2. Lista furnizorilor de servicii elaborată până la data de 27 iulie 2024;
3. Registrul de stat al incidentelor cibernetice deplin funcțional până finalizarea procesului de identificare a furnizorilor de servicii;
4. Echipa națională de răspuns la incidentele de securitate cibernetică (CSIRT) funcțională 24/7, până la data de 27 ianuarie 2024;
5. Relații de cooperare în materie de securitate cibernetică stabilite cu cel puțin 5 echipe de răspuns la incidente de securitate cibernetică din 5 state membre ale Uniunii Europene, până la 31 decembrie 2025.

3. Identificarea opţiunilor

a) Expuneți succint opțiunea „a nu face nimic”, care presupune lipsa de intervenție

În Republica Moldova, securitatea cibernetică este o problemă majoră, iar lipsa unei intervenții de politici poate avea un impact negativ semnificativ asupra economiei și securității naționale. Deși s-au adoptat documente de politici și s-au întreprins acțiuni, nu s-a reușit încă crearea sau stabilirea unei autorități competente în domeniul securității cibernetice la nivel național. Aceasta expune sectorul public și privat, precum și societatea în general la riscuri majore în ceea ce privește amenințările de securitate cibernetică.

În ceea ce privește sectorul economic, vulnerabilitatea la incidente de securitate cibernetică poate afecta afacerile prin pierderi financiare, daune reputaționale, pierderea de date și creșterea costurilor de securitate cibernetică. Aceste probleme pot afecta în special afacerile mici și mijlocii, care pot fi mai puțin capabile să își permită să investească în securitatea cibernetică și pot fi mai vulnerabile la atacuri cibernetice.

În ceea ce privește sectorul securității naționale, vulnerabilitatea la incidente de securitate cibernetică poate afecta capacitățile de informații și infrastructurile critice ale unei țări. Atacurile cibernetice pot fi utilizate pentru spionaj, sabotaj sau chiar pentru a lansa atacuri împotriva infrastructurilor critice, cum ar fi rețelele de electricitate sau gaze.

În cazul în care nu există un răspuns corespunzător la incidentele de securitate cibernetică, consecințele pot fi și mai grave. Acest lucru poate duce la o creștere a numărului și a gravității atacurilor cibernetice, precum și la o creștere a costurilor și a timpului necesar pentru a remedia problemele. În plus, lipsa unui răspuns corespunzător poate duce la pierderi de informații sensibile și la o creștere a riscului de fraude și infracțiuni.

În ceea ce privește entitățile critice, cum ar fi furnizorii de electricitate sau gaze, vulnerabilitatea la incidente de securitate cibernetică poate afecta furnizarea de energie și poate duce la întreruperi semnificative ale serviciilor. Aceste probleme pot avea un impact negativ semnificativ asupra economiei și a vieții cetățenilor.

Astfel este necesar să se ia măsuri pentru a consolida securitatea cibernetică în Republica Moldova prin crearea unei autorități naționale competente în domeniul securității cibernetice, implementarea strategiilor și a politicilor corespunzătoare și prin creșterea gradului de conștientizare și educare a cetățenilor.

Ori, în cazul lipsei în continuare a unei autorități competente la nivel național în acest domeniu și absența unor obligații legale pentru entitățile critice de a implementa măsuri de securitate bazate pe rezultatele evaluării riscurilor conduc la o serie de consecințe negative.

În sectorul privat, neinstituirea unei autorități competente în securitatea cibernetică poate duce la o neacoperire a acestui sector în ceea ce privește protecția împotriva amenințărilor cibernetice. Afacerile, în special cele mici și mijlocii, care pot fi mai vulnerabile și mai puțin capabile să investească în securitatea cibernetică, se expun riscului de pierderi financiare, daune reputaționale, pierderi de date și creșteri ale costurilor de securitate cibernetică. Aceasta poate afecta în mod direct economia națională și poate duce la scăderea încrederii investitorilor în sectorul privat.

În ceea ce privește securitatea națională, absența unei autorități competente în securitatea cibernetică la nivel național creează vulnerabilități majore în capacitățile de informații și în infrastructurile critice ale țării. Aceasta deschide calea pentru atacuri cibernetice utilizate în scopuri de spionaj, sabotaj sau chiar atacuri asupra infrastructurilor critice, cum ar fi rețelele de electricitate sau gaze. Lipsa pârghiilor legale pentru autoritățile competente de a influența situația în sectorul privat limitează capacitatea de prevenire și de răspuns la aceste amenințări cibernetice, crescând astfel riscul asupra securității naționale.

În lipsa unui răspuns coordonat corespunzător la incidentele de securitate cibernetică, consecințele pot deveni și mai grave. Se poate înregistra o creștere a numărului și a gravității atacurilor cibernetice, ceea ce duce la costuri și timp mai mari pentru remedierea problemelor. Pierderile de informații sensibile pot avea consecințe pe termen lung, cu un risc crescut de fraude și infracțiuni. Toate acestea amenință securitatea națională și pot avea un impact negativ semnificativ asupra economiei și vieții cetățenilor.

În concluzie, neinstituirea unei autorități competente la nivel național în domeniul securității cibernetice, lipsa obligațiilor legale pentru furnizorii de servicii critice și modelul organizatoric de guvernanță actual defectuos reprezintă o amenințare majoră pentru securitatea cibernetică în Republica Moldova. Este necesară intervenția urgentă pentru a consolida securitatea cibernetică prin instituirea unei autorități competente, implementarea strategiilor și politicilor adecvate, precum și prin creșterea gradului de conștientizare și educare a cetățenilor.

b) Expuneți principalele prevederi ale proiectului, cu impact, explicând cum acestea țintesc cauzele problemei, cu indicarea novațiilor și întregului spectru de soluții/drepturi/obligații ce se doresc să fie aprobate

Opțiunea recomandată presupune crearea unei autorități administrative responsabile de implementarea politicii în domeniul securității cibernetice în subordinea autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice.

Potrivit art. 107 din Constituția Republicii Moldova, organele centrale de specialitate ale statului sunt ministerele, acestea au responsabilitatea de a conduce domeniile încredințate și sunt responsabile de activitatea lor. Totodată, în scopul conducerii, coordonării și exercitării controlului în domeniul organizării economiei și în alte domenii care nu intră nemijlocit în atribuțiile ministerelor, se înființează, în condițiile legii, și alte autorități administrative.

În dezvoltarea acestor norme constituționale, Legea nr. 98/2012 privind administrația publică centrală de specialitate stabilește sistemul instituțional al administrației publice centrale de specialitate și reglementează regimul general al activității acesteia, principiile fundamentale de organizare și funcționare a administrației publice centrale de specialitate, precum și raporturile juridice care decurg din activitatea ministerelor, a Cancelariei de Stat și a altor autorități administrative centrale.

Structura organizatorică a sistemului administrativ guvernamental este determinată de natura competenței, funcțiilor și atribuțiilor ce urmează a fi exercitate de către autoritățile publice constituite în subordinea Guvernului. Astfel, potrivit art. 3 și art. 14 din Legea respectivă, pentru asigurarea implementării politicii statului în anumite subdomenii sau sfere din domeniile de activitate care îi sunt încredințate unui minister, pot fi create autorități administrative în subordinea acestuia.

Adițional, potrivit art. 7 al Legii nr. 136/2017 cu privire la Guvern, acesta este împuternicit de a stabili modul de organizare și funcționare, domeniile de activitate, structura și efectivul-limită ale ministerelor, ale altor autorități administrative centrale subordonate Guvernului și ale structurilor organizaționale din sfera lor de competență, coordonează și controlează activitatea acestora, precum și înființează în subordinea sa alte autorități administrative centrale pentru realizarea politicii statului într-un domeniu de activitate care nu intră în competența nemijlocită a ministerelor, precum și în domenii de activitate în care competențele ministerelor se intersectează, precum și le reorganizează și dizolvă.

La rândul său, Legea nr. 48/2023 privind securitatea cibernetică din punct de vedere organizațional și funcțional, reglementează prin norme speciale statutul juridic al autorității administrative (autoritate competentă) care urmează să fie desemnată de Guvern pentru exercitarea prerogativelor de putere publică în domeniul implementării laturii civile a politicii statului în domeniul securității cibernetice. Desemnarea în sensul legii urmează a fi înțeleasă fie ca instituirea unei autorități administrative noi pentru exercitarea competenței respective, fie ca atribuirea acestei competențe unei autorități existente.

Coroborând prevederile relevante ale legilor menționate mai sus și ținând cont de natura competenței ce urmează a fi exercitată de autoritatea competentă opțiunea recomandată pentru soluționarea problemelor identificate în prezenta analiză de impact este constituirea în sistemul administrativ al Ministerului Dezvoltării Economice și Digitalizării a unei autorități administrative.

Proiectul de act normativ are ca obiectiv constituirea, în sfera de competență a Ministerului Dezvoltării Economice și Digitalizării, a unei noi structuri organizaționale, cu formă de organizare juridică de agenție.

Astfel, proiectul include următoarele grupuri de reglementări:

În partea dispozitivă a hotărârii de Guvern sunt reglementate aspecte privind:

1) aprobarea Regulamentului cu privire la organizarea și funcționarea Agenției Naționale pentru Securitate Cibernetică;
2) aprobarea structurii Agenției Naționale pentru Securitate Cibernetică;
3) aprobarea efectivului limită a Agenției Naționale pentru Securitate Cibernetică;
4) stabilirea sarcinii pentru Ministerul Dezvoltării Economice și Digitalizării de a asigura, în termen 2 luni, organizarea concursului pentru ocuparea funcției de director și director adjunct al Agenției Naționale pentru Securitate Cibernetică și numirea în funcție a persoanelor desemnate drept câștigător al concursului;
5) stabilirea în sarcina directorului Agenției Naționale pentru Securitate Cibernetică cu suportul Ministerul Dezvoltării Economice și Digitalizării:

să înregistreze noua autoritate, să aprobe statele de personal, schema de încadrare și să le înregistreze în modul stabilit de legislație;

să constituie o comisie de concurs, în care, de rând cu directorul și directorul adjunct ai Agenției, să fie desemnați 3 reprezentanți ai Ministerului Dezvoltării Economice și Digitalizării, pentru a asigura componența minimă (5 membri) necesară conform cadrului normativ. Această Comisie va selecta 3 conducători de subdiviziuni structurale interne ale Agenției, ceea ce va permite ulterior directorului să constituie Comisia de concurs a Agenției în vederea selectării întregului personal al acesteia;

6) stabilirea sarcinii pentru Cancelaria de Stat, Ministerului Dezvoltării Economice și Digitalizării, în comun cu Agenția Proprietății Publice de a identifica și asigura transmiterea bunurilor necesare pentru activitatea Agenției Naționale pentru Securitate Cibernetică;

7) completarea pct. 6 din anexa nr. 1 la Hotărârea Guvernului nr. 143/2021 cu privire la organizarea și funcționarea Ministerului Dezvoltării Economice și Digitalizării cu domeniul securității cibernetice și anexa 4 a aceleași Hotărâri de Guvern cu Agenția Națională pentru Securitate Cibernetică.

Regulamentul cuprinde reglementări a componentei funcționale și a celei organizaționale, inclusiv: misiunea, domeniile de activitate, funcțiile, atribuțiile, drepturile și modul de organizare a autorității.

Structura organizațională a autorității este constituită din:

1. Direcția răspuns la incidente și crize cibernetice (CSIRT), care va fi exercita următoarele atribuții:

a) coordonează procesul de asigurare a securității cibernetice, de prevenire și de soluționare a incidentelor cibernetice;

b) monitorizează, analizează și, dacă e cazul, informează despre amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național;

c) acordă asistență furnizorilor de servicii, la solicitarea acestora, în procesul de monitorizare și protecție de către aceștia a rețelelor și sistemelor informatice pe care le dețin;

d) recepționează notificări privind incidentele cibernetice;

e) asigură răspunsul la incidentele cibernetice;

f) acordă asistență, în acest sens, furnizorilor de servicii;

g) cooperează, la nivel național și internațional, cu echipele de răspuns la incidentele cibernetice, inclusiv în cadrul unei platforme de management al incidentelor cibernetice și pentru schimbul de informații;

h) gestionează crizele în domeniul securității cibernetice la nivel național în conformitate cu planul de răspuns la incidente și crize cibernetice la nivel național;

i) ține evidența incidentelor cibernetice care i-au fost notificate;

j) monitorizează numele de domenii din spațiul de adrese în Internet al Republicii Moldova și legate de domeniul de nivel superior .md, analizează riscurile, precum și impactul potențial al acestora asupra statului, societății și securității rețelelor și sistemelor informatice;

k) asigură protecția informațiilor atribuite la secretul de stat, a datelor cu caracter personal în conformitate cu prevederile actelor normative din domeniile respective, precum și a secretului comercial și a intereselor de afaceri ale furnizorului de servicii în procesul de exercitare a competenței sale legale;

l) informează Serviciul de Informații și Securitate, cu privire la incidentele cibernetice cu impact semnificativ, prevenite sau soluționate, care au vizat obiectivele infrastructurii critice.

2. Secția prevenire și analiză care va fi responsabilă de:

a) emiterea de avertizări timpurii, alerte, anunțuri și diseminează informații privind amenințările cibernetice, vulnerabilitățile și incidentele cibernetice;

b) colectarea și analiza de date criminalistice, furnizează analize dinamice privind riscurile, incidentele cibernetice și conștientizarea situației în materie de securitate cibernetică;

c) efectuarea, la cererea unui furnizor de servicii, de scanări proactive a rețelelor și sistemelor informatice ale solicitantului pentru a detecta vulnerabilitățile cu un impact potențial semnificativ, în conformitate cu legislația;

d) implementarea, în procesul schimbului de informații cu furnizorii de servicii și cu alte persoane relevante, a unor instrumente și soluții tehnice securizate

e) asigurarea, în conformitate cu prevederile legislației, a protecției informațiilor de care ia cunoștință în exercitarea atribuțiilor;

f) exercitarea atribuțiilor de coordonator al procesului de divulgare coordonată a vulnerabilităților.

3. Direcția supraveghere și control, care va fi responsabilă de:

a) supravegherea și controlul furnizorilor de servicii;

b) emiterea actelor cu caracter obligatoriu și recomandărilor;

c) examinarea sesizărilor;

d) restricționarea utilizării sau accesului la o rețea sau sistem informatic;

e) notificarea aplicării măsurilor restrictive;
f) efectuarea investigațiilor preliminare pentru confirmarea încălcărilor.

4. **Secția identificare și evidență furnizori de servicii,** care va fi responsabilă de:
a) identificarea și ținerea evidenței furnizorilor de servicii pe teritoriul Republicii Moldova;
b) întocmirea și ținerea listei furnizorilor de servicii.

5. **Secția cooperare și schimb de informații,** care va deține și calitatea de punct unic de contract, va fi responsabilă de:
a) interacțiunea strategică internațională și schimbul de experiență;
b) interacțiunea cu autoritățile și instituțiile publice și furnizorii de servicii;
c) ținerea evidenței acordurilor privind schimbul de informații;
d) interacțiunea cu autoritățile și instituțiile publice internaționale;
e) transmiterea notificărilor și solicitărilor privind incidentele cibernetice;
f) transmite autorităților și instituțiilor publice naționale notificări și cereri în materie de securitate cibernetică primite din alte state sau de la organizații internaționale ori entități instituite de acestea.

6. **Secția metodologie, standarde, cercetare și dezvoltare,** care va fi responsabilă de:
a) elaborează și asigură promovarea celor mai bune practici și îndrumă furnizorii de servicii în gestionarea riscurilor, inclusiv pentru îndeplinirea cerințelor specifice de securitate privind rețelele și sistemele informatice;
b) elaborarea și promovarea planului național de răspuns la incidentele cibernetice și crizele în domeniul securității cibernetice.

7. **Serviciul juridic și resurse umane,** care va fi responsabil de
a) gestionarea aspectelor juridice și de resurse umane;
b) oferirea consultanței juridice pentru autoritate,
c) asigurarea respectarea legislației
d) gestionarea aspectelor de personal, inclusiv recrutarea și dezvoltarea resurselor umane.

8. **Serviciul financiar-administrativ,** care va fi responsabilă de:
a) gestionarea activităților financiare și administrative;
b) asigurarea planificării și gestionării bugetului,
c) contabilitate, achiziții publice și administrarea resurselor materiale;
d) asigurarea respectării procedurilor administrative și a standardelor financiare.

9. **Serviciul audit intern,** care va fi responsabilă de:
a) efectuarea auditului intern;
b) evaluarea eficienței, transparenței și conformității cu politicile și procedurile interne;
c) identificarea deficiențelor oferirea recomandărilor pentru îmbunătățirea proceselor și a sistemelor organizaționale.

10. **Serviciul tehnologii informaționale și comunicații,** care va fi responsabilă de:
a) gestionarea infrastructurii tehnologice, a rețelelor și a sistemelor de comunicații interne ale autorității;
b) asigurarea implementării și administrarea soluțiilor tehnice.

11. **Serviciul comunicare și relații publice,** care va fi responsabil de:
a) gestionarea comunicării și relațiilor publice;
b) dezvoltarea și implementarea strategiilor de comunicare,
c) gestionarea relațiilor cu mass-media;
d) furnizarea informațiilor și materialelor de comunicare;
e) organizarea evenimentelor și promovarea conștientizării și educației în domeniul securității cibernetice.

12. Serviciul managementul documentelor, care va fi responsabil de:

a) gestionarea documentelor și informațiilor;

b) dezvoltarea și implementarea politicilor și procedurilor pentru gestionarea și arhivarea documentelor;

c) asigurarea accesului și confidențialității informațiilor;

d) protecția secretului de stat în activitatea Agenției;

e) facilitarea schimbului eficient de informații în interiorul organizației.

Conform proiectului de act normativ se propune ca Agenția Națională pentru Securitate Cibernetică să aibă un efectiv-limită de 48 unități de personal. În tabelul de mai jos este propusă o distribuire a efectivului limită al noii entități pe subdiviziunile structurale autonome ale acesteia

Denumirea subdiviziunii	Numărul unităților de personal
Director	**1(1 fpc)**
Director adjunct	**1(1 fpc)**
Direcția răspuns la incidente și crize cibernetice	**13 (2 fpc+11 fpe)**
Direcția supraveghere și control	**7 (1 fpc+6 fpe)**
Secția prevenire și analiză	**4 (1fpc+3 fpe)**
Secția identificare și evidență furnizori de servicii	**5 (1 fpc+4 fpe)**
Secția cooperare și schimb de informații	**5 (1 fpc+4 fpe)**
Secția metodologie, cercetare și dezvoltare	**4 (1 fpc+3 fpe)**
Serviciu juridic și resurse umane	**2 (1 fpc+1 fpe)**
Serviciu financiar-administrativ	**2 (1 fpc+1 fpe)**
Serviciul audit intern	**1 (1 fpe)**
Serviciul tehnologii informaționale și comunicații	**1 (1 fpe)**
Serviciul comunicare și relații publice	**1 (1 fpe)**
Serviciul managementul documentelor	**1 (1fpe)**
Total efectiv	**48 (12 fpc + 36 fpe)**

În același timp, ținând cont de importanța și sensibilitatea sectorului, precum și calificările speciale ce urmează a fi deținute de angajații din cadrul autorității competente, în Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar urmează a fi prevăzută excepție pentru salariații autorității competente.

În mod special o salarizare specială și motivantă este necesară pentru echipa de răspuns la incidente cibernetice (CSIRT), care joacă un rol crucial în protejarea infrastructurii informaționale critice și a datelor sensibile. Iar în sectorul IT cu specializare în domeniul securității cibernetice avem o competiția acerbă pe piața muncii. Această industrie este caracterizată de o cerere ridicată de specialiști, în timp ce oferta de talente calificate este limitată. Prin urmare, pentru a atrage și reține specialiști talentați și experimentați, este necesar de oferit salarii atractive și competitive. În absența unor astfel de salarii, există riscul ca acești profesioniști să fie tentați să lucreze în sectorul privat sau să caute oportunități în alte țări, unde salariile pot fi mai mari.

Adițional, trebuie de luat în considerare natura critică a activității desfășurate de autoritatea competentă și echipa CSIRT a acesteia. Aceștia specialiști sunt responsabili de detectarea și contracararea incidentelor cibernetice, care pot avea consecințe grave asupra securității naționale, infrastructurii informaționale critice și datelor sensibile.

Calculele detaliate sunt oferite la capitolul analiza impacturilor opțiunilor.

c) Expuneți opțiunile alternative analizate sau explicați motivul de ce acestea nu au fost luate în considerare

Prima opțiune alternativă:

O opțiune alternativă analizată față de cea recomandată este opțiunea de constituire a Agenției Naționale pentru Securitate Cibernetică care să cuprindă în competența sa funcțiile descrise la opțiunea recomandată la care să se adauge și competența de centru guvernamental de răspuns la incidentele cibernetice – CERT-Gov, exercitată la momentul actual de Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică".

În acest scenariu în structura Agenției Naționale pentru Securitate Cibernetică ar putea fi constituită cu o subdiviziune structurală dedicată exercitării competențelor de echipă de răspuns la incidentele cibernetice la nivelul rețelelor și sistemelor informatice ale statului.

Excepțiile propuse la Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar în scenariul de bază ar urma să fie aplicate și în cadrul acestui scenariu.

A doua opțiune alternativă:

O altă opțiune alternativă analizată față de cea recomandată este crearea unei noi autorități administrative centrale în subordinea Guvernului, care să aibă competența de realizare a politicii statului în domeniul securității cibernetice. Adițional, ar urma în subordinea acesteia crearea unei autorități administrative responsabile de implementarea politicii în domeniul securității cibernetice.

În cazul acestui scenariu se aplică integral scenariul recomandat, doar că în acest scenariu ar urma să fie creată o autoritatea administrativă centrală responsabilă de realizarea politicii de stat în domeniul securității cibernetic care va exercita calitatea de fondator pentru Agenția Națională pentru Securitate Cibernetică. Totodată, această autoritate ar urma să preia competențele de elaborare a politicilor în domeniul securității cibernetice de la Ministerul Dezvoltării Economice și Digitalizării.

Această autoritate ar urma să aibă un efectiv limită de 8 unități de personal, dintre care 4 unități de personal responsabile de elaborarea politicilor, 3 unități de personal de suport și 1 director.

A treia opțiune alternativă:

A treia opțiune alternativă analizată față de cea recomandată este reorganizarea Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" în autoritate administrativă și subordonarea acesteia autorității administrației publice centrale de specialitate responsabile de realizarea politicii de stat în domeniul securității cibernetice (actualmente Ministerul Dezvoltării Economice și Digitalizării) și desemnarea STISC reorganizat în calitate de autoritate competentă la nivel național în domeniul securității cibernetice.

În cazul implementării acestui scenariu și stabilirii Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" în calitate de autoritate competentă la nivel național în domeniul securității cibernetice, obligativitatea reorganizării acesteia din instituție publică în autoritate administrativă rezidă din faptul că aceasta urmează să realizeze prerogative de putere publică în domeniul securități cibernetice, competențe care nu pot fi realizate decât de o autoritate publică. Or, potrivit art. 32 din Legea nr. 98/2012 privind administrația publică centrală de specialitate, instituțiile publice se instituie doar pentru realizarea unor funcţii de administrare, sociale, culturale, de învățământ şi a altor funcţii de interes public, de care este responsabil ministerul sau altă autoritate administrativă centrală, cu excepția

celor de reglementare normativ-juridică, supraveghere şi control de stat, precum şi a altor funcţii care implică exercitarea prerogativelor de putere publică.

Astfel, în cazul acestei opțiuni, Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică" ar urma să fie reorganizat în autoritate administrativă subordonată Ministerului Dezvoltării Economice și Digitalizării și desemnată în calitate de autoritate competentă la nivel național în domeniul securității cibernetice.

La fel, excepțiile propuse la Legea nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar în scenariul de bază ar urma să fie aplicate și în cadrul acestui scenariu.

Spre deosebire de opțiunea recomandată și opțiunea alternativă, în cazul acestei opțiuni ar urma reorganizarea integrală a Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" din forma de organizare juridică instituție publică în autoritate administrativă, cu completarea acesteia cu un efectiv suplimentar de aproximativ 40 de unități de personal care vor exercita funcțiile și atribuțiile prevăzute și detaliate pentru Agenția Națională pentru Securitate Cibernetică în opțiunea recomandată cu excepția unităților de personal care exercită funcții de suport.

4. Analiza impacturilor opţiunilor

a) Expuneți efectele negative şi pozitive ale stării actuale și evoluția acestora în viitor, care vor sta la baza calculării impacturilor opțiunii recomandate

Printre cele mai importante efecte negative ale stării actuale și evoluția acestora în viitor pot fi enumerate următoarele:

- ***Vulnerabilitate la atacuri cibernetice***: Fără o autoritate competentă în domeniul securității cibernetice există riscul crescut de atacuri cibernetice asupra instituțiilor, companiilor și infrastructurii critice, ceea ce poate duce la pierderi financiare, perturbarea serviciilor și compromiterea datelor, în mod special al celor sensibile.
- ***Incapacitatea de a răspunde eficient la incidente cibernetice***: Fără o echipă dedicată și bine pregătită pentru gestionarea incidentelor cibernetice, timpul de reacție la astfel de situații poate fi prelungit, ceea ce duce la creșterea impactului negativ și la extinderea daunelor produse.
- ***Incoerență în procesul de implementare a politicilor în domeniul securității cibernetice***: Absența unei autorități responsabile de implementarea politicilor în domeniul securității cibernetice poate duce la lipsa unor linii directoare și viziune clară în acest domeniu, ceea ce face dificilă coordonarea eforturilor și asigurarea unui nivel adecvat de securitate cibernetică.
- ***Impactul asupra reputației și încrederii***: Incidentele de securitate cibernetică pot afecta grav încrederea publicului în capacitatea statului și a autorităților de a asigura protecția rețelelor și sistemelor informatice care sunt critice pentru societate și stat. Acest lucru poate avea consecințe negative asupra relațiilor internaționale, investițiilor și dezvoltării economice.

În același timp putem menționa următoarele efecte pozitive ale opțiunii recomandate și evoluția acestora în viitor:

- ***Consolidarea securității cibernetice***: Crearea unei autorități competente în domeniul securității cibernetice va consolida capacitatea de a monitoriza, identifica, preveni și gestiona amenințările cibernetice. Aceasta poate duce la îmbunătățirea protecției infrastructurii critice, a datelor și a informațiilor sensibile.
- ***Reacție mai rapidă și eficientă la incidente cibernetice***: O autoritate competentă poate coordona și mobiliza o echipă de răspuns la incidente cibernetice, capabilă de acțiuni imediate și eficiente pentru a limita impactul și a restabili funcționarea normală în urma unui atac cibernetic.
- ***Dezvoltarea și implementarea unor politici coerente***: Prin crearea unei autorități competente, se va asigura implementarea unor politici coerente în domeniul securității cibernetice. Aceasta va contribui la asigurarea alinierea la standardele internaționale și colaborarea cu alte entități similare la nivel regional și global.

- ***Creșterea încrederii și a reputației***: Existenta unei autorități responsabile de securitatea cibernetică și implementarea unor măsuri adecvate poate contribui la consolidarea încrederii publicului și a partenerilor în capacitatea statului de a proteja infrastructura informațională critică a țării.

b[1]) Pentru opțiunea recomandată, identificați impacturile completând tabelul din anexa la prezentul formular. Descrieți pe larg impacturile sub formă de costuri sau beneficii, inclusiv părțile interesate care ar putea fi afectate pozitiv și negativ de acestea

Beneficii

- ***Consolidarea securității cibernetice:*** Implementarea soluției propuse va duce la o îmbunătățire semnificativă a situației în domeniul securității cibernetice. Sistemele și tehnologiile avansate pot detecta și bloca atacurile cibernetice, protejând datele și informațiile sensibile, precum și reacționa imediat.
- ***Protecția informațiilor și a drepturilor utilizatorilor*****:** Soluția propusă va contribui la o mai bună protecție a informațiilor personale și a drepturilor utilizatorilor. Implementarea unor măsuri suplimentare de securitate poate preveni accesul neautorizat la date și utilizarea abuzivă a acestora.
- ***Reducerea costurilor asociate incidentelor cibernetice*****:** Incidentele cibernetice pot avea consecințe financiare semnificative, cum ar fi pierderi de date, întreruperi ale activității și daune reputaționale. Prin implementarea soluției, autoritățile publice și mediul privat vor beneficia de riscuri reduse asociate incidentelor și pot economisi costurile de recuperare și remediere.
- ***Îmbunătățirea încrederii și a reputației*****:** O securitate cibernetică mai puternică și protecția adecvată a informațiilor va consolida încrederea mediului privat în stat și a utilizatorilor și a clienților în mediul privat și stat.
- ***Siguranța infrastructurii critice:*** Soluția propusă ar consolida securitatea infrastructurii critice, cum ar fi rețelele energetice, sistemul bancar, transportul și comunicarea, etc. Prin prevenirea și gestionarea eficientă a incidentelor cibernetice, se reduce riscul de întreruperi majore în funcționarea acestor servicii vitale și se asigură stabilitatea și continuitatea acestora.
- ***Creșterea nivelului de competență în domeniul securității cibernetice:*** Implementarea opțiunii recomandate ar implica o investiție semnificativă în formarea și dezvoltarea personalului specializat în securitatea cibernetică. Acest lucru ar conduce la creșterea nivelului de competență în domeniu, generând o forță de muncă calificată și capabilă să facă față amenințărilor cibernetice într-un mod eficient și profesionist.
- ***Stimularea inovării și cercetării:*** Implementarea opțiunii recomandate ar avea ca impact impulsionarea inovației și cercetării în domeniul securității cibernetice în Republica Moldova. Dezvoltarea și adoptarea de tehnologii și soluții noi ar putea contribui la consolidarea poziției țării în această sferă și ar putea genera oportunități de dezvoltare economică și colaborare internațională.
- ***Protejarea mediului înconjurător:*** În contextul creșterii dependenței de tehnologia informației și comunicațiilor, implementarea opțiunii recomandate poate contribui, chiar dacă indirect la îmbunătățirea protecției mediului înconjurător, inclusiv prin prevenirea unor situații excepționale în special cu caracter tehnogen, precum consumul excesiv de resurse și producerea de deșeuri electronice.

Costuri:

- ***Costuri salariale:*** Funcționarea autorității competente în domeniul securității cibernetice necesită o echipă calificată cu o salarizare motivantă și corespunzătoare atribuțiilor stabilite. Urmează a fi remarcat că echipa de răspuns la incidentele cibernetice are un rol crucial în asigurarea unei comunicări eficiente și disponibilitate permanentă a canalelor de comunicare, de a opera într-un mediu securizat, de a gestiona cererile în mod eficient, de a menține confidențialitatea și credibilitatea operațiunilor, de a avea personal pregătit și disponibil în permanență, și de a asigura continuitatea serviciilor prin utilizarea sistemelor redundante și a spațiului de lucru de rezervă, urmând, de asemenea, a coopera cu alte echipe de răspuns la incidentele cibernetice din rețele internaționale. Astfel, este crucial ca angajații implicați în echipa de răspuns la incidentele cibernetice să beneficieze de un salariu foarte competitiv, în special având în vedere importanța și

complexitatea funcției pe care o desfășoară. Pentru a asigura atragerea și reținerea specialiștilor calificați în domeniul securității cibernetice, se propune pentru angajații din echipa de răspuns la incidentele cibernetice să primească un spor de salariu de 600%, în timp ce restul angajaților autorității, care trebuie, de asemenea, să fie foarte calificați, să beneficieze de un spor de 200%. Această abordare asigură că specialiștii în securitate cibernetică sunt remunerați în mod adecvat și competitiv în comparație cu media din sectorul privat și cu media europeană. Prin acordarea unor salarii atractive și competitive, autoritatea va putea atrage și păstra experți calificați în domeniul securității cibernetice, asigurând astfel o echipă de înaltă calitate în asigurarea unui răspuns adecvat la incidentele și crizele cibernetice. Conform calculelor estimative, cheltuielile totale pentru salarizarea angajaților vor fi de **25,5 milioane lei anual**. Din această sumă, aproximativ **11,2 milioane** lei vor fi alocate echipei responsabile de realizarea funcției de echipă de răspuns la incidentele cibernetice. Este important de menționat că aceste cifre includ și impozitele angajaților și angajatorului, asigurând transparența și corectitudinea estimărilor. În tabelul de mai jos este prezentat detaliat modul de formare a acestor cheltuieli salariale:

Titlul funcției		Clasa de salarizare conform vechimii în muncă (minim)		**Salariul de bază lunar (lei)**	**Sporul pru gradul profesional/ (lei)**	**Spor de performanța (10% din**	**Spor lunar 1300 lei**	**Total salariu lunar**	**Spor salarial (600 % pentru echipa CSIRT și 200 % pentru restul angajaților din salariul de baza)**	**Total venit lunar/persoană (salariu + spor)**
				1900						
Director	**1**	**110**	**9,77**	**18.563**				**18.563**	**37.126**	***55.689***
Director adjunct	**1**	**106**	**8,98**	**17.062**				**17.062**	**34.124**	***51.186***
Şef Direcţie	**1**	**95**	**7,14**	**13.566**				**13.566**	**27.132**	***40.698***
Şef Direcţie (CSIRT)	**1**	**95**	**7,14**	**13.566**				**13.566**	**81.396**	***94.962***
Şef adjunct Direcţie (CSIRT)	**1**	**91**	**6,57**	**12.483**				**12.483**	**74.898**	***87.381***
Şef secţie	**4**	**83**	**5,55**	**10.545**				**42.180**	**84.360**	***31.635***
Şef serviciu	**2**	**78**	**5,00**	**9.500**				**19.000**	**38.000**	***28.500***
Contabil şef	**1**	**78**	**5,00**	**9.500**				**9.500**	**19.000**	***28.500***
Auditor intern principal	**1**	**72**	**4,41**	**8.379**				**8.379**	**16.758**	***25.137***
Inspector principal	**4**	**70**	**4,23**	**8.037**				**32.148**	**64.296**	***24.111***
Specialist principal	**20**	**61**	**3,51**	**6.669**				**133.380**	**266.760**	***20.007***
Specialist principal (CSIRT)	**11**	**61**	**3,51**	**6.669**				**73.359**	**513.513**	***53.352***
Total	**48**			**134.539**	**0**	**0**	**0**	**393.186**	**1.257.363**	
					Salariu anu			**19.806.588**		
					29%			**5.743.911**		
					Total general			**25.550.499**		

- ***Costuri operaționale:*** Implementarea soluției vor implica cheltuieli inițiale semnificative pentru dezvoltarea și configurarea sistemelor necesare. Aceste costuri pot include achiziționarea de echipamente specializate, dezvoltarea de software personalizat sau personalizarea soluțiilor existente pentru a se potrivi nevoilor autorității. Adițional, vor fi necesare costuri de mentenanță a hardware-ului și software-ului, actualizările tehnologice periodice, monitorizarea și gestionarea incidentelor de securitate, precum și suport tehnic pentru utilizatori. Estimările preliminare, bazate pe experiențe analogice la nivelul statelor membre UE, indică că suma necesară pentru aceste echipamente se situează în jurul valorii de 10 mil. de lei (500.000 EUR). Aceste resurse asigură funcționalitatea și eficiența operațională a echipei în gestionarea incidentelor cibernetice.

- ***Costuri de formare și dezvoltare a personalului:*** Pentru a utiliza eficient și pentru a gestiona riscurile de securitate a rețelelor și sistemelor informatice critice, este necesară formarea și dezvoltarea continuă a personalului. Acest lucru poate include participarea la cursuri de specializare, programe de certificare și alte activități de învățare pentru a înțelege și aplica bunele practici în materie de securitate cibernetică. Pentru a asigura nivelul adecvat de competență și expertiză în domeniul securității cibernetice, instituții precum TRANSITS, CERT/CC, SANS Institute și FIRST

oferă astfel de programe de formare. Pentru a acoperi costurile de formare anuale, este recomandată alocarea unor resurse financiare minime cuprinse între 3 000 și 5 000 EUR pe expert.

Totodată, potrivit analizei de impact[29] la Directiva NIS1, experții Comisiei Europene au stabilit că „*Pentru cele trei state membre care nu au înființat încă CERT-uri naționale/guvernamentale (Cipru, Irlanda și Polonia), costul estimat al punerii în funcțiune a infrastructurii și serviciilor aferente, pe baza interviurilor realizate cu CERT-uri care sunt deja operaționale, ar fi de aproximativ 2,5 milioane EUR pentru fiecare CERT*.". Ținând cont că standardele care urmează să le întrunească autoritatea competentă din Republica Moldova sunt similare cu cele din țările UE, pentru a asigura operaționalizarea integrală a acesteia (inclusiv salarizarea, instruirea, etc.), costul final pentru primul an de activitate poate fi estimat la aproximativ 50 milioane lei (2,5 mln. EUR). Acest cost poate varia în funcție de spațiul care va fi identificat și investițiile necesare pentru renovarea și adaptarea conform standardelor cerute de Directiva NIS 2.

Totodată, ținem să relevăm că Planul de acțiuni privind implementarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărârea Guvernului 811/2015[30], a estimat costurile de creare, dotare și asigurare a funcționalității unui centru de reacție la incidente cibernetice la nivel național la circa 49,6 mil. lei, dintre care 29,7 mil lei urmau a fi dedicate în anul 2016 exclusiv acțiunilor de creare a acestui centru.

Părțile interesate care pot fi avantajate sau afectate de aceste costuri și beneficii includ:

- ***Mediul de afaceri***: din perspectiva protecției rețelelor și sistemelor informatice proprii mediul de afaceri va fi avantajat de suportul oferit de Agenție în gestionarea incidentelor cibernetice, de informații actualizate privind amenințările și vulnerabilitățile la nivel de țară și în consecință, de o reacție la timp la potențialele amenințări sau incidente cibernetice. Din perspectiva creșterii nivelului de protecție a rețelelor și sistemelor informatice ale altor persoane juridice, mediul privat va fi avantajat de faptul că va crește credibilitatea partenerilor de afaceri, dar și oportunitățile de investiție, sustenabilitatea din punct de vedere a securității cibernetice a acestora contribuind semnificativ la asigurarea continuității serviciilor critice prestate. Ar putea fi afectat din perspectiva
- ***Utilizatori/consumatori/cetățenii***: vor fi avantajați de disponibilitatea crescută a serviciilor de care beneficiază și de o protecție corespunzătoare a datelor personale.
- ***Autorități publice:*** Vor fi avantajate de îmbunătățirea cadrului instituțional, creșterea capacităților de gestionare a incidentelor cibernetice.

b[2]) Pentru opțiunile alternative analizate, identificați impacturile completînd tabelul din anexa la prezentul formular. Descrieți pe larg impacturile sub formă de costuri sau beneficii, inclusiv părțile interesate care ar putea fi afectate pozitiv și negativ de acestea

Opțiunea alternativă 1: <u>Transferul competenței de centru guvernamental de răspuns la incidentele cibernetice către autoritatea administrativă responsabilă de implementarea politicii în domeniul securității cibernetice din subordinea autorității administrației publice centrale de specialitate (Ministerul Dezvoltării Economice și Digitalizării).</u>

Beneficii:

- Consolidarea coordonării și guvernării în domeniul securității cibernetice, prin transferul competenței de centru guvernamental de răspuns la incidentele cibernetice către autoritatea administrativă responsabilă de răspuns la incidentele cibernetice la nivel național;
- Eficientizarea utilizării resurselor și expertizei disponibile în cadrul autorității administrației publice centrale specializate la momentul actual în domeniul securității cibernetice;

[29] https://www.consilium.europa.eu/ro/documents-publications/public-register/public-register-search/results/?AllLanguagesSearch=False&OnlyPublicDocuments=False&DocumentNumber=6342%2F13%7C6342%2F*%2F13&DocumentLanguage=FR

[30] https://www.legis.md/cautare/getResults?doc_id=110324&lang=ro

- Creșterea capacității de răspuns la incidentele cibernetice și consolidarea securității cibernetice la nivel național;
- Autoritatea administrației publice centrale de specialitate (Ministerul Dezvoltării Economice și Digitalizării) ar dispune de instrumentarul instituțional suficient și necesar pentru a realiza corespunzător politica statului în domeniul securității cibernetice, ceea ce va avea ca efect consolidarea proceselor de cooperare și coordonare a proceselor;
- Sectorul public și privat ar putea beneficia de o mai bună protecție împotriva amenințărilor cibernetice prin intermediul unei autorități centrale mai puternice.

Costurile la această opțiune, comparativ cu opțiunea recomandată, ar urma să crească cu aproximativ **3 mil. lei anual**. Acest cost este dedus din transferul a 4 angajați care exercită funcțiile și atribuțiile pentru centru guvernamental de răspuns la incidentele cibernetice exercitată la momentul actual de la Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică" către Agenția Națională pentru Securitate Cibernetică. Acești salariați în cadrul Agenției Naționale pentru Securitate Cibernetică ar urma să fie salariați similar angajaților din echipa de răspuns la incidentele cibernetice la nivel național.

Părți interesate:

- Ministerul Dezvoltării Economice și Digitalizării și Agenția Națională pentru Securitate Cibernetică ar avea o responsabilitate și competență extinsă în domeniul securității cibernetice.
- Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică" ar urma să-și piardă statutul de centru guvernamental de răspuns la incidentele cibernetice.
- Personalul din Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică" ar putea fi afectat de schimbările în ceea ce privește responsabilitățile și structura organizațională.

Opțiunea alternativă 2: **Crearea unei noi autorități administrative centrale în subordinea Guvernului pentru realizarea politicii statului în domeniul securității cibernetice.**

Beneficii:

- Consolidarea capacității administrative și coordonarea îmbunătățită a politicilor în domeniul securității cibernetice prin intermediul unei autorități dedicate elaborării de politici.
- Crearea unei structuri specializate și focusate exclusiv pe realizarea politicii de stat în domeniul securității cibernetice.

Costurile la această opțiune, comparativ cu opțiunea recomandată, ar urma să crească cu aproximativ **300 mii lei** anual. Acest cost este generat de crearea a unei autorități administrative centrale noi cu 8 angajați, 4 dintre care ar urma să fie transferați de la Ministerul Dezvoltării Economice și Digitalizării. Astfel, după cum se prezintă în tabelul de mai jos, costul anual integral ar fi de 1,06 mln lei, iar mai mult jumătate din această sumă urmând a fi transferată din bugetul actual al Ministerul Dezvoltării Economice și Digitalizării, urmare a transferului de personal responsabil de elaborarea politicilor în domeniul securității cibernetice. Costurile respective sunt calculate reieșind din legislația actuală.

În același timp, în eventualitatea aplicări acestui scenariu, urmează a se ține cont că dezvoltarea politicilor în domeniul securității cibernetice, la fel ca și în cazul implementării politicilor în acest domeniu, sunt necesare competențe și calificări corespunzătoare. Acești specialiști ar urma să dețină cunoștințe solide în domeniul sistemelor informatice, rețelelor și programării, pentru a înțelege în detaliat tehnologiile și amenințările cibernetice existente. Adițional, pe lângă expertiza tehnică, persoanele responsabile cu elaborarea politicilor în domeniul securității cibernetice trebuie să fie familiarizate cu reglementările și standardelor relevante și trebuie să fie în măsură să integreze aceste reglementări în politicile elaborate.

Prin urmare, reieșind din cele menționat supra, în cazul angajaților autorității administrative centrale ar urma să fie aplicat un spor salarial de 200 %, similar aplicat angajaților autorității competente, ceea ce ar genera un cost suplimentar de peste **2 milioane de lei.**

În concluzie, în eventualitatea aplicării excepțiilor menționate supra, am obține un cost suplimentar de **2,3 milioane lei.**

Denumirea subdiviziunii structurare, titlul funcției	Număr de unități	Clasa de salarizare	Coeficientul de salarizare	Salariul de bază lunar (lei)	Sporul pru gradul profesional/ (lei)	Spor de performanta (10% din sal. de baza)	Spor lunar 1300 lei	Total salariu lunar
				1900				
Director general	**1**	**120**	**12,04**	**22876**				**22876**
Șef Secție	**1**	**95**	**7,14**	**13566**				**13566**
Consultant principal	**3**	**70**	**4,23**	**8037**				**8037**
Contabil șef	**1**	**78**	**5,00**	**9500**				**9500**
Auditor intern principal	**1**	**72**	**4,41**	**8379**				**8379**
Specialist principal	**1**	**61**	**3,51**	**6669**				**6669**
Total	**8**			**69027**				**69027**
					Salariu anual			**828.324**
					29%			**240.214**
					Total general			**1.068.538**

Părți interesate:

- Guvernul ar beneficia de autoritate specializată în elaborarea politicilor în domeniul securității cibernetice și alta care să implementeze politici adecvate în acest domeniu.
- Angajații actuali ai Ministerului Dezvoltării Economice și Digitalizării ar urmă să fie afectați salarial urmare a transferului în noua autoritate administrativă.

Opțiunea alternativă 3: **Reorganizarea și extinderea competențelor și responsabilităților existente ale Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" și resubordonarea acesteia.**

Beneficii:

- Utilizarea expertizei și resurselor deja existente în cadrul Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" pentru a dezvolta capacități în domeniul securității cibernetice.
- Sinergie mai strânsă dintre echipa care exercită funcțiile și atribuțiile pentru centru guvernamental de răspuns la incidentele cibernetice și echipa de răspuns la incidentele cibernetice la nivel național.
- Reducerea costurilor prin utilizarea infrastructurii și personalului deja existent în cadrul Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică".

Costurile în acest scenariu ar depinde de modul de salarizare a angajaților actuali din cadrul Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" urmare a reorganizării. Astfel dacă angajații din cadrul instituției publice, prin introducerea unei excepții legislative, păstrează nivelul actual de salarizare în cadrul noii autorități administrative și vor acoperi funcțiile de suport pentru echipa care va realiza competențele autorității administrative responsabile de implementarea politicii în domeniul securității cibernetice, atunci rezultă o economie de circa **5 mil.lei**.

Părți interesate:

- Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică" ar avea oportunitatea de a-și extinde activitățile și expertiza în domeniul securității cibernetice, consolidându-și poziția de instituție de referință în domeniu.

- Guvernul ar beneficia de utilizarea eficientă a resurselor deja existente și a expertizei din cadrul Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" pentru a consolida securitatea cibernetică la nivel național.
- Alte entități sau instituții care au competențe și responsabilități în domeniul securității cibernetice ar putea avea nevoie de o colaborare și coordonare suplimentară cu Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică", ceea ce poate implica schimbări și adaptări în funcționarea lor.
- Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică" ar putea fi suprasolicitat din punct de vedere al resurselor și capacităților sale.

c) Pentru opțiunile analizate, expuneți cele mai relevante/iminente riscuri care pot duce la eșecul intervenției și/sau schimba substanțial valoarea beneficiilor și costurilor estimate și prezentați presupuneri privind gradul de conformare cu prevederile proiectului a celor vizați în acesta

Opțiunea recomandată: **Crearea unei noi autorități administrative pentru gestionarea securității cibernetice responsabile de implementarea politicii în domeniul securității cibernetice în subordinea Ministerului Dezvoltării Economice și Digitalizări.**

Riscuri:

- *Lipsa de susținere din partea autorităților și instituțiilor existente, în mod special din partea Ministerului Finanțelor:* Există posibilitatea ca instituțiile și autoritățile să se opună creării unei noi autorități, deoarece acest lucru poate implica schimbări în structura, competențele și responsabilitățile lor, dar și suporta un cost suplimentat destul de înalt din bugetul de stat.
- *Resurse financiare insuficiente*: Bugetul alocat pentru crearea și funcționarea noii autorități poate să nu fie suficient pentru a realiza toate obiectivele propuse. Aceasta poate duce la subfinanțare și limitarea capacităților de gestionare a securității cibernetice, afectând eficacitatea intervenției.
- *Lipsa personalului calificat și a experților în securitatea cibernetică*: Găsirea și recrutarea personalului cu expertiză și experiență adecvată în securitatea cibernetică poate fi o provocare.
- *Complexitatea coordonării și colaborării cu alte entități*: Noii autorități le-ar putea fi dificil să stabilească relații de colaborare și să coordoneze activitățile cu alte entități și instituții existente. Diferitele niveluri de autoritate, competențe și interese pot crea obstacole în implementarea eficientă a măsurilor de securitate cibernetică.

Presupuneri privind gradul de conformare:

Poate fi presupus că părțile interesate vor fi dispuse să coopereze și să colaboreze în implementarea intervenției propuse. La fel, s-ar putea presupune că autoritățile competente vor accepta și sprijini crearea noii autorități administrative pentru gestionarea securității cibernetice responsabile de implementarea politicii în acest domeniu, iar resursele necesare vor fi alocate în mod adecvat pentru a realiza obiectivele propuse. De asemenea, se presupune că va exista un efort susținut pentru a recruta și a forma personalul calificat și că se vor dezvolta mecanisme eficiente de coordonare și colaborare cu alte entități relevante.

Opțiunea alternativă 1: **Transferul competenței de centru guvernamental de răspuns la incidentele cibernetice către autoritatea administrativă responsabilă de implementarea politicii în domeniul securității cibernetice în subordinea autorității administrației publice centrale de specialitate (Ministerul Dezvoltării Economice și Digitalizării).**

Riscuri:

- *Suprasolicitarea resurselor existente*: Extinderea competențelor și de centru guvernamental de răspuns la incidentele cibernetice pentru Agenția Națională pentru Securitate Cibernetică poate duce la suprasolicitarea resurselor și capacităților sale. Acest lucru poate afecta negativ capacitatea autorității de a se ocupa eficient de cerințele și provocările în creștere ale securității cibernetice.

- *Lipsa de susținere din partea autorităților și instituțiilor existente, în mod special din partea Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" și Ministerului Finanțelor*. Există posibilitatea ca instituțiile și autoritățile deja existente să se opună transferului acestor competențe către noua autoritate, deoarece acest lucru poate implica schimbări în structura, competențele și responsabilitățile lor, dar și suporta un cost suplimentat destul de înalt din bugetul de stat.
- *Resurse financiare insuficiente*: Bugetul alocat pentru crearea și funcționarea noii autorități ar urma să crească și mai mult.
- *Lipsa personalului calificat și a experților în securitatea cibernetică*: Riscul de la opțiunea de bază rămâne valabil și la această opțiune, găsirea și recrutarea personalului cu expertiză și experiență adecvată în securitatea cibernetică poate fi o provocare.

Presupuneri privind gradul de conformare:

Poate fi presupus că autoritatea ce urmează a fi creată existentă va fi deschisă și receptivă la extinderea rolului său în gestionarea securității cibernetice și va adopta măsurile necesare pentru a-și dezvolta competențele și expertiza în acest domeniu. De asemenea, putem presupune că și alte instituții și autorități relevante ar accepta și sprijini această extindere și va colabora în mod eficient. Cu toate acestea, există riscul rezistenței și opoziției din partea Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" și Ministerului Finanțelor, ceea ce poate afecta gradul de conformare și cooperare în implementarea intervenției.

Opțiunea alternativă 2: **Crearea unei noi autorități administrative centrale în subordinea Guvernului pentru realizarea politicii statului în domeniul securității cibernetice și a unei autorități administrative subordonate acesteia responsabilă de implementarea politicii de stat în acest domeniu.**

Riscuri:

- *Creșterea birocrației:* Crearea unei noi autorități administrative centrale și a unei autorități administrative responsabile de implementarea politicii în domeniul securității cibernetice ar putea duce la o creștere a birocrației. Acest lucru ar putea afecta eficiența și agilitatea în luarea deciziilor și implementarea măsurilor de securitate cibernetică.
- *Competiție pentru resurse*: Crearea de noi structuri administrative poate duce la competiție pentru resurse, inclusiv buget și personal calificat. Dacă resursele sunt limitate sau împărțite ineficient între structurile administrative, acest lucru ar putea afecta capacitatea fiecărei entități de a-și îndeplini responsabilitățile în mod eficient.

Presupuneri privind gradul de conformare:

Poate fi presupus că prin crearea de structuri administrative suplimentare, Guvernul urmărește să își întărească abordarea și să se asigure că securitatea cibernetică este o prioritate. Astfel, se poate presupune că autoritatea administrativă centrală nou creată va depune eforturi semnificative pentru a asigura un grad ridicat de conformare cu politicile și reglementările relevante.

Opțiunea alternativă 3: **Reorganizarea și extinderea competențelor și responsabilităților Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică" și resubordonarea acesteia MDED.**

Riscuri:

- *Lipsa de susținere din partea autorităților și instituțiilor existente, în mod special din partea Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică"*. Există posibilitatea ca instituțiile și autoritățile deja existente să se opună acestui model, deoarece acest lucru poate implica schimbări în structura, competențele și responsabilitățile lor.
- *Resurse financiare insuficiente*: Deși sunt mai mici resursele financiare necesare față de opțiunea recomandată, aceasta oricum poate crea un efort financiar substanțial pentru bugetul de stat.

- *Lipsa personalului calificat și a experților în securitatea cibernetică*: Găsirea și recrutarea personalului nou cu expertiză și experiență adecvată în securitatea cibernetică poate fi o provocare.

Presupuneri privind gradul de conformare:

Poate fi presupus că Guvernul ar fi interesat de această opțiune, reieșind din costul puțin mai redus față de opțiunea recomandată, în acest caz ar însemna o reorganizare integrală a Instituției publice "Serviciul Tehnologia Informației și Securitate Cibernetică", însă aceasta poate revedea modul actual de asigurare a securității cibernetice la nivel guvernamental.

d) Dacă este cazul, pentru opțiunea recomandată expuneți costurile de conformare pentru întreprinderi, dacă există impact disproporționat care poate distorsiona concurența și ce impact are opțiunea asupra întreprinderilor mici și mijlocii. Se explică dacă sunt propuse măsuri de diminuare a acestor impacturi

Nu implică costuri de conformare pentru întreprinderi.

Concluzie

e) Argumentați selectarea unei opțiunii, în baza atingerii obiectivelor, beneficiilor și costurilor, precum și a asigurării celui mai mic impact negativ asupra celor afectați

Selectarea acestei opțiuni se bazează pe o analiză detaliată a problemelor, soluțiilor și obiectivelor propuse, luând în considerare beneficiile și costurile implicate, precum și minimizarea impactului negativ asupra celor afectați. Opțiunea aleasă are potențialul de a contribui semnificativ la dezvoltarea capacităților naționale de securitate cibernetică și la consolidarea cooperării naționale și internaționale în acest domeniu. Prin atingerea obiectivelor propuse, se vor crea condiții favorabile nu doar pentru reducerea numărului de incidente cibernetice la nivel național, dar pentru monitorizarea și cunoașterea despre existența unor amenințări sau incidente, precum și pentru instituirea unei echipe de răspuns la incidentele de securitate cibernetică (CSIRT) recunoscute la nivel internațional.

Alegerea acestei opțiuni este susținută de o serie de beneficii semnificative. În primul rând, implementarea măsurilor propuse va duce la o creștere a securității cibernetice la nivel național, protejând informațiile și drepturile utilizatorilor. De asemenea, această opțiune va spori încrederea cetățenilor și mediului de afaceri în autoritățile publice.

Pe lângă beneficiile în domeniul securității cibernetice, implementarea acestei opțiuni va stimula și inovația și cercetarea în domeniu. Dezvoltarea capacităților naționale de securitate cibernetică va implica investiții în tehnologii avansate și în formarea și dezvoltarea continuă a personalului. Acest lucru va promova dezvoltarea industriei de securitate cibernetică și va crea oportunități pentru inovare și avansare în domeniu. De asemenea, prin cooperarea la nivel național și internațional, se va facilita schimbul de informații și bune practici, contribuind creșterea nivelului de protecție a rețelelor și sistemelor informatice utilizate în furnizarea serviciilor critice.

În ceea ce privește costurile, este important să se recunoască că implementarea acestei opțiuni va implica cheltuieli salariale substanțiale și cheltuieli inițiale semnificative pentru dezvoltarea și configurarea sistemelor necesare, precum și costuri operaționale continue pentru funcționarea și întreținerea acestor sisteme. De asemenea, pot fi necesare investiții suplimentare pentru conformitatea reglementară și pentru formarea și dezvoltarea continuă a personalului. Cu toate acestea, trebuie avut în vedere că costurile asociate incidentelor cibernetice pot fi mult mai mari și pot avea consecințe financiare și reputaționale serioase. Prin urmare, investițiile în securitatea cibernetică pot fi considerate o măsură preventivă necesară și justificată.

În concluzie, opțiunea propusă are potențialul de a aduce beneficii semnificative Republicii Moldova prin dezvoltarea capacităților de securitate cibernetică, consolidarea cooperării naționale și internaționale și stimularea inovației. Implementarea obiectivelor specifice propuse va contribui la o protecție adecvată a infrastructurii informaționale critic împotriva incidentelor cibernetice, la instituirea unei echipe de răspuns la incidentele de securitate cibernetică recunoscute la nivel internațional și, în general la creșterea nivelului de securitate cibernetică la nivel național. Chiar dacă implică costuri,

acestea sunt justificate de necesitatea protejării informațiilor și drepturilor utilizatorilor, prevenirea pierderilor economice și consolidarea încrederii în mediul digital. Prin urmare, această opțiune reprezintă o abordare strategică și necesară pentru a face față provocărilor din domeniul securității cibernetice.

5. Implementarea şi monitorizarea

a) Descrieți cum va fi organizată implementarea opțiunii recomandate, ce cadru juridic necesită a fi modificat și/sau elaborat și aprobat, ce schimbări instituționale sunt necesare

Pentru implementarea opțiunii recomandate este necesar de aprobat și publicat proiectul propus de hotărâre de Guvern cu privire la constituirea, organizarea și funcționarea Agenției Naționale pentru Securitate Cibernetică și asigurarea unei abordări coordonate între autoritățile publice, după cum urmează:

- ***Organizare și resurse***: Va fi necesară asigurarea resurselor umane, tehnice, tehnologice și financiare pentru o bună funcționalitate a Agenției Naționale pentru Securitate Cibernetică și implementarea eficientă a opțiunii.
- ***Cadru juridic***: Pentru asigurarea unui nivel adecvat de salarizare a angajaților noii entități va fi necesară revizuirea și modificarea Legii Nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar, prin introducerea unor sporuri specifice angajaților Agenției Naționale pentru Securitate Cibernetică.
- ***Cooperări instituționale:*** Implementarea opțiunii recomandate va necesita stabilirea mecanismelor de cooperare și colaborare cu alte autorități și instituții publice relevante, precum și dezvoltarea parteneriatelor cu sectorul privat și societatea civilă. Este important să se asigure coordonarea eficientă și sinergiile între toate părțile implicate pentru atingerea obiectivelor stabilite.
- ***Comunicare și conștientizare***: Implementarea opțiunii recomandate trebuie însoțită de eforturi ample de comunicare și conștientizare în rândul furnizorilor de servicii, autorităților, instituțiilor publice și utilizatorilor finali. Este esențial să se ofere informații clare și accesibile cu privire la rolul autorității, să se promoveze bunele practici și să se faciliteze schimbul de informații relevante pentru securitatea cibernetică.

În concluzie, implementarea opțiunii recomandate va implica o abordare integrată care cuprinde organizarea eficientă, revizuirea cadrului juridic, cooperării instituționale și eforturi de comunicare și conștientizare. Prin aceste măsuri, se urmărește consolidarea capacităților și eficacității în domeniul securității cibernetice, promovarea conformității cu legislația și dezvoltarea unei culturi de securitate cibernetică în întreaga societate.

b) Indicați clar indicatorii de performanță în baza cărora se va efectua monitorizarea

Pentru a efectua monitorizarea și evaluarea progresului în atingerea obiectivelor propuse, vor fi utilizați următorii indicatori de performanță:

Obiectiv general: Capacitățile naționale de securitate cibernetică pentru reducerea numărului de incidente cibernetice la nivel național dezvoltate și cooperarea internațională consolidată.

Obiectiv specific 1. *Indicator de performanță:* 90 % de personal angajat în cadrul autorității competente în domeniul securității cibernetice până la data de 27 ianuarie 2024.

Obiectiv specific 2. *Indicator de performanță:* 100 % furnizori de servicii identificați până la data de 27 iulie 2024;

Obiectiv specific 3. *Indicator de performanță:* 100 % furnizori de servicii interconectați prin intermediul Registrului de stat al incidentelor cibernetice până la data de 1 ianuarie 2025;

Obiectiv specific 4. *Indicator de performanță:* 100 % personal angajat în cadrul subdiviziunii responsabile de realizare funcțiilor echipei de răspuns la incidentele de securitate cibernetică (CSIRT) până la data de 27 ianuarie 2024.

Obiectiv specific 5. *Indicator de performanță:* Cel puțin 5 relații de cooperare în materie de securitate cibernetică stabilite cu cel puțin 5 echipe de răspuns la incidente de securitate cibernetică din cel puțin 5 state membre ale Uniunii Europene, până la 31 decembrie 2025.

c) Identificați peste cât timp vor fi resimțite impacturile estimate și este necesară evaluarea performanței actului normativ propus. Explicați cum va fi monitorizată și evaluată opțiunea

Impacturile estimate ale opțiunii propuse vor fi resimțite pe parcursul implementării opțiunii selectate și a cadrului normativ în domeniul securității cibernetice, în mod special Legea nr. 48/2023 privind securitatea cibernetică. Evaluarea performanței actului normativ propus se va realiza printr-un proces continuu de monitorizare și evaluare a progresului în raport cu indicatorii de performanță stabiliți.

Procesul de monitorizare și evaluare va implica următoarele aspecte:

- ***Colectarea și analiza datelor***: Se vor colecta și analiza date relevante privind implementarea măsurilor propuse și progresul în atingerea obiectivelor. Aceste date pot include informații despre funcționarea autorității competente în domeniul securității cibernetice, actualizarea listei furnizorilor de servicii, cooperarea și schimbul de informații la nivel național și internațional, instituirea echipei de răspuns la incidentele cibernetice la nivel național, capacitățile de monitorizare și analiză a amenințărilor și vulnerabilităților, răspunsul la incidentele cibernetice și cooperarea cu alte entități relevante.
- ***Analiza rezultatelor***: Datele colectate vor fi analizate pentru a evalua progresul și performanța în atingerea obiectivelor propuse. Se vor identifica eventualele deficiențe, obstacole sau dificultăți întâmpinate în implementare și se vor propune măsuri corective sau ajustări, dacă este necesar.
- ***Rapoarte și comunicare***: Se vor elabora rapoarte periodice pentru a prezenta rezultatele evaluării performanței și a progresului în implementarea strategiei de securitate cibernetică. Aceste rapoarte vor fi comunicate autorităților competente, sectorului privat și altor părți interesate relevante. Comunicarea transparentă și eficientă a rezultatelor obținute va facilita înțelegerea și implicarea tuturor actorilor implicați.

Prin acest proces de monitorizare și evaluare continuă, se va asigura că opțiunea propusă este eficientă, adaptată la contextul specific al Republicii Moldova și capabilă să îndeplinească obiectivele stabilite într-un mod eficient și cu cel mai mic impact negativ asupra celor afectați.

6. Consultarea

a) Identificați principalele părți (grupuri) interesate în intervenția propusă

Cercul de subiecți interesați în intervenția propusă poate fi grupat în următoarele categorii:

- ***Guvernul și autoritățile publice relevante***: Aceasta poate include Ministerul Dezvoltării Economice și Digitalizării, Cancelaria de Stat, Ministerul Finanțelor, Ministerului Justiției, Ministerul Afacerilor Interne, Ministerul Apărării, Serviciul de Informații și Securitate și alte instituții guvernamentale care au tangență cu securitatea cibernetică.
- ***Sectorul privat:*** Companiile din sectorul IT și telecomunicații, furnizorii de servicii de internet, băncile și alte instituții financiare, operatorii de infrastructură critică și alte entități din sectorul privat care au tangență directă cu domeniul securității cibernetice.
- ***Organizații non-guvernamentale***: ONG-urile care realizează analize în domeniul securității cibernetice pot avea un rol consultativ și pot aduce expertiză în dezvoltarea politicilor și a reglementărilor în acest domeniu. Ele pot reprezenta interesele societății civile și pot contribui la promovarea unei abordări echilibrate și inclusivă în gestionarea securității cibernetice.
- ***Mediul academic***: Universitățile, centrele de cercetare și alte instituții academice sunt importante părți interesate în dezvoltarea autorității competente pentru securitatea cibernetică. Aceste entități pot furniza expertiză tehnică și științifică, pot contribui la formarea specialiștilor în securitatea cibernetică și pot desfășura cercetări relevante pentru dezvoltarea sectorului.

- ***Publicul larg***: Este esențial să se implice și să se informeze publicul larg cu privire la importanța securității cibernetice și la rolul autorității competente. Publicul trebuie să fie conștient de riscurile cibernetice și de măsurile pe care le poate lua pentru a se proteja. Consultarea și implicarea cetățenilor pot contribui la dezvoltarea unor politici și practici mai eficiente în gestionarea securității cibernetice.

b) Explicați succint cum (prin ce metode) s-a asigurat consultarea adecvată a părților

După finalizarea elaborării proiectului, analiza de impact, proiectul de act normativ propriu-zis și nota informativă urmează a fi supuse unor consultări preliminare cu subdiviziunea structurală internă a Ministerului Dezvoltării Economice și Digitalizării responsabilă de realizarea politicii de stat în domeniul securității cibernetice, precum și cu Instituția publică "Serviciul Tehnologia Informației și Securitate Cibernetică" .

După consultarea opiniilor preliminare și ajustarea corespunzătoare a proiectului de act normativ și documentelor de suport, analiza de impact, conform rigorilor stabilite de Hotărârea Guvernului nr.23/2019 „Cu privire la aprobarea Metodologiei de analiză a impactului în procesul de fundamentare a proiectelor de acte normative", urmează a fi supusă examinării de către:

a) Cancelaria de Stat, având în vedere că proiectul prevede reorganizări şi reforme structurale/instituționale ale sistemului autorităților administrației publice centrale de specialitate;
b) Ministerul Finanțelor, având în vedere faptul că prevederile proiectului de act normativ conține reglementări ce vor avea impact asupra bugetului public național.

După examinarea pachetului de documente de către instituțiile menționate mai sus, și ajustarea eventuală a acestora, proiectul de act normativ urmează a fi prezentat Cancelariei de Stat pentru înregistrare în vederea examinării în ședința Secretarilor generali ai ministerelor.

Ulterior, potrivit prevederilor art. 32 din Legea nr. 100/2017 cu privire la actele normative și în conformitate cu procedurile stabilite de Regulamentul Guvernului, aprobat prin Hotărârea Guvernului nr. 610/2018, proiectul de act normativ și analiza de impact urmează a fi transmise pentru examinare în cadrul Ședinței secretarilor generali de stat, cu scopul înregistrării oficiale a proiectului de către Cancelaria de Stat și, în cazul susținerii, lansării acestuia în avizări și consultări publice oficiale. Proiectul și analiza de impact urmează a fi lansate în consultări publice, publicate pe portalul particip.gov.md, inclusiv consultate suplimentar în cadrul meselor rotunde cu persoanele ce vor fi vizate de proiectul propus, în scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional.

c) Expuneți succint poziția fiecărei entități consultate față de documentul de analiză a impactului și/sau intervenția propusă (se expune poziția a cel puțin unui exponent din fiecare grup de interese identificat)

Poziția fiecărei entități consulate urmează a fi analizată după consultarea publică a documentului de analiză a impactului și a proiectului de act normativ propus.

Anexă
Tabel pentru identificarea impacturilor

Categorii de impact	**Punctaj atribuit**			
	Opțiunea propusă	*Opțiunea alternativă 1*	*Opțiunea alternativă 2*	*Opțiunea alternativă 3*
Economic				
costurile desfășurării afacerilor	0	0	0	0
povara administrativă	-1	-1	-2	-2
fluxurile comerciale și investiționale	0			
competitivitatea afacerilor	0			

activitatea diferitor categorii de întreprinderi mici și mijlocii	+1	+1	+1	+1
concurența pe piață	0	0	0	0
activitatea de inovare și cercetare	+1	+1	+1	+1
veniturile și cheltuielile publice	-1	-2	-2	+1
cadrul instituțional al autorităților publice	+3	+2	+1	+1
alegerea, calitatea și prețurile pentru consumatori	0	0	0	0
bunăstarea gospodăriilor casnice și a cetățenilor	0	0	0	0
situația social-economică în anumite regiuni	0	0	0	0
situația macroeconomică	0	0	0	0
alte aspecte economice	0	0	0	0
Social				
gradul de ocupare a forței de muncă	0	0	0	0
nivelul de salarizare	0	0	0	0
condițiile și organizarea muncii	0	0	0	0
sănătatea și securitatea muncii	0	0	0	0
formarea profesională	0	0	0	0
inegalitatea și distribuția veniturilor	0	0	0	0
nivelul veniturilor populației	0	0	0	0
nivelul sărăciei	0	0	0	0
accesul la bunuri și servicii de bază, în special pentru persoanele social-vulnerabile	0	0	0	0
diversitatea culturală și lingvistică	0	0	0	0
partidele politice și organizațiile civice	0	0	0	0
sănătatea publică, inclusiv mortalitatea și morbiditatea	0	0	0	0
modul sănătos de viață al populației	0	0	0	0
nivelul criminalității și securității publice	+3	+3	+3	+3
accesul și calitatea serviciilor de protecție socială	+1	+1	+1	+1
accesul și calitatea serviciilor educaționale	0	0	0	0
accesul și calitatea serviciilor medicale	0	0	0	0
accesul și calitatea serviciilor publice administrative	+1	+1	+1	+1
nivelul și calitatea educației populației	0	0	0	0
conservarea patrimoniului cultural	0	0	0	0
accesul populației la resurse culturale și participarea în manifestații culturale	0	0	0	0
accesul și participarea populației în activități sportive	0	0	0	0
discriminarea	0	0	0	0
alte aspecte sociale	0	0	0	0
De mediu				
clima, inclusiv emisiile gazelor cu efect de seră și celor care afectează stratul de ozon	0	0	0	0
calitatea aerului	0	0	0	0
calitatea și cantitatea apei și resurselor acvatice, inclusiv a apei potabile și de alt gen	0	0	0	0
biodiversitatea	0	0	0	0
flora	0	0	0	0
fauna	0	0	0	0
peisajele naturale	0	0	0	0
starea și resursele solului	0	0	0	0
producerea și reciclarea deșeurilor	0	0	0	0

utilizarea eficientă a resurselor regenerabile și neregenerabile	0	0	0	0
consumul și producția durabilă	+1	+1	+1	+1
intensitatea energetică	0	0	0	0
eficiența și performanța energetică	0	0	0	0
bunăstarea animalelor	0	0	0	0
riscuri majore pentru mediu (incendii, explozii, accidente etc.)	0	0	0	0
utilizarea terenurilor	0	0	0	0
alte aspecte de mediu	0	0	0	0
Tabelul se completează cu note de la -3 la +3, în drept cu fiecare categorie de impact, pentru fiecare opțiune analizată, unde variația între -3 și -1 reprezintă impacturi negative (costuri), iar variația între 1 și 3 – impacturi pozitive (beneficii) pentru categoriile de impact analizate. Nota 0 reprezintă lipsa impacturilor. Valoarea acordată corespunde cu intensitatea impactului (1 – minor, 2 – mediu, 3 – major) față de situația din opțiunea „a nu face nimic”, în comparație cu situația din alte opțiuni și alte categorii de impact. Impacturile identificate prin acest tabel se descriu pe larg, cu argumentarea punctajului acordat, inclusiv prin date cuantificate, în compartimentul 4 din Formular, lit. b[1]) și, după caz, b[2]), privind analiza impacturilor opțiunilor.				
Anexe				
Proiectul preliminar de act normativ				