Analiză de impact
la proiectul de lege privind securitatea cibernetică

Titlul analizei impactului (poate conţine titlul propunerii de act normativ):	Proiectul Legii privind securitatea cibernetică
Data:	23.12.2022
Autoritatea administraţiei publice (autor):	Ministerul Economiei
Subdiviziunea:	Direcția politici în domeniul tehnologiei informației și economiei digitale
Persoana responsabilă şi datele de contact:	Sergiu Florea, 022 250-618

Compartimentele analizei impactului

1. Definirea problemei

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

Problema principală care urmează a fi soluționată prin inițiativa de reglementare legală propusă poate fi descrisă ca fiind un nivel general insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor legate de securitatea rețelelor și a sistemelor informatice, ceea ce poate submina sau subminează buna funcționare, pe de o parte, a activității administrative, în mod special prestarea serviciilor publice, de către administrația publică centrală și locală, iar pe de altă parte buna funcționare a activității economice desfășurată de către întreprinderile din mediul privat, ceea ce afectează în consecință întreaga economie națională și, implicit, activitatea socială.

Această problemă fundamentală cuprinde un set de elemente componente specifice care necesită a fi puse în evidență pentru a releva importanța unei intervenții imediate pe dimensiunea instituirii consolidării și și asigurării unei funcționalități adecvate a mecanismului de asigurarea a securității cibernetice la nivel național, după cum urmează.

- disfuncționalități în activitatea economică a diferiților actori, de stat sau privați, activitate care e bazată din ce în ce mai mult pe producerea de bunuri și prestarea de servicii, prin utilizarea tot mai intensă a tehnologiilor informaționale;
- numărul, frecvența și complexitatea în creștere a incidentelor de securitate cibernetică;
- o percepere deficitară a întinderii fenomenului respectiv, a gravității impacturilor incidentelor de securitate cibernetică asupra vieții administrative, economice și sociale sau, cel puțin asupra gravității și complexității incidentelor;
- reziliența cibernetică scăzută a unor sectoare și domenii în care buna funcționare a securității rețelelor și sistemelor informatice este primordială pentru menținerea unei bune funcționări a activității economice, sociale, administrative sau de altă natură critică pentru întreaga țară
- un nivel scăzut de conștientizare comună a potențialului negativ pe care îl comportă contextul actual național și lipsa unor mecanisme viabile care să permită reacționarea comună, imediată și eficace în situații de criză.

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

Potrivit documentului de concept al proiectului Strategiei naționale de transformare digitală[1] industria tehnologiei informației și comunicațiilor (TIC) din Moldova a cunoscut o creștere dinamică, datorită cererii ridicate de pe piață, concurenței și efortului consolidat al tuturor actorilor implicați. Acesta generează anual circa 7% din Produsul Intern Brut (PIB) al țării, apropiindu-se de o valoare totală a veniturilor de circa 15 miliarde MDL sau 900 milioane USD.

[1] https://particip.gov.md/ru/document/stages/anunt-privind-initierea-elaborarii-strategiei-de-transformare-digitala-a-republicii-moldova-pentru-anii-20232030-stdm-2030/9355

Pe parcursul ultimilor 5 ani, piața de comunicații electronice a avut o perioadă de concurență și creștere agilă, poziționând țara în destinații de top pe dimensiunea Internet de mare viteză, accesibilitate, iar recent – cu disponibilitatea Internetului Gigabit. În perioada 2015-2020, motorul creșterii industriei TIC în Moldova a devenit sectorul tehnologiei informației (IT), care a crescut de patru ori, depășind telecomunicațiile. O politică și un cadru legislativ dedicat pentru tehnologia informației și industriile digitale au jucat un rol central în evoluția sa remarcabilă și dinamică. Comparând ponderea în PIB a sectorului IT în 2020 de circa 3,6% cu cea de 0,8% în 2013, când sectorul IT a fost declarat ca prioritate de politică, dinamica este remarcabilă. Creșterea în industria IT a fost determinată de avantajele Moldovei ca destinație de externalizare a serviciilor IT, bazate pe cost, locație și competențe, precum și de un regim fiscal și administrativ facilitat pentru rezidenții Virtual Moldova IT Park. Rapoartele globale privind digitalizarea (Indicele UN DESA e-Guvernare, Indicele de dezvoltare în rețea NRI, Indicele de țară digitală, etc.), rapoartele ANRCETI și sondajele naționale anuale ale Agenției de Guvernare Electronică (AGE) atestă realizări considerabile ale Republicii Moldova în accesul la internet și dispozitive IT, precum și crearea platformelor de e-guvernare.

Totuși, dezvoltarea rapidă a tehnologiei informației și comunicațiilor electronice și a proceselor de transformare digitală deși au adus beneficii indiscutabile în toate domeniile, în același timp, au fost însoțite de creșterea semnificativă și continuă a numărului de amenințări la adresa securității cibernetice.

Intensificarea digitalizării a avut drept consecință evoluția semnificativă a acestor amenințări. Criza provocată de pandemia COVID-19 a demonstrat importanța serviciilor electronice pentru populație, sectorul public și privat. Totodată această criză ne-a demonstrat cât de rapid pot evolua amenințările la adresa securității cibernetice și cât de sensibile sunt serviciile electronice și economia digitală în fața acestor provocări cibernetice.

Spre exemplu raportul de evaluare[2] efectuat de ITU arată o imagine de ansamblu asupra amenințărilor cibernetice în Republica Moldova. La fel ca în alte țări, Moldova este afectată de diferite tipuri de atacuri cibernetice. Acestea vizează nu numai entitățile guvernamentale, ci și sectorul privat și populația în general. Deși autoritățile specializate urmăresc și monitorizează peisajul amenințărilor cibernetice legate de entitățile guvernamentale, lipsește o înțelegere holistică a atacurilor cibernetice care au loc în țară. Tipurile comune de incidente de securitate cibernetică sunt legate de: scams; phishing (including smishing and vishing); ransomware; web defacement; denial of service. Din 2015, țara s-a confruntat cu patru tipuri de atacuri, inclusiv DDOS, phishing, atacuri de forță brută care au încercat să obțină acces la sistemele informatice guvernamentale și deturnarea paginilor web oficiale. Sectorul privat este vizat în egală măsură de amenințările cibernetice. Între timp, IMM-urile se străduiesc să se apere și, prin urmare, reprezintă cea mai vulnerabilă parte a sectorului privat. Acest lucru ridică îngrijorări deosebite, deoarece în 2019 IMM-urile reprezentau aproximativ 98,6% din numărul total de întreprinderi[3], iar mai puțin de 17% dintre acestea au integrat cu succes tehnologiile digitale în activitatea lor. Acest lucru dezvăluie un potențial uriaș neexploatat, dar evidențiază și necesitatea urgentă a IMM-urilor de a-și transforma afacerile și de a adopta protocoale de securitate cibernetică.[4] IMM-urile sunt adesea victime ale atacurilor ransomware care au ca rezultat criptarea bazelor lor de date contabile. Cetățenii sunt, de asemenea, supuși atacurilor cibernetice, iar cele mai frecvente sunt vishingul și smishingul. Infractorii cibernetici au succes în aceste tipuri de atac datorită nivelului redus de cultură digitală și igiena cibernetică. Una dintre grupurile criminale prinse în 2021 pentru furt de bani din conturile bancare a folosit Viber pentru a contacta cetățenii și a se prezenta ca angajați ai băncii. Începând din 2020 și până în septembrie 2021 când au fost prinși, au făcut peste 40 de retrageri din conturile bancare ale mai multor persoane fizice.

Lipsa unor politici bine definite și reglementărilor naționale pune în pericol funcționarea economiei în Republica Moldova, în mod special a celei digitale. În acest sens, reziliența cibernetică

[2] Assessment Report of Moldova National Computer Incident Response Team (cirt-mdmd), ITU, septembrie 2022
[3] https://statistica.gov.md/newsview.php?l=ro&idc=168&id=6716
[4] https://www.odimm.md/ro/digitalizarea

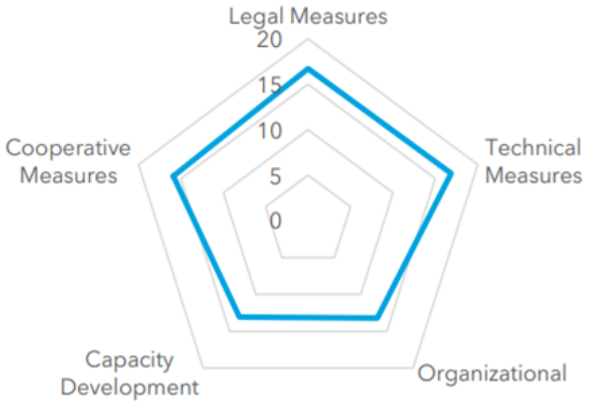
a persoanelor juridice (publice și private), care sunt prestatorii de servicii esențiale și critice pentru funcționarea economiei naționale și a statului în ansamblu, devine un element de importanță majoră.

Republica Moldova nu dispune de proceduri mature între autoritățile guvernamentale competente și marile întreprinderi critice pentru a coopera și a face schimb de informații fără întârzieri nejustificate, în special în ceea ce privește identificarea entităților critice, a riscurilor, a amenințărilor cibernetice și a incidentelor, precum și în ceea ce privește riscurile, amenințările și incidentele necibernetice care afectează entitățile critice, inclusiv măsurile de securitate cibernetică și fizică luate de entitățile critice, precum și rezultatele activităților de supraveghere desfășurate cu privire la astfel de entități

Conform Indicelui global de securitate cibernetică (GCI) al ITU pentru 2020, Moldova ocupă locul 33 în regiunea Europei și locul 63 la nivel mondial. GCI este o referință de încredere care măsoară angajamentul a 194 de țări față de securitatea cibernetică la nivel mondial, sporind în același timp gradul de conștientizare a importanței și dimensiunilor problemelor de securitate cibernetică și evaluând rezistența și fiabilitatea sectorului TIC al țărilor. Metodologia de evaluare a GCI analizează modul în care fiecare țară abordează aspectele legate de securitatea cibernetică în cadrul politicilor sale naționale. Aceasta se realizează cu ajutorul unui chestionar care abordează principalii factori care contribuie la gradul de pregătire al unei țări în materie de securitate cibernetică. Potrivit raportului de evaluare[5] efectuat de ITU în vederea instituirii la nivel național a unei echipe de răspuns la incidentele de securitate cibernetică, în pofida îmbunătățirilor în domeniul TIC, performanța Moldovei în cadrul Indexului global de securitate cibernetică (GCI) 2020 a scăzut. Acest declin poate fi atribuit în principal eliminării și adăugării de noi întrebări, precum și modificărilor aduse metodologiei și ponderării GCI. Cu toate acestea, Republica Moldova a înregistrat progrese semnificative începând cu 2015 în ceea ce privește măsurile legate de elaborarea și punerea în aplicare a politicilor interne, a acordurilor internaționale și a obligațiilor pentru a proteja infrastructura informațională critică a țării.

Performanța Republicii Moldova în Indexul Global al Securității Cibernetice (GCI)[6] pentru anul 2020 este ilustrată în imaginea de mai jos:

Moldova (Republic of)



Development Level:
Developed Country, Landlocked Country

Area(s) of Relative Strength
Legal, Technical Measures
Area(s) of Potential Growth
Organizational, Capacity Development Measures

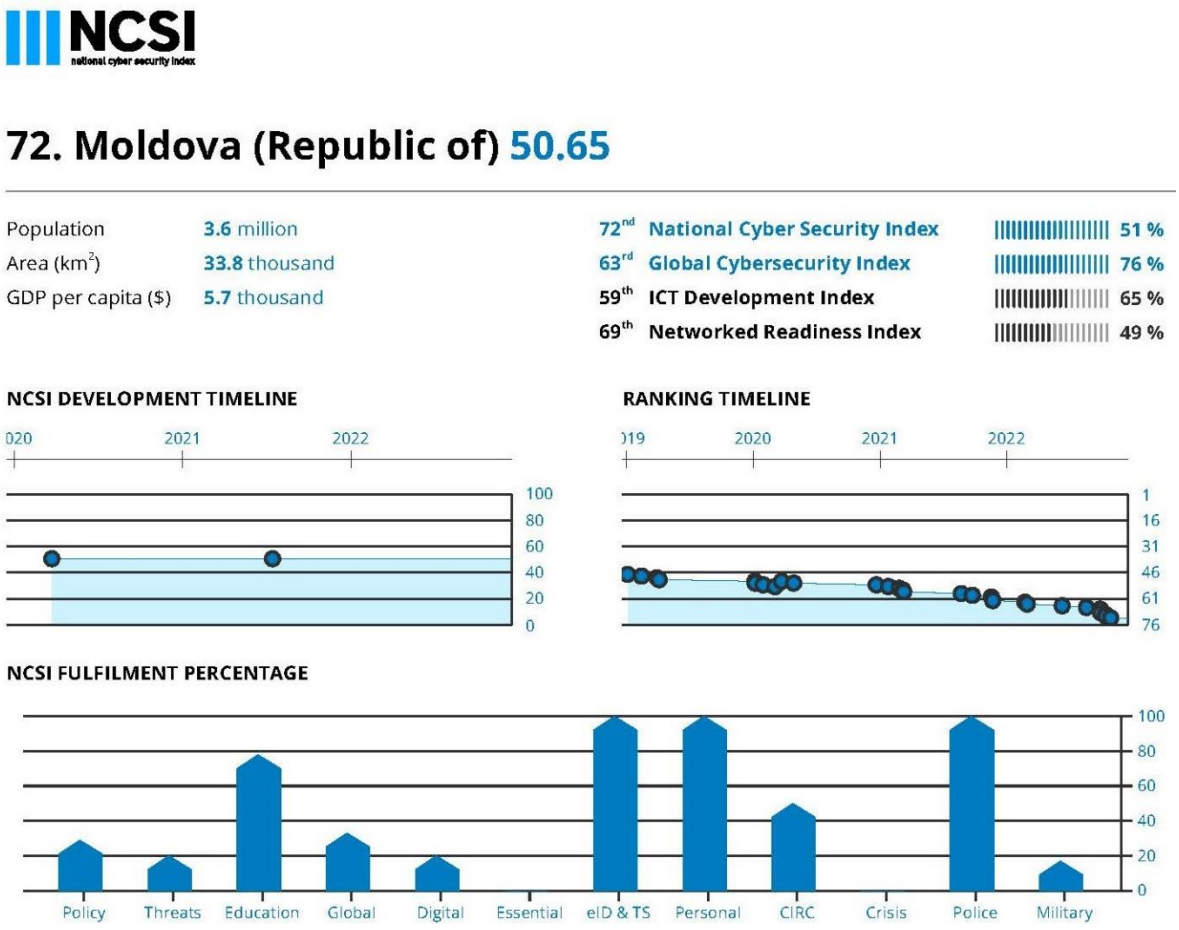
Overall Score	Legal Measures	Technical Measures	Organizational Measures	Capacity Development	Cooperative Measures
75.78	16.73	16.86	13.21	13.09	15.89

Source: ITU Global Cybersecurity Index v4, 2020

Acest grafic arată că Republica Moldova mai are loc pentru îmbunătățiri în anumiți piloni ai GCI. Printre aceștia se numără structurile de măsuri organizaționale și să adopte măsuri de evaluare a nivelului de dezvoltare a securității cibernetice la nivel național.

[5] Assessment Report of Moldova National Computer Incident Response Team (cirt-mdmd), ITU, septembrie 2022
[6] https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

În același context, evaluarea maturității în domeniul securității cibernetice a Republicii Moldova este reflectată și de indicele național de securitate cibernetică (NCSI)[7]. Acesta este un indice global în timp real, care măsoară gradul de pregătire a țărilor pentru a preveni amenințările cibernetice și a gestiona incidentele cibernetice. NCSI este, de asemenea, o bază de date cu materiale de evidență disponibile publicului și un instrument pentru consolidarea capacităților naționale în domeniul securității cibernetice. În figura de mai jos este reflectată poziția Republicii Moldova și principalii indicatori care reflectă maturitatea țării în materie de securitate cibernetică.



Restanțele cele mai accentuate sunt dezvoltarea politicilor de securitate cibernetică, analiza amenințărilor cibernetice și a informațiilor, protecția serviciilor digitale, cooperarea militară în domeniul cibernetic, care sunt situate sub nivelul de 30%, iar protecția serviciilor esențiale și managementul crizelor de securitate cibernetică având valoarea 0%.

c) Expuneți clar cauzele care au dus la apariția problemei

Problematica enunțată și descrisă în subcompartimentele anterioare, rezumată la reziliența cibernetică scăzută a actorilor esențiali, perturbarea activității cărora ar putea prejudicia considerabil viața economică și socială caracterizată în mod special printr-un nivel insuficient de protecție împotriva incidentelor, riscurilor și amenințărilor la securitatea rețelelor și a sistemelor informatice ale acestora are la bază o serie de cauze, principalele dintre care constau în următoarele:

1. lipsa unui cadru instituțional și normativ care să stabilească în mod clar responsabilitățile și, implicit, acțiunile ce necesită a fi întreprinse în caz de incidente și crize de securitate cibernetică atât de autoritățile administrației publice cât și de către diverși actori din sectorul privat.
2. Absența unei echipe de răspuns la incidentele de securitate cibernetică la nivel național (CSIRT național), al cărui obiectiv principal este de a spori siguranța, securitatea și

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

protecția digitală a țării și are un mandat oficial formal pentru a îndeplini o astfel de responsabilitate la nivel național.

3. măsuri de securitate a rețelelor și sistemelor informatice și cerințe față de astfel de măsuri insuficiente sau chiar lipsa acestora, ale unor actori din sectorul privat, a căror activitate poate fi calificată ca fiind esențială în prestarea unor servicii;
4. schimbul insuficient de informații cu privire la incidente, riscuri și amenințări de securitate cibernetică. Majoritatea breșelor de securitate nu sunt raportate și trec neobservate, în principal din cauza reticenței companiilor de a împărtăși aceste informații, de teama daunelor aduse reputației sau a răspunderii. De cele mai multe ori, persoanele responsabile de securitatea rețelelor și a sistemelor informatice împărtășesc informațiile relevante doar cu grupuri mici pe care le consideră de încredere, mai degrabă decât să treacă prin canalele oficiale. Schimbul insuficient de informații cu privire la amenințări și riscuri duce la o pregătire insuficientă, iar schimbul insuficient de informații cu privire la incidente duce la o reacție insuficientă. Indisponibilitatea unor date și informații fiabile privind amenințările și incidentele de securitate cibernetică împiedică autoritățile publice responsabile să elaboreze politici bazate pe date concrete și să reacționeze în timp util la incidentele care afectează rețelele guvernamentale.
5. De asemenea, nu există în prezent un cadru instituțional, procedural și normativ-juridic pentru schimbul de informații de încredere privind amenințările, riscurile și incidentele de securitate între sectorul public și cel privat.
6. lipsa unui cadru coerent de gestionare a crizelor de securitate cibernetică în caz de incidente cibernetice de mare amploare sau care ar putea sau au impact semnificativ asupra sectoarelor critice;
7. Lipsa unor norma legale primare privind obligativitatea implementării de către furnizorii de servicii esențiali a unor măsurilor de asigurare a securității cibernetice, precum și a unui mecanism, inclusiv a unei autorități competente în exercitarea funcției de supraveghere și control a modului de implementare a unor astfel de mecanisme.

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

Problematica asigurării securității informaționale a țării a constituit totdeauna o preocupare în legătură cu procesul de transformare digitală a țării. Această preocupare a fost reflectată de-a lungul anilor în documentele de politici, ca parte componentă a procesului de dezvoltare a societății informaționale în Republica Moldova, reflectată în documente de politici precum Strategia Națională de edificare a societății informaționale – "Moldova electronică", Strategia națională de dezvoltare a societății informaționale "Moldova Digitală 2020", Programul de modernizare tehnologică a Guvernării, etc.

Cu toate acestea o abordare oficială mai pronunțată față de domeniul securității cibernetice și problematicii acestuia a fost acordată odată cu adoptarea de către Parlament, în anul 2017 a Concepției securității informaționale a Republicii Moldova și, în anul 2018, de către Guvern, a Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, obiectivul de bază al căruia a constituit crearea unui sistem de management al securității cibernetice a Republicii Moldova prin securizarea serviciilor societăți informaționale, contribuind astfel la dezvoltarea unei economii bazate pe cunoaștere, ceea ce, la rândul său, va stimula creșterea gradului de competitivitate economică și de coeziune socială, precum și va asigura crearea de noi locuri noi de muncă.

Actualmente, aceleași obiective sunt consacrate și în Strategia securității informaționale una dintre problemele de bază identificate de aceasta fiind lipsa unei entități de tip CERT (Centru de reacție la incidente de securitate cibernetică), la nivel național, responsabile de prevenirea și reacția la incidente din domeniul securității cibernetice.

Deși un set de acțiuni în conformitate cu aceste documente de politici au fost întreprinse de către autoritățile responsabile totuși până în prezent, în Moldova nu s-a reușit crearea sau stabilirea unei autorității competente pe domeniul securității cibernetice la nivel național.

Această situație limitează autoritățile publice responsabile în realizarea misiunii de care sunt responsabile – realizarea politicii de stat în domeniul securității cibernetice. În cazul lipsei

elementelor menționate, sectorul public și privat, precum și societatea vor fi supuse în continuare unor riscuri majore aferente amenințărilor de securitate cibernetică.

Un element negativ este lipsa totală a sistemului de răspuns la incidentele de securitate cibernetică la nivel național, precum și lipsa suportului eficient pentru mediul de afaceri.

Lipsa unor reguli de protecție a rețelelor și sistemelor informatice și de prevenție a incidentelor va duce la devieri de la entitate la entitate. Respectiv schimbul de informații (cel voluntar) ar putea fi inutil din motivul perceperii diferite și neconcordanțelor între procedurile interne ale entităților.

În special este de menționat un alt element negativ prin prisma situației geopolitice în regiune, când sectorul public nu va dispune de instrumente de comunicare transparentă cu alte state și de asigurare a schimbului de informații privind incidentele și vulnerabilitățile, asigurând interesele sectorului public și mediului de afaceri din Moldova.

Lipsa reglementării domeniului securității cibernetice va vulnerabiliza autoritățile publice, persoane fizice și persoane juridice în față provocărilor de securitate cibernetică, care sunt permanent în creștere.

Pentru entitățile esențiale și importante, impactul monetar al unei încălcări a datelor este substanțial. Cel mai recent raport *IBM Cost of a Data Breach*[8] a stabilit că în anul 2022 costul mediu al unei încălcări a datelor la nivel global a atins un maxim istoric de 4,35 milioane USD. Această cifră reprezintă o creștere cu 2,6% față de anul precedent și o creștere cu 12,7% față de anul 2020.

Raportul respectiv evidențiază principalii factori care contribuie la costurile mai mari ale încălcării datelor, privite prin prisma sectoarelor și regiunilor geografice și detaliază măsurile pe care organizațiile le pot lua pentru a minimiza riscurile de încălcare a securității:

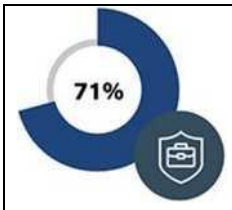
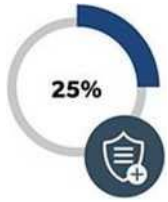
- Costurile suportate privind încălcarea datelor sunt cu 3,05 milioane USD mai mici pentru în cazul organizațiile care folosesc instrumente de inteligență artificială (AI) și automatizare;
- Organizațiile care au o echipă CSIRT și își testează în mod regulat planul de răspuns la incidente au economisit în medie 2,66 milioane USD;
- Organizațiile care au implementat o arhitectură de încredere zero au în medie cu 1 milion USD mai puțin în costuri de încălcare;
- Tehnologiile de detectare și răspuns extinse (XDR) au ajutat la economisirea în medie de 29 de zile în timpul de răspuns la încălcare.

Raportul IBM din 2022 a citat mai multe componente contributive care afectează costurile de încălcare a datelor. Costul mediu al unei breșe de date pentru organizațiile cu infrastructură critică a fost în general de 4,82 milioane USD - cu 1 milion USD mai mult decât costul mediu pentru organizațiile din alte industrii. Costul mediu al unui atac de phishing în 2022 a fost calculat la 4,91 milioane USD, comparativ cu 4,54 milioane USD pentru ransomware și 4,50 milioane USD pentru acreditările furate sau compromise.

Potrivit raportului, în timp ce costurile de încălcare a datelor asociate cu reputația deteriorată, timpul de oprire a afacerii și reglementările/litigiile rămân semnificative, o tendință mai recentă este o creștere bruscă a costurilor primelor de asigurare cibernetică din cauza frecvenței și gravității încălcărilor, împreună cu plățile considerabile pentru ransomware. Pe tema ransomware-ului, dovezile sugerează că companiile sunt din ce în ce mai deschise să plătească răscumpărări ca parte a răspunsului lor la încălcare, chiar și alocă milioane de dolari în acest scop. Conform raportului IBM din 2022, 62% dintre cele 550 de organizații care suferă de încălcări studiate au declarat că nu au suficient personal pentru a-și satisface nevoile de securitate.

Potrivit *Consultancy.eu*, care este o platformă online pentru industria de consultanță, costurile și cheltuielile asociate unui incident cibernetic pot fi clasificate în patru segmente de mai jos.

[8] https://www.ibm.com/downloads/cas/3R8N1DZJ

	**Asistență și măsuri de urgență** • Identificarea, evaluarea și limitarea evenimentului de securitate (IT Forensic) • Furnizarea de asistență juridică (Încălcarea confidențialității datelor) • Furnizarea de asistență pentru gestionarea crizelor sau comunicare
	**Costuri adiționale** • Restabilirea sistemului informatic la starea sa anterioară • Menținerea operabilității sistemului IT • Pregătirea cererii • Prevenirea sau limitarea răspunderii/detectarea și controlul oricărei utilizări necorespunzătoare a datelor cu caracter personal (încălcarea datelor). • Strategie de comunicare • Notificare către autoritate sau către persoane fizice (încălcarea datelor) • Răscumpărare • Costurile de apărare rezultate în urma unei investigații efectuate de o autoritate de reglementare • Amenzi din partea autorităților naționale, pentru încălcarea drepturilor de protecție a datelor cu caracter personal
	**Acoperire de răspundere** Cheltuieli de apărare și daune care decurg din pretenții formulate de terți: • Un eveniment de securitate • Încălcare a confidențialității datelor cu caracter personal • Defăimarea, deteriorarea reputației, încălcarea proprietății intelectuale, încălcarea vieții private etc
	**Pierderea cifrei de afaceri și creșterea costului muncii** • Întreruperea afacerii • Cheltuieli suplimentare

Incapacitatea întreprinderilor și a autorităților de a reacționa rapid la un incident și de a atenua impactul acestuia vor conduce, cel mai probabil, la o descreștere a încrederii generale a cetățenilor în economia digitală, ceea ce ar putea avea un impact negativ asupra creșterii economice și a investițiilor.

Situația poate, de asemenea, alimenta în continuare criminalitatea informatică, extremism, pericolul terorismului, alte fenomene negative, precum și război hibrid.

Situația existentă nu va preveni eventualele pierderi financiare cauzate de atacurile cibernetice, cum și nu va duce la prevenirea riscurilor/daunelor de mediu în cazul unui atac asupra unui serviciu esențial.

Respectiv, incidentele de securitate cibernetică vor provoca imediat sau vor avea potențialul de a provoca perturbări operaționale sau pierderi financiare substanțiale la diferite nivele ale oricărei entități și chiar la nivel de economie națională.

Ca urmare a incidentului vor fi afectate direct sau cel puțin indirect alte persoane fizice sau juridice, cauzând pierderi materiale sau morale considerabile.

Pentru mediul privat în continuare vor surveni daune din cauza perturbării serviciilor digitale drept rezultat al incidentelor de securitate cibernetică, fiind necesare investiții enorme pentru asigurarea securității cibernetice proprii din motivul lipsei suportului din partea autorităților.

Pentru mediul public, aceasta ar însemna, de asemenea, un risc de creștere a cheltuielilor bugetare pentru atenuarea ad-hoc a amenințărilor, precum și costuri suplimentare pentru soluționarea situațiilor de urgență legate de incidentele de securitate cibernetică.

Pentru societate, lipsa unei abordări a incidentelor de securitate cibernetică va duce la pierderii de venituri datorate perturbărilor economice potențiale.

e) Descrieți cadrul juridic actual aplicabil raporturilor analizate şi identificați carenţele prevederilor normative în vigoare, identificați documentele de politici şi reglementările existente care condiţionează intervenţia statului

<u>Cadrul de politici și cadrul normativ</u>

Cadrul politicii de securitate cibernetică este oferit de un set de documente de politică 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 oferit de documentele de politici legi și:

Concepția securității informaționale[9], 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 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[10] 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 Strategiei securității informaționale a Republicii Moldova pentru anii 2019–2024 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

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

[10] https://www.legis.md/cautare/getResults?doc_id=111979&lang=ro

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[11]
- Strategia Națională de Apărare și Planul de Acțiuni privind implementarea Strategiei Naționale de Apărare 2018–2022, aprobate prin Hotărârea Parlamentului nr. 134/2018[12]
- Planul individual de acțiuni de parteneriat Republica Moldova – NATO pentru anii 2022–2023, aprobat prin Hotărârea Guvernului nr. 26/2022[13].

Din perspectiva **cadrului normativ, l**a nivel național, Republica Moldova nu are o lege-cadru care să reglementeze sistemic problemele de securitate cibernetică. Normele juridice care reglementează aspectele organizatorice, instituționale și funcționale în domeniul asigurării protecției și securității rețelelor și sistemelor informaționale sunt dispersate în câteva în legi.

Legea nr. nr 467/2003[14] cu privire la informatizare si resursele informaționale de stat (art.23) și **Legea nr. 71/2007[15] 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***[16]. 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

[11] https://www.legis.md/cautare/getResults?doc_id=105346&lang=ro
[12] https://www.legis.md/cautare/getResults?doc_id=110013&lang=ro
[13] https://www.legis.md/cautare/getResults?doc_id=129865&lang=ro
[14] https://www.legis.md/cautare/getResults?doc_id=132933&lang=ro
[15] https://www.legis.md/cautare/getResults?doc_id=131038&lang=ro
[16] https://www.legis.md/cautare/getResults?doc_id=133262&lang=ro

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**[17] 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** [18]privind aprobarea măsurilor necesare asigurării securității cibernetice la nivel guvernamental, care completează, în special, cu măsuri organizatorice decizia sus-menționată, dar numai pentru autoritățile și instituțiile publice care fac parte din structura administrativă guvernamentală;
- **Hotărârea Guvernului Decizia nr. 388/2022**[19] 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.

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[20]. 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.

Viceprim-ministru pentru digitalizare, activează conform domeniilor de competență stabilite prin Hotărârea Guvernului nr. 118/2021, printre care - aplicarea tehnologiei informației în sectorul public, precum și dezvoltarea societății informaționale. În virtutea atribuțiilor date, coordonează activitatea STISC și AGE.

Ministerul Economiei este autoritatea administrației publice centrale de specialitate responsabilă de elaborarea documentelor de politici și actelor normative în domeniul informatizării, resurselor și sistemelor informaționale de stat, dezvoltării industriei tehnologiei informației, economiei digitale.

Ministerul Infrastructurii și Dezvoltării Regionale 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

[17] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro
[18] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro
[19] https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro
[20] https://www.legis.md/cautare/getResults?doc_id=132064&lang=ro

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.[21] În cadrul STISC funcționează **CERT-Gov[22]** . CERT-Gov[23] 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 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 (Hotărârea de Guvern nr.760/2010 [24]privind organizarea și funcționarea Agenției de E-Guvernare) 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). (anexa nr. 4 la Hotărârea Guvernului nr. 414/2018[25]). De asemenea, Agenția are și responsabilități ce țin de asigurarea securității informației în autoritățile și instituțiile din sectorul public. Agenția de e-Guvernare împreună cu partenerii săi ia măsuri juridice, organizatorice și tehnice complexe de garantare a securității informațiilor [26]. 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) avea un rol important în protejarea infrastructurii critice din țară, precum și a sistemelor speciale de telecomunicații [27]. 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 Economiei privind CIIP. Potrivit informațiilor de la mai multe părți interesate, SIS nu a avut rolul de lider în dezvoltarea CIIP și armonizarea legislației moldovenești cu Directiva NIS. Potrivit pct. 115 din Strategia de securitate a informațiilor, Serviciul de Securitate și Informații are rolul principal în procesul de monitorizare și coordonare a implementării Strategiei de securitate a informațiilor 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 cazurile de criminalitate informatică, cu

[21] https://www.legis.md/cautare/getResults?doc_id=128904&lang=ro
[22] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro
[23] https://stisc.gov.md/ro/cert-gov-md
[24] https://www.legis.md/cautare/getResults?doc_id=130646&lang=ro
[25] https://www.legis.md/cautare/getResults?doc_id=128904&lang=ro
[26] http://www.egov.md/en/about
[27] https://www.legis.md/cautare/getResults?doc_id=129284&lang=ro

investigarea întregului spectru de infracțiuni prevăzute de articolul 2-10 Convenția de la Budapesta, precum și a infracțiunilor conexe împotriva sau cu utilizarea sistemelor informatice și a datelor.

Agenția Națională de Reglementare pentru Comunicații Electronice și Tehnologia Informației[28] (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[29]. Cu toate acestea, această entitate este autonomă față de Guvern în activitatea sa de reglementare. Potrivit legii, Agenția aprobă regulile [30]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.[31]

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 propriul CERT 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)

Obiectivul general al intervenției preconizate este creșterea nivelului de reziliență cibernetică a serviciilor critice pentru întreaga societate, în ambele sectare privat sau public, asigurând un nivel ridicat de protecție a rețelelor și sistemelor informatice ale furnizorilor de servicii utilizate în procesul de prestare a serviciilor lor.

Ca **obiective specifice** care odată realizate vor asigura atingerea obiectivului general enunțat mai sus ținem să evidențiem următoarele:

- Instituirea/desemnarea unei autorități competente în domeniul securității cibernetice cu funcții de supravegherea și control, identificare și menținere în stare de actualitate a listei furnizorilor de servicii, interacțiune strategică la nivel internațional și schimb de experiență cu organizații, state sau alte entități relevante la nivel european în primul rând, uniformizare a practicilor în gestionarea incidentelor cibernetice și coordonarea operațională a situațiilor de criză
- Desemnarea/ instituirea unei CSIRT cu competențe la nivel național, asigurarea recunoașterii internaționale a acesteia, în mod special la nivel european, care să exercite monitorizează și analizează amenințările cibernetice, vulnerabilitățile și incidentele cibernetice la nivel național răspunsul la incidente cibernetice, asigurarea schimbului de informații și coordonare a procesului de divulgare a vulnerabilităților; Pentru ca un CSIRT național să fie eficient în interiorul țării sale, acesta ar trebui să stabilească și să mențină relații bune cu părțile interesate naționale și transnaționale, inclusiv cooperarea cu alte echipe naționale și CSIRT - atât în regiunea sa geografică, cât și la nivel mondial;
- Implementarea unor măsuri de securitate de către furnizorii de servicii care să asigure atingerea unui nivel minim comun de securitate a rețelelor și sistemelor informaționale proprii ceea ce implicit va acea ca efect creșterea nivelului de pregătire și de răspuns la incidentele cibernetice și amenințările de acest fel.
- Asigurarea unei cooperări 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;
- Dezvoltarea unor capabilități înalte de reacție la incidentele semnificative sau care ar putea avea impacturi cu potențiale prejudicii considerabile, atât autorităților responsabile

[28] https://en.anrceti.md/informatie_sumara
[29] https://www.legis.md/cautare/getResults?doc_id=125209&lang=ro
[30] https://www.legis.md/cautare/getResults?doc_id=119924&lang=ro
[31] https://en.anrceti.md/node/35

de implementarea politicii de stat în domeniul securității cibernetice, cât și furnizorilor de servicii.

În același context este necesar de evidențiat că un obiectiv convergent al contextului expus îl constituie necesitatea, având în vedere statutul de țară candidat pentru aderarea la Uniunea Europeană a Republicii Moldova, alinierii legislației naționale la legislația Uniunii Europene, transpunerea Directivei (UE) 2022/... a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (*Directiva NIS 2*) având un caracter de prioritate națională în domeniul securității cibernetice.

3. Identificarea opţiunilor

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

Opțiunea respectivă presupune păstrarea status-quo-ului actual, fără o intervenție la nivel normativ, instituțional și organizatoric. În această situație autoritățile responsabile de realizarea politicii de stat în domeniul securității cibernetice urmează să continue activitățile orientate spre asigurarea unui nivel adecvat de securitate a rețelelor și sistemelor informatice, astfel încât prestare serviciilor esențiale să aibă un caracter continuu. Schimbul de informații între diverși furnizori de servicii și actori statali urmează în continuare să aibă loc, în ce privește sectorul privat, pe baze preponderent de voluntariat. Din această perspectivă, în ce privește furnizorii de servicii esențiale din mediul privat, funcția de supraveghere și control al autorităților competente va fi afectată de lipsa unor reglementări legale coerente, care să constituie temeiul juridic primordial de exercitare a unor astfel de competențe.

Deși măsuri susținute au fost întreprinse pentru îmbunătățirea gestionarii riscurilor și incidentelor cibernetice în sectorul public, totuși având în vedere interconexiunile TIC din domeniul public cu cel privat și caracterul intersectorial și chiar transfrontalier al amenințărilor și incidentelor de securitate cibernetică, o creștere a nivelului de protecție cibernetică la nivel național este un obiectiv greu de realizat dacă nu chiar imposibil fără perfecționarea mecanismelor de interacțiune, de responsabilizare, de schimb de informații obligatoriu și, în ultimă instanță de supraveghere și control al acestora.

De asemenea, păstrarea situației actuale va influența credibilitatea țării pe plan internațional, în mod deosebit din punctul de vedere operațional ce ține de schimbul de informații cu partenerii europeni și internaționali în domeniul securității cibernetice.

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

Aprobarea unei legi cadru care să reglementeze domeniul securității cibernetice are ca obiectiv principal ca prin implementarea cerințelor, măsurilor și mecanismelor legale instituite să se asigure un nivel înalt de securitate cibernetică a rețelelor și sistemelor informatice în Republica Moldova, capabil să asigure protecția intereselor vitale ale persoanelor fizice și juridice, ale societății și ale statului, precum și a intereselor naționale ale Republicii Moldova în spațiul cibernetic.

Proiectul de lege are ca ***obiect de reglementare*** cadrul juridic, organizațional și de cooperare în domeniul securității cibernetice a persoanelor juridice de drept public și a persoanelor juridice de drept privat, stabilește competența acestora în materie de securitate cibernetică, determină cadrul național general de gestionare a crizelor în domeniul securității cibernetice, instituie cerințe, măsuri și mecanisme pentru asigurarea securității rețelelor și sistemelor informatice care sunt esențiale pentru funcționarea societății, precum și stabilește modul de gestionare a incidentelor cibernetice.

Proiectul este structurat în 6 capitole după cum urmează:

În ***capitolul I – Dispoziții generale*** sunt reglementate aspecte ce țin de domeniul de aplicare al legii, principalele noțiuni utilizate și definițiile acestora, aspecte generale privind procesul de identificare a persoanelor juridice asupra cărora prevederile legii urmează să fie aplicate, precum și principiile generale conform cărora subiecții legii urmează să le aplice în procesul de asigurare a securității cibernetice.

Acest capitol de asemenea stabilește principalele criterii în baza cărora autoritatea competentă urmează să identifice persoanele juridice ca furnizori de servicii, criterii ce au la bază regula principală a dimensiunii organizației, dar și criterii specifice precum categoria de servicii prestate (ex. prestatorii de servicii de încredere, furnizorii de rețele și servicii de comunicații electronice accesibile publicului, etc), calitatea prestatorului de servicii (operator al obiectivelor infrastructurii critice), impact pe care l-ar putea avea perturbarea prestării serviciului, dependența serviciului de rețelele și sistemele informatice, importanța și interconexiunile cu alte servicii sau sectoare și subsectoare.

Capitolul II „Cadrul instituțional, cooperarea și coordonarea strategică la nivel național" cuprinde norme juridice ce reglementează problematice generale ale raporturilor juridice instituite în procesul de planificare și coordonare strategică în domeniul securității cibernetice la nivel național, inclusiv competența Guvernului de aprobare a Strategiei naționale de securitate cibernetică, misiunea Consiliului coordonator în domeniul securității informaționale, aspecte funcționale ale Autorității competente în domeniul reglementat de prevederile legii, modul de instituire/desemnare, atribuții specifice funcției de CSIRT național și de punct unic de contact la nivel național. De asemenea capitolul vizat stabilește norma legale primare de reglementare a cadrului național general de gestionare a crizelor în materie de securitate cibernetică, inclusiv responsabilitatea autorității de a aproba Planul național de răspuns la incidentele și crizele de securitate cibernetică, în baza cadrului metodologic aprobat de Guvern în ce privește elaborarea, actualizarea și implementarea prevederilor acestui plan. În același context, în acest capitol sunt propuse reglementări fundamentale ce vizează instituirea, organizarea și funcționarea Registrului de stat al incidentelor cibernetice și a sistemului informațional ce-l formează.

Capitolul III – Obligații privind asigurarea securității cibernetice – cuprinde reglementări privind măsurile obligatorii de securitate ce urmează a fi întreprinse de către persoanele juridice, identificate de autoritatea competentă ca furnizorii de servicii, pentru a asigura un nivel înalt de securitate a rețelelor și sistemelor informatice proprii, responsabilitățile acestora în legătură cu măsurile respective, aspecte procedurale generale și obligațiile concrete în procesul de gestionare a incidentelor cibernetice semnificative, responsabilitățile în relațiile cu persoanele juridice terțe care nu cad sub incidența prevederilor legii.

De asemenea, capitolul cuprinde reglementări generale privind asigurarea de către echipa de răspuns la incidente cibernetice a autoritatea competentă a procesului de gestionare a acțiunilor orientate spre prevenirea și soluționarea a incidentelor, dar și spre prevenirea și atenuarea impactului asupra continuității serviciului sau a securității rețelei și/sau a sistemului informatic cauzat de un incident cibernetic.

De rând cu acestea, acest capitol include și prevederi privind notificarea voluntară, ceea ce dreptul furnizorilor de servicii să notifice autoritatea competentă cu privire la incidente cibernetice, amenințări cibernetice și incidente evitate la limită, iar persoanele juridice de drept public sau de drept privat care nu sunt identificate de autoritatea competentă ca furnizori de servicii – să transmită acesteia notificări cu privire la incidente cibernetice semnificative, amenințările cibernetice și incidentele evitate la limită.

În contextul acestor reglementări, capitolul în speță abordează și problematica schimbului de informații voluntar, prin instituirea contextului juridico-normativ suficient pentru crearea unor comunități și platforme de schimb de informații, între furnizorii de servicii și dintre aceștia și alte persoane juridice care nu intră în domeniul de aplicare al prezentei legi. Astfel subiecții respectivi pot face schimb reciproc de informații relevante în materie de securitate cibernetică, în mod voluntar, inclusiv de informații referitoare la amenințări cibernetice, incidente evitate la limită, vulnerabilități, tehnici și proceduri, indicatori de compromitere, tactici adversariale, informații specifice actorului care generează amenințări, alerte de securitate cibernetică și recomandări privind configurația instrumentelor de securitate cibernetică pentru detectarea atacurilor cibernetice. Conform proiectului de act normativ autoritatea competentă trebuie să intermedieze acest schimb de informații prin crearea și gestionarea unor platforme, inclusiv tehnico-tehnologice, și comunități de încredere, iar pentru a asigura protecția informațiilor ce au un caracter potențial sensibil, autoritatea competentă urmează să-și aroge funcția de a facilita semnarea acordurilor de schimb de informații între participanții la astfel de platforme și comunități.

În ***Capitolul IV – Supraveghere și control de stat*** sunt cuprinse normele juridice ce reglementează aspectele privind exercitarea de către autoritatea competentă a funcțiilor de supraveghere și control de stat. Astfel aceste funcții urmează a fi realizate prin monitorizarea continuă a modului în care aceștia realizează obligațiile ce le revin conform prevederilor prezentei legi și a actelor normative de punere în aplicare a acesteia. Atunci când un furnizor de servicii responsabil de gestionarea incidentului cibernetic nu este în măsură să răspundă sau să soluționeze în timp util un incident cibernetic, autoritatea competentă asigură aplicarea măsurilor necesare pentru soluționarea incidentului cibernetic utilizând, dacă este necesar, asistență profesionistă terță.

În același context, pentru a contracara o amenințare gravă imediată asupra securității rețelelor și sistemelor informatice sau pentru a elimina o perturbare gravă în cazul unui incident cibernetic sunt stabilite expres condițiile în care autoritatea competentă poate restricționa utilizarea sau accesul la un sistem informatic. În ce privește controlul sunt stabilite reglementările primare minime necesare pentru asigurarea legalității intervenției autorității competente pe această dimensiune.

În ambele cazuri, ale supravegherii controlului de stat, pentru implementarea prevederilor legii conform articolelor corespunzătoare din capitolul respectiv al proiectului de lege, Guvernul urmează să adopte acte normative care să reglementeze mai detaliat modul de aplicare a măsurilor de supraveghere și modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin.

Capitolul V – Răspunderea – abordează generic, în scop de interconexiune cu legislația cadru din domeniul administrativ, contravențional, penal și de altă natură, problematica răspunderii, pe de o parte a autorității competente inclusiv a personalului acesteia, iar pe de altă parte a persoanelor juridic care cad sub incidența prevederilor legii în calitate de furnizori de servicii, inclusiv angajații acestora.

Capitolul VI – Dispoziții finale și tranzitorii – prevede termenul de intrare în vigoare al legii – 1 an din data publicării, precum și termenele concrete și sarcinile stabilite:

Guvernului: de a întreprinde măsurile necesare pentru instituirea/desemnarea autorității competente, reglementarea modului de organizare și funcționare a acesteia și dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege, de a prezenta propuneri Parlamentului privind aducerea actelor normative în concordanță cu prezenta lege și de aduce în concordanță actele proprii;

Autorității competente: de a identifica furnizorii de servicii, îi va notifica în modul stabilit și îi va include în Lista furnizorilor de servicii, întocmită în condițiile legii și de a aproba actele normative necesare punerii în aplicare a legii;

Autorităților și instituțiilor publice să acorde suportul necesar autorității competente în procesul de identificare a furnizorilor de servicii.

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

În contextul obiectivelor urmărite, mai ales de transpunere în cadrul legislativ național a Directivei NIS2, inclusiv a necesității instituirii sau desemnării unei autorități competente la nivel național și a unei echipe de răspuns la incidentele de securitate cibernetică la nivel național o opțiune alternativă opțiunii de reglementare se prezintă ca fiind inutilă. Or, pentru a acoperi domeniul de aplicare al NIS2 chiar și în măsură limitată presupune instituirea unor norme legale primare care ar reglementa obligațiunile entităților din sectorul privat în contextul gestionării riscurilor și incidentelor cibernetice, precum și a crizelor în domeniul securității cibernetice

Este necesar de evidențiat faptul că intervenție la nivel legislativ: o lege cadru sau modificări la legislația actuală sunt modalități ale uneia și aceleiași opțiuni.

4. Analiza impacturilor opţiunilor

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

Lipsa unei intervenții prompte și bine structurate din partea statului ar putea fi tradusă în următoarele efecte sau consecințe nefavorabile:

- Lipsa unui cadrului legislativ menit să reglementeze exact și transparent securitatea cibernetică la nivel național în continuare va crea temei de perturbare și afectare directă și indirectă a societății;
- Lipsa cadrului de cooperare la nivel național și de participare la nivel internațional în domeniul asigurării securității cibernetice va limita atât instituțiile statului, cât și furnizorii de servicii de a face față provocărilor prin prevenirea incidentelor și minimizare a riscurilor în baza experienței altor state;
- Lipsa autorității competente la nivel național și a entității de drept public și privat care deține competențe și responsabilități privind securitatea cibernetică, lipsa punctului unic de contact la nivel național și echipei naționale de intervenție în caz de incidente de securitate cibernetică va limita statul și entitățile în mecanisme transparente și eficiente de asigurare a securității cibernetice;
- Lipsa informației privind stabilirea exacte a entităților (publice și private) care sunt esențiale și importante în contextul unei eventuale perturbări a serviciului furnizat, care ar putea avea un impact asupra siguranței publice, a securității publice sau a sănătății publice sau ar putea genera riscuri sistemice, în special pentru sectoarele în care o astfel de perturbare ar putea avea un impact transfrontalier în continuare va duce la limitarea statului în exercitarea atribuțiilor în asigurarea securității cibernetice, iar a entităților în suport din partea statului;
- Lipsa unor cerințe de securitate pentru entitățile esențiale și importante, stabilite la nivel național va duce la diferențe esențiale între entități și drept rezultat la incapacitatea unei colaborări eficiente a acestora în prevenirea incidentelor de securitate cibernetică;
- Lipsa obligațiilor de gestionare și de raportare a riscurilor privind securitatea cibernetică pentru entitățile esențiale și importante, stabilite la nivel național, va duce potențiale perturbări a serviciilor esențiale și importante;
- Consecințe negative asupra rezilienței cibernetice a entităților survenite din cauza lipsei regimul de supraveghere în domeniul securității cibernetice;
- Resursele financiare și umane pe care entitățile (publice și private) le alocă pentru asigurarea securității cibernetice și nivelul de maturitate în abordarea riscurilor de securitate cibernetică variază foarte mult. Acest lucru agravează și mai mult diferențele dintre entități în ceea ce privește reziliența cibernetică;
- Entitățile (publice și private) nu dispun de mecanisme reglementate de schimb sistematic de informații. Acest lucru are consecințe negative, în special asupra eficacității măsurilor de securitate cibernetică și asupra nivelului de cunoaștere comună a situației la nivelul național;
- Diminuarea transferului de know-how în țară, fapt care ar contribui nemijlocit la stagnarea evoluției sectorului de securitate cibernetică;
- Aspecte de ordin social precum: gradul redus al ocupării forței de muncă, migrarea profesioniștilor în căutarea oportunităților de angajare mai avantajoase peste hotare, reconversia profesională;
- Majorarea costurilor Guvernului în atingerea obiectivelor propuse în documentele de planificare strategică.

b[1]) Pentru opțiunea recomandată, 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	

Beneficii

Impact asupra securității și protecției rețelelor și sistemelor informatice. În cadrul acestei opțiuni, protecția consumatorilor, a sectorului public și a celui privat împotriva incidentelor, amenințărilor și riscurilor de securitate cibernetică ar fi îmbunătățită considerabil. Obligațiile impuse furnizorilor de servicii ar asigura că toate entitățile sunt dotate corespunzător, atât din perspectiva capacităților tehnice și organizaționale, cât și în ceea ce privește pregătirea. Un set minim comun de cerințe ar contribui la crearea unui climat de încredere reciprocă, care este o condiție prealabilă pentru orice cooperare eficientă, în mod special între sectorul public și cel privat. Funcționarea

continuă și stabilă și fiabilă a serviciilor esențiale și importante este esențială pentru economia digitală și pentru întreaga societate.

O cooperare sigură și eficientă la nivel național ar permite o prevenire și o reacție coerentă și coordonată la incidentele, riscurile și amenințările semnificative la adresa rețelelor și sistemelor informatice utilizate în procesul prestării serviciilor. Introducerea unor cerințe de gestionare a riscurilor de securitate cibernetică pentru persoanele juridice de drept public și cele de drept privat ar crea un stimulent puternic pentru gestionarea și dimensionarea eficientă a riscurilor de securitate. Obligația de a raporta de către aceștia a incidentelor cibernetice cu impact semnificativ ar spori capacitatea de reacție la incidente și ar promova transparența.

Disponibilitatea datelor și informațiilor-cheie privind securitatea rețelelor și sistemele informatice ar permite, de asemenea, autorităților publice responsabile să efectueze analize specifice și să întocmească statistici și, prin urmare, să utilizeze informații fiabile privind securitatea rețelelor și sistemelor informatice pentru a stabili cele mai adecvate priorități în acest domeniu. Opțiunea de reglementare, prin creșterea nivelului de securitate, ar permite țării noastre să-și crească credibilitatea în ce privește nivelul de protecție și securitate a rețelelor și sistemelor sale informatice și să beneficieze în consecință de informații pertinente de la partenerii săi internaționali.

Impactul economic. Ca urmare a creșterii nivelului de securitate, problemele de securitate ar fi mai rapid remediate și impactul lor ar fi diminuat. De asemenea, pierderile financiare asociate ar fi reduse. Aceste beneficii ar fi resimțite în mod egal în toate sectiarele relevante ale economiei naționale, deoarece vor fi unificate procedurile pentru toate entitățile care vor intra în domeniul de aplicare al legii, permițând astfel crearea unor condiții de concurență echitabile și sprijinind dezvoltarea economică. Acest lucru ar spori încrederea întreprinderilor și a consumatorilor în lumea digitală și în internet și ar crea astfel noi oportunități pentru întreprinderi și pentru economia digitală. Utilizatorii se vor simți mai în siguranță online, ceea ce va spori încrederea acestora în internet, în beneficiul economiei naționale. În special, promovarea unei abordări de gestionare a riscurilor și a unei culturi a securității ar fi benefică pentru atât pentru sectorul privat cât și pentru cel public. Efectuarea evaluării riscurilor de securitate cibernetică le-ar permite și le-ar stimula să aloce eficient resursele pentru a gestiona aceste riscuri și, prin urmare, ar crește valoarea organizației pentru public.

De asemenea, întrucât întreprinderilor din același sector li s-ar cere să pună în aplicare măsuri de securitate similare, întreprinderile ar vor concura pe picior de egalitate. Organizațiile ar fi mai bine echipate pentru a face față incidentelor și atacurilor, ceea ce ar avea ca rezultat o mai mare disponibilitate, fiabilitate și calitate a serviciilor lor. Acest lucru ar crește nivelul de încredere și de satisfacție al celor care utilizează aceste servicii, ar crește profiturile și ar favoriza dezvoltarea economică. Promovarea unei culturi îmbunătățite a gestionării riscurilor ar stimula, de asemenea, cererea de produse și soluții TIC sigure. Acest lucru ar crea noi oportunități și ar valorifica investițiile în cercetare prin îmbunătățirea perspectivelor de exploatare comercială a acestora.

Impactul social. Un nivel mai ridicat de securitate ar îmbunătăți încrederea on-line a cetățenilor, care ar putea profita pe deplin de avantajele lumii digitale, în mod special în ce privește serviciile digitale guvernamentale. Aceste servicii esențiale ar deveni mai atractive datorită fiabilității și disponibilității ridicate. Acest lucru le poate conferi cetățenilor din regiunile rurale sau îndepărtate cu acces limitat la serviciile offline o mai mare încredere. În cele din urmă, este foarte probabil ca această opțiune să stimuleze crearea unui corp de profesioniști în domeniul asigurării securității rețelelor și sistemelor informatice și, implicit al ocupării forței de muncă a personalului din acest domeniu, inclusiv datorită cerințelor de a efectua evaluări ale riscurilor de securitate cibernetică și de a adopta măsuri de securitate adecvate.

Impact asupra competitivității. În general, este de așteptat ca o disponibilitate, o fiabilitate și o calitate sporită a serviciilor oferite în sectoarele critice care se bazează în mare măsură pe rețele și sisteme informatice va fi în beneficiul competitivității economiei naționale în ansamblu. De exemplu, disponibilitatea platforme sigure pentru comerțul electronic și alte servicii bazate pe web ar putea aduce importante beneficii economice și ar permite unei game largi de întreprinderi să aducă noi produse și servicii pe piață.

În cele din urmă, se așteaptă un impact pozitiv și pentru furnizorii de produse și servicii de securitate din domeniul tehnologiei informației și comunicațiilor . În primul rând, se așteaptă o creștere a cererii. În plus, dezvoltarea de măsuri de securitate specifice pentru sectoarele din domeniul de aplicare, combinată cu o abordare uniformă la nivelul național, va permite dezvoltarea de produse inovatoare și realizarea de economii de scară.

Estimarea costurilor.

Implementarea acestei inițiative va implica pe de o parte costuri:

1. pentru bugetul de stat, determinate de necesitatea instituirii/desemnării autorității competente și creării unui CSIRT național sau atribuirii competenței unui astfel de CSIRT către CERT-GOV,
2. pentru furnizorii de servicii din sectorul privat privind necesitatea conformării cerințelor noi stabilite de noul cadru legal în domeniul securității cibernetice.

1. În ce privește costurile privind autoritatea competentă și CSIRT național modelul de cost estimat pentru înființarea acestora este în mare măsură determinat de obiectivele stabilite pentru această organizație, de poziția sa juridică și de grupul de interese.

Cu toate acestea, se poate argumenta că anumite resurse critice pot fi identificate în continuare pentru a asigura alinierea la cerințele care decurg din legislația UE (Directiva NIS2). Finanțarea Autorității competente și a CSIRT ar trebui să acopere investițiile inițiale pentru a pune în funcțiune echipa (CAPEX), precum și costurile operaționale recurente (OPEX) pentru personal, instalații și licențe de software, precum și costurile necesare pentru furnizarea și întreținerea serviciilor.

a) Astfel **realizarea funcției de CSIRT național, inclusiv gestionarea incidentelor: prevenție detecție și răspuns** (cerințele de conformare stabilite de art. 11 alin. (1) din Directiva NIS2) implică anumite elemente critice ale misiunii ce urmează a fi realizată, precum:

Expertiză și resurse suficiente echipa ar trebui să includă experți în securitatea rețelelor, analiza jurnalizării, criminalistică informatică și reverse engineering, precum și în arhitectură de securitate și securitate avansată a informațiilor. De asemenea, este important ca echipa să dispună de resurse proprii de dezvoltare, deoarece natura specifică a activității CSIRT înseamnă că toate instrumentele necesare nu pot fi externalizate, ci unele dintre ele trebuie dezvoltate chiar de către echipă. Succesul în răspunsul la incidente la nivel național necesită, de asemenea, cunoașterea funcționării statului și a serviciilor critice, a gestionării riscurilor și a crizelor și a continuității activității. De asemenea, trebuie asigurate hardware și software necesare, comunicații, o locație securizată și alte lucruri necesare pentru această activitate.

Informații privind amenințările. Culegerea și analiza continuă a informațiilor privind incidentele de securitate, atât la nivel național, cât și internațional, fac posibilă identificarea rapidă a amenințărilor și rezolvarea mai eficientă a incidentelor. Conceptul de incident trebuie definit cu precizie, împreună cu procesul de raportare și analiză a incidentelor. Pe lângă colectarea de informații din surse publice (OSINT), raportarea la nivel național și schimbul de informații, schimbul internațional de informații cu organizații surori din alte țări este foarte de dorit.

Astfel finanțarea minimă a acestor elemente critice este compusă din componentele:

Personal - Un CERT cu servicii complete, care funcționează numai în timpul orelor de birou și care își menține propriile sisteme, necesită un minim de 6-8 angajați cu normă întreagă (FTE), iar pentru o operațiune 7x24 (3 schimburi pe zi), minim 12 FTE. Personalul trebuie să se califice pentru a avea o expertiză tehnică solidă și competențele-cheie ale angajaților CERT/CSIRT (de exemplu, așa cum sunt descrise în orientările ENISA[32]) Este important să se asigure formarea constantă și contemporană a întregului personal. Formarea externă de înaltă calitate pentru personalul CSIRT este, de exemplu, organizată de TRANSITS , CERT/CC , SANS Institute , și FIRST. Resursele financiare minime ar trebui să fie cuprinse între 3 000 și 5 000 EUR pe expert pentru a acoperi costurile de formare anuale. **Acestea ar constitui un minim de 18 000 EUR și un maxim de 60 000 EUR pe an.**

[32] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

În ce privește salarizarea personalului o estimarea inițială a costurilor de salarizare a personalului CCA depinde în mod direct de statutul juridic al acestui personal. Statutul juridic al personalului este determinat de forma juridică de organizare în care va funcționa autoritate competentă, precum și de locul pe care îl va ocup în structura actuală a administrației publice guvernamentale:

a) instituție publică (prevăzută la articolul 32 din Legea nr. 98/20141 privind administrația publică centrală de specialitate) sau

b) autoritate administrativă centrală sau autoritate administrativă, subordonată unui minister (articolele 14 și 17 din aceeași lege).

În cazul în care noua entitate va fi organizată **sub forma juridică a unei instituții publice**, ceea ce ar fi justificat din perspectiva unei salarizări mai corespunzătoare profilului, dar ar contraveni Legii nr. 98/2014 privind administrația publică centrală de specialitate din punctul de vedere al convergenței prerogativelor exercitate cu forma de organizare juridică, la salarizarea personalului acesteia se vor aplica prevederile Hotărârii Guvernului nr. 743/20022 privind salarizarea angajaților din unitățile cu autonomie financiară. În acest caz, salariile angajaților vor varia în funcție de funcția deținută, pe baza salariului minim de 3.500 lei, stabilit prin Hotărârea Guvernului nr. 670/2022 privind stabilirea cuantumului salariului minim pe țară, după cum urmează:

Poziția	**Nivelul de salarizare /lei**	
	min	**max**
Director	Directorul urmează să primească un salariu egal cu trei salarii medii lunare pe autoritate pentru perioada de la începutul anului până la sfârșitul lunii de gestiune și este stabilit în contractul de gestiune încheiat cu directorul instituției publice.	
Director adjunct	35.700	47.600
Șef de subdiviziune	11.900	35.700
Specialist	11.900	26.775

În cazul în care noua entitate va fi organizată sub forma juridică a unei autorități administrative centrale sau a unei autorități administrative, subordonată unui minister, atunci prevederile Legii nr. 270/2018 privind sistemul unitar de salarizare în sectorul bugetar vor fi aplicabile salariilor personalului acesteia. Tabelul de mai jos cuprinde informații privind salariile de bază aproximative ale angajaților noii entități, fără a lua în considerare variabile precum: sporul lunar pentru gradul profesional; sporul lunar pentru un titlu științific și/sau științific/didactic; sporul lunar pentru un titlu onorific; sporul de performanță; alte sporuri speciale:

poziția	**Nivelul de salarizare /lei**	
	Min.	**Max.**
Director General /Director al autorității administrative centrale (demnitate publică)	16.850	19.100
Director General adjunct/ Deputy Director adjunct al autorității administrative centrale (funcționar public)	15.500	17.550
Director al autorității administrative subordonate ministerului (funcționar public)	18.550	21000
Director adjunct al autorității administrative subordonate ministerului (funcționar public)	15500	19.350
	9.700	15000

Șef de subdiviziune (funcționar public)		
Poziții de execuție (funcționar public)	5700	9700

Sediu

Există, de asemenea, cerințe speciale de securitate pentru sediile CERT/CSIRT, de exemplu:

- încăperi securizate pentru amplasarea oricăror servere și depozite de date ale CSIRT;
- încăperi securizate și izolate fonic pentru discuțiile privind activitățile și investigațiile CSIRT;
- seif pentru depozitarea datelor și notelor neelectronice;
- Un distrugător și o instalație pentru distrugerea completă a suporturilor (de exemplu, EMP) care nu mai sunt necesare.
- Separarea fizică a personalului CSIRT de alte părți ale organizației, inclusiv controlul accesului.

Volumul investițiilor rămâne un subiect care urmează a fi clarificat având în vedere caracteristicile speciale ale locației unui CSIRT național..

Echipamente IT pentru utilizarea CSIRT/CERT. Lista propusă în continuare este una neexhaustivă:

- mecanisme de comunicare securizate, cum ar fi telefoane, faxuri și e-mailuri securizate;
- sisteme hard, inclusiv computerele de lucru (de exemplu, versiunea întărită Microsoft Enterprise).
- Rețea proprie, separată de rețeaua celorlalte subdiviziuni sau personal care nu e implicat nemijlocit în activitățile CSIRT;
- Facilitate de reinstalare rapidă a sistemelor care au fost în afara zonei securizate sau care au fost utilizate pentru analiza malware;
- Instrumente și infrastructură specifice CSIRT, cum ar fi sistemul de gestionare a cazurilor (sistem de ticketing etc.), baza de date de contacte a membrilor echipei, a mandanților și a altor POC etc.
- Configurarea și întreținerea instrumentelor de securitate
- Dezvoltarea de instrumente de securitate
- Instrumente de detectare a intruziunilor, instrumente de monitorizare a rețelei
- instrumente de interogare a domeniilor și a adreselor IP
- instrumente de evaluare a vulnerabilității
- Instrumente de expertiză criminalistică
- Instrumente de analiză a programelor malware
- Honeypots, etc.

Costurile mai specifice depind de dimensiunea reală a echipei și de funcțiile acesteia. **Costul inițial estimat este de aproximativ 500 000 EUR.**

b) Funcții realizate în contextul cadrului de gestionare a crizelor și f**uncțiile de organizare a coordonării naționale a CIIP, identificarea serviciilor esențiale/critice și a furnizorilor de servicii, stabilirea și menținerea listei entităților esențiale/critice**

Personalul și competențele necesare sunt dictate de necesitate de

- expertiză juridică pentru care e recomandabil să se dispună de cel puțin 3 experți juridici cu normă întreagă care pot participa la elaborarea de regulamente și legislație.
- Expertiză în domeniul protecția infrastructurii informaționale critice, al gestionării riscurilor și al gestionării crizelor – pentru care sunt necesari cel puțin 6 persoane angajate cu normă întreagă care să stabilească și să mențină o cooperare solidă cu părțile interesate, atât în sectorul public, cât și în cel privat.

De asemenea va fi necesară formare și participare la exerciții internaționale. Este important faptul că toți experții au nevoie de formare periodică pentru a-și menține cunoștințele relevante și a-și dezvolta competențele. Se recomandă cu insistență organizarea sau participarea la cel puțin 1 curs de formare la nivel internațional anual. În cadrul cooperării internaționale, ar trebui să se ia în considerare costurile de deplasare a 2-4 experți care permit participarea la un exercițiu anual (cel puțin). De exemplu, participarea la exerciții cu focuri reale organizate de CCDCOE al NATO (exercițiul tehnic Locked Shields) și/sau la exerciții de gestionare a crizelor orgnaizate sub auspiciile ENISA.

În context este necesar de evidențiat că Directiva NISD2 pune accentul pe identificarea entităților critice/esențiale care intră în domeniul de aplicare al acesteia și creează o listă de operatori (entități) care furnizează servicii esențiale (vitale) în statul în cauză. Lista ar trebui să conțină toate serviciile furnizate pe teritoriul unui anumit stat și ar trebui să fie completată prin includerea de noi servicii. Lista de servicii stabilită de fiecare stat membru ar servi ca o contribuție suplimentară la evaluarea practicii de reglementare a fiecărui stat membru în vederea asigurării nivelului general de coerență a procesului de identificare între statele membre.

c) Schimbul de informații

Cooperarea cu comunitatea națională de IT, infrastructura critică și serviciile esențiale.

Este important să înțelegem că funcționarea serviciilor IT de care are nevoie societatea depinde în mare măsură de companiile din sectorul privat. În mod obișnuit, profesioniștii din domeniul IT își dezvoltă propriile comunități spontane sau organizate, de la alianțe profesionale la forumuri online. Este important ca un CSIRT să colaboreze cu aceste comunități și să fie vizibil pentru acestea. Aceasta oferă acces rapid la informațiile necesare privind schimbările de securitate, accelerează schimbul de informații și chiar subliniază disponibilitatea unor expertize sau resurse IT specifice care pot fi utilizate pentru a răspunde la incidente în caz de urgență. Instrumente specifice de schimb de informații sunt necesare pentru a permite notificarea incidentelor și schimbul de informații sensibile (de exemplu, poșta electronică securizată și platformele desemnate pentru schimbul de informații privind amenințările cibernetice).

Comunicare și vizibilitate

Informarea publicului, precum și a instituțiilor partenere cu privire la amenințările la adresa securității trebuie să fie o activitate regulată și trebuie să existe un proces clar în acest sens. Deși campaniile de informare și comunicarea cu mass-media pot fi realizate și prin intermediul partenerilor, este recomandabil să existe o funcție corespunzătoare în cadrul CSIRT-ului însuși. Un CSIRT ar trebui, de asemenea, să fie vizibil în social media și să interacționeze cât mai mult posibil cu grupul său de interes.

Formatele pentru schimbul de informații pot consta în:

1) Platforme tehnice pentru schimbul de date privind vulnerabilitatea tehnică și amenințările (de exemplu, MISP).

2) formate și evenimente formale și non-formale de creare de rețele pentru părțile interesate.

Pentru realizarea acestor funții vor fi necesare pentru **relațiile publice- cel puțin 2 persoane** cu normă întreagă care ar trebui să se ocupe de relațiile publice și cu mass-media ale Autorității competente, precum și cel puțin **5 analiști** cu normă întreagă care pot analiza datele privind incidentele și amenințările și pot furniza rapoarte publice și clasificate privind peisajul amenințărilor, analize ale incidentelor etc.

d) Funcția de supraveghere și audit

Autoritatea competentă trebuie să instituie o funcție solidă de supraveghere și audit care să supravegheze și să testeze punerea în aplicare a reglementărilor naționale în materie de securitate cibernetică. Se recomandă, de asemenea, ca autoritatea respectivă să aibă propria echipă independentă de testare a securității (echipa RED). Pentru aceasta autoritatea trebuie să includă în statul său de personal experți în supraveghere - numărul acestora depinde de numărul de subiecți supravegheate. Prin urmare, determinarea resurselor umane necesare necesită o înțelegere a numărului de entități esențiale/importante care intră în domeniul de aplicare a noii legi. De asemenea autoritate va avea nevoie de experți în testare (RED Team)- 3-4 experți tehnici de înaltă calificare cu normă întreagă și cu capacitate de testare a penetrării, etc.

În concluzie pentru realizarea funcțiilor enunțate mai sus autoritatea competentă, în cazul în care va include în competența sa și realizarea funcției de CSIRT național va avea necesarul de **minim 25 de angajați**, fără a include aici conducătorii, personalul de suport (în cazul creării unei entități noi) și personalul dedicat realizării funcției de supraveghere (după cum s-a menționat mai sus numărul acestuia este direct dependent de numărul furnizorilor de servicii). Având în vedere prevederile cadrului normativ național în domeniul salarizării**,** și presupunând că personalul respectiv este divizat în patru subdiviziuni (numărul funcțiile fundamentale ce urmează a fi realizate de autoritatea competentă) **remunerarea anuală a muncii acestui personal ar constitui:**

- în cazul instituției publice: **între 3,6 mil. lei și 8,5 mil lei anual;**
- în cazul unei autorități administrative centrale sau autorități administrative în subordinea unui minister**: între 1,9 mil lei și 3,2 mil. lei anual.**

La aceste cheltuieli de personal urmează a fi adăugate cheltuieli investiționale unice inițiale de circa 10 mil. lei în echipamentul și instrumentariul tehnic al CSIRT.

De asemenea, o estimare a costurilor ce țin de asigurarea cu sediu ce corespunde cerințelor Directivei NIS2 urmează a fi efectuat atunci când Guvernul, în temeiul prevederilor legale propuse în proiect va exercita dreptul său discreționar de a decide înființarea unei noi entități sau atribuirea competențelor unei autorități existente.

În analiza de impact 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*****.”.**

În același context, Agenția Europeană pentru Securitate Cibernetică a publicat un ghid[33] privind modul de creare și asigurare a funcționalității unui CSIRT care oferă informații și privind costurile estimative la nivelul țărilor membre, necesare pentru instituirea unui CSIRT național.

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

Nu este cazul.

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

Există riscul implementării lente a prevederilor legii din motivul domeniului nou de reglementare, drept urmare, unele problemele existente riscând să-și păstreze actualitatea pentru o anumită perioadă de timp.

Un alt risc este insuficiența resurselor umane calificate în corespundere cu nivelul de salarizare existent la moment. Respectiv, sunt necesare acțiuni de asigurare a unei remunerări adecvate.

Alt risc este pericolul dotării insuficiente a Autorității competente pentru exercitarea atribuțiilor ce-i revin. În vederea minimizării riscului respectiv, se consideră oportună abordarea organismelor specializate UE și programelor europene și regionale care pot asigura un suport în crearea, dotarea și instruirea Autorității competente naționale.

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 sînt propuse măsuri de diminuare a acestor impacturi

Estimarea costurilor de implementare a legii pentru întreprinderile care vor cădea sub incidența obligațiilor stabilite de lege actualmente este o provocare în condițiile unei lipse acute a datelor statistice primare în domeniu securității cibernetice, precum și lipsei unor evaluări și analize

[33] https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

financiare bazate pe astfel de date la nivel național. Totuși anumite orientări pe această dimensiune sunt acordate de Comisia Europeană în procesul de evaluare a costurilor de conformare pentru mediul privat în procesul de pregătire a propunerii de Directivă NIS1: *„Pornind de la costurile totale de conformare pentru sectorul privat, care variază între 360 și 720 de milioane de euro, costul de conformare pentru fiecare întreprindere mică și mijlocie s-ar situa între 2 500 și 5 000 de euro. La efectuarea calculului, s-a presupus că întreprinderile mici și mijlocii reprezintă 20% din cifra de afaceri a întreprinderilor private vizate de regulament și reprezintă 68% din toate întreprinderile afectate, adică puțin peste 28 000 de întreprinderi. Acesta este costul mediu estimat pentru fiecare IMM pentru atingerea nivelului actual de "cel mai bun din clasă" în ceea ce privește protecția NIS. Pe măsură ce tehnologiile evoluează, riscurile, pe de o parte, și măsurile de protecție, pe de altă parte, vor continua să evolueze și ele. Astfel, vor fi necesare investiții continue pentru a ține pasul cu stadiul actual al tehnologiei, dar este foarte dificil, în acest stadiu, să se prevadă care vor fi costurile pe care le implică menținerea pasului cu evoluțiile tehnologice. Cu toate acestea, aceste investiții vor garanta că atât întreprinderile mari și mici, cât și economia europeană vor fi bine poziționate pentru a profita de avantajele pieței globale a securității cibernetice, care, potrivit estimărilor, se va număra printre segmentele cu cea mai rapidă creștere din sectorul tehnologiei informației (IT) în următorii 3-5 ani; în 2011, piața securității cibernetice valora 63,7 miliarde de dolari și se preconizează că va crește între 80 și 120,1 miliarde de dolari până în 2017.”*

În ce privește costurile pentru entitățile administrației publice și furnizorii de servicii esențiali asociați cu raportarea obligatorie a unui incident semnificativ, Comisia Europeană a estimat în aceeași analiză de impact următoarele:

„Pentru a evalua costurile de raportare a incidentelor grave din NIS, a fost extrapolată o estimare a notificărilor care ar trebui efectuate pe parcursul unui an, pe baza datelor existente privind punerea în aplicare a articolului 13a din directiva-cadru privind comunicațiile electronice. Pe această bază, numărul de notificări de incidente NIS preconizate s-ar ridica la aproximativ 1 700 pe an. Presupunând că un angajat ar trebui să aloce 0,5 zile lucrătoare pentru notificare și că notificarea ca atare ar avea costuri neglijabile (de exemplu, ar fi efectuată prin intermediul unui e-mail), costul preconizat pentru fiecare notificare de încălcare ar fi de 125 EUR, ceea ce ar duce la un cost total pentru notificarea încălcărilor pe bază anuală de 212 500 EUR la nivelul UE. În ceea ce privește posibilele investigații care pot fi inițiate de către autoritățile competente din NIS cu privire la respectarea obligațiilor de gestionare a riscurilor și de notificare a incidentelor NIS, nu este posibil în acest stadiu să se estimeze dacă și câte investigații ar putea fi inițiate. Cu toate acestea, se poate presupune în mod rezonabil că între 10 și 20% din notificările de incidente NIS ar putea fi urmate de o investigație, ceea ce corespunde unei valori absolute de 170-340 de investigații preconizate pe an. Ținând cont de costul salarial standard, costul maxim pentru entitatea afectată ar fi de maximum 25 000 EUR pe investigație…”

În plus, Agenția Europeană pentru Securitate Cibernetică a publicat Raportul privind investițiile NIS 2021[34], care acoperă toate cele 27 de state membre ale UE și oferă informații suplimentare cu privire la alocarea bugetelor NIS ale OES/DSP, impactul economic al incidentelor de securitate cibernetică și organizarea securității cibernetice în cadrul acestor operatori

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

Analiza beneficiilor și costurilor opțiunilor, în mod special al celei recomandate, în contextul bunelor practici reflectate în studiile și rapoartele de evaluare ale situației în materie de securitate cibernetică în Republica Moldova putem concluziona că opțiunea recomandată în prezenta analiză de elaborare și adoptare a unei legi cadru privind securitate cibernetică este opțiunea preferabilă, recomandabilă și cea mai plauzibilă în contextul actual național și internațional al Republicii Moldova.

În același context relevăm stringența soluționării problematicii instituționale și organizaționale prin instituirea/ desemnarea unei autorități competente și a unui CSIRT național cu

[34] https://www.enisa.europa.eu/publications/nis-investments-2021

capacități suficiente și necesare pentru a preveni, detecta și răspunde adecvat amenințărilor și incidentelor de securitate cibernetică.

Opțiunea recomandată, prin determinarea clară a domeniului de aplicare al legii, va asigura transparența în aplicarea cerințelor de către furnizorii de servicii, la care se adaugă un cadru transparent de supraveghere și de asigurare a respectării legii.

De asemenea prin intervenția propusă vor fi stabilite precondițiile necesare pentru stabilirea clară a responsabilităților și a răspunderii, precum și a mecanismelor orientate spre o promovare a unei mai mari încrederi atât la nivel de autorități, cât și la nivel de întreprinderi, stimulând schimbul de informații și asigurând o asistența reciprocă bazată pe încredere și diligență.

Este cert că opțiunea recomandată presupune costuri de implementare atât pentru sectorul public cât și pentru cel privat, dar în rezultatul implementării măsurilor și cerințelor propuse în proiectul de lege se va asigura o creștere consecventă a nivelului de reziliență cibernetică a entităților-cheie din Republica Moldova, vor fi generate, bineînțeles pe termen mediu și lung economii de costuri atât pentru sectorul privat, cât și pentru societate.

Opțiunea va genera anumite sarcini administrative suplimentare și costuri de asigurare a conformității pentru autoritățile publice, dar în contextul atingerii unui nivel sporit de securitate cibernetică, ar duce, în cele din urmă, la economii de costuri prin prisma minimizării pierderilor economiei naționale din cauza amenințărilor la adresa securității cibernetice.

Pe termen mediu și lung, atingerea unei creșteri a capacităților în materie de securitate cibernetică la nivel național ar aduce beneficii substanțiale printr-o cooperare la nivel operațional, stimulare și asistență reciprocă și o mai bună interacțiune cu mediul privat.

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 sînt necesare

1. Cadrul juridic ce necesită a fi modificat și/sau elaborat și aprobat

În conformitate cu prevederile art. 20 alin (2) din proiectul actului normativ, Guvernul urmează, în termen de cel mult 6 luni din data publicării Legii privind securitatea cibernetică să asigure elaborarea și să prezinte Parlamentului propuneri de modificare a legilor în vigoare care sunt conexe domeniului reglementat de actul normativ în speță. Astfel, deși la momentul actual este destul de ambițios de a identifica prevederile specifice ale unor legi-cadru ce reglementează alte domenii și care cu certitudine necesită a fi modificate în contextul aducerii în concordanță cu prevederile legii în speță, totuși ar putea fi anticipată necesitatea, cel puțin a examinării, în contextul realizării acestui obiectiv, a următoarelor legi care cuprind reglementări privind securitatea și protecția :

- Legea nr. 1069/2000 cu privire la informatică;
- Legea nr.467/2003 cu privire la informatizare și la resursele informaționale de stat;
- Legea nr.71/2007 cu privire la registre;
- Legea nr. 241/2007 comunicațiilor electronice;
- Legea nr.133/2011 privind protecția datelor cu caracter personal;
- Legea nr. 124/2022 privind identificarea electronica și serviciile de încredere;

În același context, unei examinări aprofundate urmează a fi supuse legile cadru care reglementează sectoarelor, subsectoarele și tipurile de entități ce prestează servicii în acestea, enumerate în anexele 1 și 2 la Directiva NIS2, în contextul în care Guvernul urmează să aprobe lista acestor sectoare și subsectoare de rând cu tipurile persoanelor juridice. Examinarea acestei categorii de acte normative naționale urmează a fi efectuată în primul rând din perspectiva armonizării acestora cu actele sectoriale relevante ale Uniunii Europene, menționate de altfel în anexele respective ale Directivei NIS2.

În continuare pentru a asigura implementarea prevederilor legale noi, urmează a fi supuse dacă nu unei revizuiri, cel puțin unei examinări aprofundate în scopul confirmării conformității cu prevederile noii legi a următoarelor acte normative Guvernamentale:

- Hotărârea Guvernului nr. 201/2017[35] privind aprobarea cerințelor minime obligatorii de securitate cibernetică;

[35] https://www.legis.md/cautare/getResults?doc_id=98644&lang=ro

- Hotărârea Guvernului nr. 482/2020[36] privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental;
- Hotărârea Guvernului nr. 388/2022[37] cu privire la aprobarea Concepției Sistemului informațional „Registrul de stat al incidentelor de securitate cibernetică".

În același context, Guvernul urmează să aprobe un set de acte normative de unere în aplicare a noului cadru normativ în domeniul securității cibernetice, prevăzute de proiectul de act normativ:

lista sectoarelor, subsectoarelor și, respectiv, a tipurilor și categoriilor de persoane juridice care prestează servicii în aceste sectoare și/sau subsectoare (art. 2 alin. (5);

cadrul metodologic privind identificarea persoanelor juridice de drept publice sau privat ca fiind furnizori de servicii (art. 2 alin. (5);

Strategia națională de securitate cibernetică (art.6 alin. (3), având la bază pe de o parte rezultatele și concluziile procesului de analiză a modului de implementare a Strategiei naționale de securitate informațională, aprobată prin Hotărârea Parlamentului nr. 257/2018, și pe de altă parte prevederile articolului 7 al Directivei (UE) 2022/... a Parlamentului European și a Consiliului privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (*Directiva NIS 2*):

- stabilirea sau modificarea modului de organizare și funcționare a entității care va exercita funcțiile autorității competente (art. 7 alin. (1)
- modul de coordonare de către autoritatea competentă a procesului de divulgare a vulnerabilităților (art. 7 alin. (4) lit. i));
- aprobă cadrul metodologic privind elaborarea, actualizarea și implementarea prevederilor planului național de răspuns la incidente cibernetice și crize de securitate cibernetică, interacțiunea dintre autoritățile și instituțiile publice cu atribuții în procesul de elaborare și actualizare, precum și interacțiunea acestora cu sectorul privat (art. 8 alin. (4).
- modul de organizare și funcționare a Registrului de stat al incidentelor cibernetice și a sistemului informațional corespunzător art. 9 alin. (1);
- asigurarea, prin intermediul organismului național de standardizare și în cooperare cu autoritatea competentă, aprobarea Standardului Moldovenesc în domeniul securității informațiilor, securității cibernetice și protecția confidențialității în baza standardelor și a specificațiilor tehnice europene și internaționale relevante pentru securitatea rețelelor și a sistemelor informatice art. 10 alin. (4);
- cerințele specifice privind măsurile de securitate a rețelelor și sistemelor informatice, în funcție de sectorul, subsectorul, categoria și/sau tipul furnizorului de servicii (art. 10 alin. (4);
- procedura de notificare a incidentelor cibernetice, inclusiv interacțiunea dintre furnizorul de servicii și autoritatea competentă, modul de stabilire a impactului unui incident cibernetic și formatul informațiilor evaluărilor și rapoartelor prezentate în procesul de gestionare a unui incident cibernetic (art. 11 alin. (8).
- regulamentul privind condițiile și cerințele în care sunt semnate de către autoritățile și instituțiile publice acordurile de schimb de informații în materie de securitate cibernetică (art. 15 alin. (3);
- modul de aplicare a măsurilor de supraveghere de către autoritatea competentă (art. 16 alin. (5);
- modul de realizare a controlului de către autoritatea competentă asupra respectării de către furnizorii de servicii a obligațiilor ce le revin conform Legii privind securitatea cibernetică (art. 17 alin. (5).

2. Schimbările instituționale preconizate prin aprobarea proiectului de act normativ

În temeiul art. 7 alin. (1) din proiectul de act normativ Guvernul urmează să desemneze autoritatea competentă la nivel național în domeniul securității cibernetice. De asemenea, potrivit

[36] https://www.legis.md/cautare/getResults?doc_id=122272&lang=ro
[37] https://www.legis.md/cautare/getResults?doc_id=132011&lang=ro

prevederilor art. 20 alin. (2) Guvernul urmează să asigure dotarea ei cu resurse umane, financiare și tehnice necesare pentru îndeplinirea atribuțiilor stabilite de lege.

Potrivit proiectului de act normativ Guvernului i se conferă o marjă discreționară în procesul de desemnare a acestei autorități competente fie prin instituirea unei autorități/instituții publice noi fie prin identificarea și atribuirea competenței prevăzute de proiectul de act normativ unei entități publice existente.

În oricare dintre cazurile menționate Guvernul urmează, după aprobarea sau, după caz, revizuirea modului de organizare a entității desemnate ca fiind autoritatea competentă în sensul prevederilor proiectului de lege, să inițieze procesul de ajustare a structurii, efectivului-limită și organigramei entității respective și să asigure aprobarea statelor de personal noi ș a schemei de încadrare corespunzătoare.

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

Monitorizarea modului de implementare a opțiunii recomandate de reglementare printr-o lege cadru a domeniului securității cibernetice, urmează a se efectua în conformitate cu următorii indicatori de performanță:

1) ***În interiorul perioadei tranzitorii:***
   - instituirea și asigurarea funcționalității depline a echipei de răspuns la incidentele de securitate cibernetică la nivel național și, implicit a autorității competente în domeniul securității cibernetice;
   - gradul de corespundere a CSIRT național criteriilor stabilite de art. 11 din Directiva NIS2
   - ponderea numărului actelor normative de implementare a legii aprobate, prevăzute în textul legii;
   - finalizarea procesului de identificare a furnizorilor de servicii de către autoritatea competentă, în conformitate cu procedurile stabilite de lege și de actele normative de punere în aplicare a acesteia, în termenul de 3 luni din data finalizării procesului de constituire și asigurării funcționalității depline a acesteia.
2) ***După finalizarea perioadei tranzitorii:***
   - indicatorii de monitorizare și cei de evaluare ce vor fi stabiliți de Strategia națională de securitate cibernetică și Planul de acțiuni de implementare a acesteia aprobate de Guvern în temeiul prevederilor legii;
   - numărul incidentelor de securitate cibernetică prevenite și soluționate de CSIRT în raport cu perioadele precedente de până la instituire conform prevederilor legii;
   - ponderea furnizorilor de servicii care corespund cerințelor stabilite de măsurile de securitate prevăzute de lege, în numărul total de furnizori de servicii identificați de către autoritatea competentă, estimare ce urmează a fi efectuată de autoritatea competentă în procesul de supraveghere și control al corespunderii acestor furnizori cu cerințele stabilite de lege.

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

Într-o **primă etapă** evaluarea performanței implementării prevederilor proiectului de lege va fi determinată de perioada tranzitorie de circa 18 luni (intrarea în vigoare - 12 luni de la data publicării + 6 luni de la data intrării în vigoare a legii pentru aprobarea de către Guvern a Strategiei naționale de securitate cibernetică) în interiorul căreia urmează a fi aprobat întregul cadrul normativ de punere în aplicare a prevederilor legii, de aducere în concordanță cu prevederile legii a cadrului normativ legal și cel al Guvernului. Astfel, un indicator de performanță inițial ar fi aprobarea de către Guvern, în termenele stabilite de proiectul de act normativ al întregului spectru de acte normative necesare punerii în aplicare a prevederilor noii legi.

De asemenea, în perioada tranzitorie de 6 luni după publicarea legii, Guvernul urmează să instituie (desemneze) autoritatea competentă, dotând-o cu resursele umane, financiare și tehnice corespunzătoare. Nivelul de performanță în acest context urmează a fi evaluat în conformitate cu

criteriile stabilite la art. 11 alin. (1) din Directiva NIS2 pentru echipa de răspuns la incidentele de securitate cibernetică instituită la nivel național (CSIRT), și anume:

1) disponibilitate ridicată a canalelor lor de comunicare evitând punctele unice de defecțiune;
2) dispunerea de mai multe mijloace pentru a fi contactate și pentru a contacta alte entități în orice moment;
3) specificarea clară a canalelor de comunicare și difuzarea acestora bazei de utilizatori și a partenerilor de cooperare;
4) localuri și sistemele informatice de suport situate în amplasamente securizate;
5) sistem și mecanisme adecvate de gestionare și procesare a cererilor, în special în vederea facilitării eficace și eficiente a transferurilor;
6) asigurarea confidențialității și credibilității operațiunilor;
7) personal adecvat pentru a asigura disponibilitatea permanentă a serviciilor echipei CSIRT, inclusiv instruit și cu formare continuă permanentă, asigurată în mod corespunzător sarcinilor pe care le realizează, și capabil să-și dezvolte singur capacitățile tehnice;
8) sisteme redundante și spațiu de lucru de rezervă pentru a asigura continuitatea serviciilor lor.

Într-o etapă ulterioară, care începe cu aprobarea de către Guvern a Strategiei naționale de securitate cibernetică și a planului de acțiuni pentru implementarea acesteia, indicatorii de performanță în baza cărora se va evalua modul și gradul de implementare a inițiativei în speță, inclusiv în vederea evaluării creșterii rezilienței cibernetice și a nivelului de asigurare a securității rețelelor și sistemelor informatice la nivel național, vor constitui indicatorii de monitorizare și evaluare stabiliți în documentul respectiv de politici. Astfel, în conformitate cu indicatorii de monitorizare a activităților și a indicatorilor de evaluare de realizare a obiectivelor stabilite în Strategia și în planul respectiv de acțiuni, urmează a fi măsurat nivelul de atingere a obiectivelor urmărite prin aprobarea proiectului de act normativ în speță.

6. Consultarea

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

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

1. ***Guvernul și autoritatea administrației publice centrale de specialitate responsabilă de realizarea politicii de stat în domeniul securității cibernetice*** (competență exercitată în prezent de Ministerul Economiei, în coordonarea Viceprim-ministrului pentru digitalizare) – din perspectiva, pe de o parte, a necesității instituirii unui mecanism instituțional și organizațional viabil de implementare a politicii de stat în domeniul securității cibernetice, în vederea asigurării rezilienței cibernetice a cercului de subiecți care cad sub incidența actului normativ, iar, pe de altă parte – necesitatea armonizării cadrului normativ național ;
2. ***Persoanele juridice de drept public***, inclusiv ***autoritățile administrației publice locale*** – categorie care prin efectul legii sunt identificate ca furnizori de servicii;
3. ***Persoanele juridice de drept privat, inclusiv întreprinderile de stat,*** care cad sub incidența prevederilor proiectului de act normativ, adică care urmează, în baza mecanismului propus în proiectul de act normativ și dezvoltat în actele normative de punere în aplicare al acestuia, să fie identificate de autoritatea competentă ca furnizori de servicii, în funcție de sectoarele/subsectoarele în care aceștia prestează serviciile respective;
4. ***Persoanele juridice de drept privat, altele decât cele menționate la pct. 3,*** care deținând rețele și sisteme informatice ce sunt utilizate în procesul de prestare a serviciilor, deși nu vor cădea sub incidența obligațiilor stabilite de actul normativ, totuși vor dispune de dreptul de notificare voluntară și participare la platforme și comunități privind schimbul de informații în materie de securitate cibernetică.
5. ***Utilizatorii finali ai serviciilor*** prestate de furnizorii de servicii din perspectiva interesului pe care îl au în creșterea calității serviciilor de care beneficiază, în mod special din punctul de vedere al securității și protecției datelor cu caracter personal.

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

După finalizarea elaborării proiectului, analiza de impact, proiectul de act normativ propriu-zis și tabelul de concordanță al proiectului urmează a fi supuse unor consultări preliminare cu viceprim-ministrul pentru digitalizare, Instituția publică Serviciul Tehnologia Informației și Securitate Cibernetică precum și cu subdiviziunea structurală internă a Ministerului Economiei responsabilă de realizarea politicii de stat în domeniul securității cibernetice.

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;
c) Grupul de lucru al Comisiei de stat pentru reglementarea activității de întreprinzător, având în vedere faptul că proiectul de act normativ conține norme de reglementare a activității de întreprinzător.

După examinarea pachetului de documente de către instituțiile menționate a literele a)-c), 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 poziţia fiecărei entităţi consultate față de documentul de analiză a impactului şi/sau intervenţia 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 alterativă 1*	*Opțiunea alterativă 2*
Economic			
costurile desfășurării afacerilor	-2		
povara administrativă	-1		
fluxurile comerciale și investiționale	0		
competitivitatea afacerilor	0		
activitatea diferitor categorii de întreprinderi mici și mijlocii			
concurența pe piață	0		
activitatea de inovare și cercetare	+1		
veniturile și cheltuielile publice	-1		
cadrul instituțional al autorităților publice	+2		

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

eficiența și performanța energetică	0		
bunăstarea animalelor	0		
riscuri majore pentru mediu (incendii, explozii, accidente etc.)	0		
utilizarea terenurilor	0		
alte aspecte de mediu	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