

**GUVERNUL REPUBLICII MOLDOVA**

HOTĂRÎRE nr. \_\_\_\_\_  
din \_\_\_\_\_

**CU PRIVIRE LA PROGRAMUL NAȚIONAL DE SECURITATE  
CIBERNETICĂ A REPUBLICII MOLDOVA PENTRU ANII 2016-2020**

---

În temeiul prevederilor Legii nr.64-XII din 31 mai 1990 cu privire la Guvern (republicată în Monitorul Oficial al Republicii Moldova, 2002, nr.131-133, art. 1018), cu modificările și completările ulterioare, Guvernul

**HOTĂRÂSTE:**

1. Se aprobă Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (se anexează).
2. Ministerele și autoritățile administrative centrale vor prezenta Ministerului Tehnologiei Informației și Comunicațiilor, semestrial, pînă la data de 1 august și 1 februarie, informația despre executarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, conform responsabilităților stabilite în acesta.
3. Ministerul Tehnologiei Informației și Comunicațiilor va generaliza informația recepționată și va prezenta Guvernului, semestrial, pînă la data de 1 septembrie și 1 martie, raportul despre executarea Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020.
4. Monitorizarea și coordonarea procesului de realizare a Programului național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 se pune în sarcina Ministerului Tehnologiei Informației și Comunicațiilor.

**PRIM-MINISTRU**

**VALERIU STRELET**

## **PROGRAMUL NAȚIONAL DE SECURITATE CIBERNETICĂ A REPUBLICII MOLDOVA PENTRU ANII 2016-2020**

### **I. DISPOZIȚII GENERALE**

1. Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (în continuare – Program) are drept scop 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 rîndul său va stimula creșterea gradului de competitivitate economică, de coeziune socială, precum și de creare a locurilor noi de muncă.

2. Termenii utilizati în Program au semnificația:

1) *Amenințare cibernetică* – circumstanță sau eveniment care constituie un pericol potențial la adresa securității cibernetice;

2) *Apărare cibernetică* – acțiuni desfășurate în scopul protecției, monitorizării, analizării, detectării, contracarării agresiunilor și asigurării răspunsului oportun împotriva amenințărilor asupra infrastructurilor cibernetice destinate apărării naționale;

3) *Atac cibernetic* – acțiune ostilă desfășurată în spațiul cibernetic de natură să afecteze securitatea cibernetică;

4) *Audit de securitate cibernetică* – evaluare sistemică, detaliată, măsurabilă și tehnică a modului în care politicile de securitate cibernetică sunt aplicate la nivelul infrastructurilor cibernetice, precum și emiterea de recomandări pentru minimizarea riscurilor identificate;

5) *Incident cibernetic* – eveniment survenit în spațiul cibernetic ale cărui consecințe afectează securitatea cibernetică;

6) *Eveniment survenit în spațiul cibernetic* – acțiune desfășurată în spațiul cibernetic care are drept consecință modificarea stării infrastructurilor cibernetice;

7) *Infrastructuri cibernetice* – infrastructuri din domeniul tehnologiei informației și comunicații, constând din sisteme informatiche, aplicații aferente, rețele și servicii de comunicații electronice;

8) *Infrastructuri cibernetice de interes național (ICIN)* – infrastructurile cibernetice care susțin servicii publice sau de interes public, precum și servicii ale societății informaționale, a căror afectare poate aduce atingere securității naționale sau prejudicii grave statului sau cetățenilor acestuia;

9) *Managementul identității* – metode de validare a identității persoanelor cînd acestea accesează anumite infrastructuri cibernetice;

10) *Managementul riscului* – un proces complex, continuu și flexibil de identificare, evaluare și contracarare a riscurilor la adresa securității cibernetice, bazat pe utilizarea unor tehnici și instrumente complexe, pentru prevenirea pierderilor de orice natură;

11) *Operații în rețelele de calculatoare* – un proces complex de planificare, coordonare, sincronizare, armonizare și desfășurare a acțiunilor în spațiul cibernetic

pentru protecția, controlul și utilizarea rețelelor de calculatoare, în scopul obținerii superiorității informaționale, concomitent cu neutralizarea capabilităților adversarului;

12) *Reziliența infrastructurilor cibernetice* – capacitatea componentelor infrastructurilor cibernetice de a rezista unui incident sau atac cibernetic și de a reveni în starea de normalitate;

13) *Risc de securitate în spațiul cibernetic* – probabilitatea ca o amenințare să se materializeze, exploatând o anumită vulnerabilitate specifică infrastructurilor cibernetice;

14) *Securitate cibernetică* – stare de normalitate rezultată în urma aplicării unui ansamblu complex de măsuri proactive și reactive prin care se asigură în spațiul cibernetic confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic, a sistemelor și resurselor informaționale, a serviciilor publice și private. Măsurile proactive și reactive includ politici, concepte, standarde și ghiduri de securitate, managementul riscului, activități de instruire și conștientizare, implementarea de soluții tehnice de protecție a infrastructurilor cibernetice, managementul identității, managementul consecințelor;

15) *Spațiu cibernetic* – mediu virtual, generat de infrastructurile cibernetice, incluzând conținutul informațional procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acest mediu;

16) *Vulnerabilitate în spațiul cibernetic* – ineficacitatea în proiectarea și implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente care poate fi exploatață de către o amenințare.

17) Alți termini din Program sunt utilizați în sensul definit în legile privind prevenirea și combaterea criminalității informaticе nr.20-XVI din 03.02.2009, comunicațiilor electronice nr.241-XVI din 15.11.2007 și cu privire la informatizare și la resursele informaționale de stat nr.467-XV din 21.11.2003.

### 3. Principiile securității cibernetice:

1) *Protecția drepturilor și libertăților fundamentale ale omului.* Asigurarea securității cibernetice poate fi adecvată și eficientă doar în cazul în care se bazează pe drepturile și libertățile fundamentale ale omului, inclusiv pe valorile general umane. Orice transfer, procesare sau stocare de date, inclusiv celor cu caracter personal, comercial și confidențial nu pot fi asigurate fără utilizarea unor sisteme informaționale, rețele și servicii de comunicații electronice securizate. Orice tratare a informațiilor efectuat în scopul asigurării securității cibernetice trebuie să fie conformă cadrului legal și tratatelor la care Republica Moldova este parte.

2) *Accesul pentru toți.* Accesul sigur și liber la Internet și resursele acestuia este un drept al fiecărei persoane. Accesibilitatea limitată sau lipsa acestui acces, precum și analfabetismul digital constituie un dezavantaj și pentru cetăteni și pentru autorități.

3) *Reziliența cibernetică.* Sesizarea preventivă sau anticipată a amenințărilor și atacurilor cibernetice, altor evenimente survenite în spațiul cibernetic este esențială datorită caracterului lor transfrontalier și de materializare asimetrică. Astfel, acestea urmează a fi depistate pentru eliminarea sau diminuarea efectelor care pot afecta starea de normalitate a securității cibernetice. Amenințările cibernetice apar urmăre exploatarii unor vulnerabilități. Mediul de amenințări și vulnerabilități este extrem de fluid și dinamic: amenințările pot apărea în decurs de zile sau chiar ore. Urmăre acestui mediu

specific, responsabilitii și coordonatorii de securitate cibernetică trebuie să monitorizeze continuu acest mediu, să depisteze amenințările cibernetice și să consulte permanent sursele recunoscute de informare ale companiilor-lider în domeniul securității cibernetice, experții din mediul academic și diverse publicații.

4) *Administrare multiparticipativă*. Spațiul cibernetic nu poate fi ținut sub control de o singură entitate atât la nivel local sau național, cât și la nivel regional sau global. În spațiul cibernetic nu pot fi fixate frontiere analogic frontierelor între unitățile administrativ-teritoriale sau state. Astfel, pentru a asigura reziliența cibernetică, autoritățile publice și sectorul privat trebuie să-și dezvolte abilitățile necesare și să coopereze în mod eficient între ele. Prin administrare multiparticipativă și acțiuni comune, autoritățile publice și sectorul privat pot să combată cu succes riscurile și amenințările cibernetice, pot contribui cu un răspuns coordonat și eficient la evenimentele survenite în spațiul cibernetic, care au dimensiuni naționale și transfrontaliere.

5) *Responsabilitatea comună și răspunderea personalizată de asigurare a securității cibernetice*. Dependența crescîndă a activităților umane de tehnologiile informației și comunicațiilor implică vulnerabilități care urmează a fi identificate, analizate minuțios și eliminate sau diminuate în dependență de pericolul potențial la adresa securității cibernetice. Toate părțile implicate în executarea activităților de asigurare a securității cibernetice, fie că sunt autorități publice, fie că aparțin sectorului privat sau sunt doar simpli cetățeni, trebuie să recunoască această responsabilitate comună și răspundere personalizată, să întreprindă acțiuni proprii și comune de protecție, să contribuie la consolidarea securității cibernetice și apărării cibernetice în conformitate cu cadrul legal.

## II. SITUAȚIA ACTUALĂ ȘI IDENTIFICAREA PROBLEMEI DE BAZĂ

4. Proliferarea tehnologiilor informației și de comunicații moderne, ridică la un alt nivel abordarea amenințărilor, riscurilor și vulnerabilităților dintr-o societate informațională. În prezent, la nivel mondial, atacurile cibernetice capătă o frecvență, complexitate și o ampoloare din ce în ce mai mare, aducînd pagube enorme sectorului guvernamental, privat și cetățenilor, urmare caracterului lor asimetric. Accesarea neautorizată a rețelelor și serviciilor de comunicații electronice, modificarea, ștergerea sau deteriorarea neautorizată de date informative, restricționarea ilegală a accesului la aceste date și spionajul cibernetic constituie constrîngeri la nivel global. Amenințările și risurile, atacurile și incidentele cibernetice, precum și alte evenimente survenite în spațiul cibernetic se materializează prin exploatarea vulnerabilităților de natură umană, tehnică și procedurală. Prejudiciile economice urmare exploatarii unor asemenea vulnerabilități sunt destul de semnificative.

5. Astfel, potrivit rapoartelor Norton<sup>1</sup> pentru anii 2012 și 2013, costul global al criminalității cibernetice este în creștere. Pierderile globale au constituit în anul 2013 circa 113 miliarde dolari față de 110 miliarde dolari în 2012, iar pierderile în mediu pe o victimă au constituit 298\$ în 2013 față de 197\$ în anul 2012. Potrivit datelor din aceleasi rapoarte, suntem supuși în permanență unor riscuri majore la accesarea rețelelor wi-fi neprotejate. Este destul de mare riscul accesării neautorizate a poștei

<sup>1</sup> Sursa. <https://www.symantec.com>

electronice personale (54% în anul 2013 față de 64% în 2012) urmare interceptării parolei de accesare, precum și riscul accesării neautorizate a paginilor personale a utilizatorilor rețelelor sociale (56% în anul 2013 față de 63% în 2012). Este destul de ridicat și riscul în comerțul electronic, efectuat prin magazine on-line, accesate prin intermediul rețelelor wi-fi neprotejate (29% în anul 2013 față de 31% în anul 2012). A crescut riscul accesării neautorizate a conturilor bancare urmare efectuării operațiunilor prin intermediul rețelelor wi-fi neprotejate, care în anul 2013 a crescut la 29% față de 24% în 2012. Accesarea conturilor bancare prin intermediul rețelelor wi-fi neprotejate sporește considerabil riscul interceptării datelor de acces și, prin urmare, accesării neautorizate ulterioare a acestora în scopuri criminale.

6. Urmare ratei destul de mare a riscurilor de accesare sus enunțate, precum și a altor riscuri cibernetice specifice, numărul victimelor în anul 2013, care au suferit în urma unor fraude, atacuri și incidente cibernetice, a constituit circa 379 milioane față de 558 milioane de victime în anul 2012. Astfel, în anul 2013 au fost afectați: 64% de proprietari ai dispozitivelor mobile, 63% de utilizatori ai rețelelor sociale, 68% de utilizatori ai rețelelor wi-fi publice, 65% de părinți ai copiilor și 68% de piețe emergente. În pofida numărului foarte mare de victime, doar o parte din utilizatori ai Internetului conștientizează faptul că dispozitivele electronice ale acestora (telefoane mobile, tablete, laptopuri, calculatoarele, etc.) pot fi supuse unor atacuri cibernetice în urma conectării acestora la Internet, impactul cărora poate fi esențial diminuat dacă se vor respecta cele mai simple recomandări de siguranță. Anume acest fapt favorizează considerabil creșterea criminalității cibernetice (informatică) prin exploatarea vulnerabilităților de natură umană.

7. Până în prezent, nu este efectuat nici un audit de securitate cibernetică, nu există studii sau rapoarte, care în complexitate ar reflecta situația Republicii Moldova privind criminalitatea informatică, amenințările și riscurile cibernetice, atacurile și incidentele cibernetice, alte evenimente survenite în spațiul cibernetic, numărul victimelor și prejudiciile economice urmare materializării acestora.

8. Unica sursă oficială, care include date statistice privind criminalitatea informatică este Registrul de evidență a infracțiunilor, a cauzelor penale, a persoanelor care au săvîrșit infracțiuni și a materialelor cu privire la infracțiuni din cadrul Sistemului informațional integral automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvîrșit infracțiuni. Potrivit informației extrase din sistemul informațional automatizat "Registrul informației criminalistice și criminologice", prezentată de Ministerul Afacerilor Interne, începînd cu anul 2013 și pînă în august 2015 inclusiv, au fost înregistrate 72 infracțiuni informatic pe art.259-261<sup>1</sup> și art.208<sup>1</sup> ale Codului Penal al Republicii Moldova, cu un prejudiciu material estimat la circa 21588 mii lei. În particular, urmare activităților Procuraturii Generale și Inspectoratului General al Poliției, au fost înregistrate: în 2013 – 23 de infracțiuni cu un prejudiciu de circa 14139 mii lei, în 2014 – 24 de infracțiuni cu un prejudiciu de circa 1323 mii lei, iar în primele 8 luni ale anului 2015 – 25 de infracțiuni cu un prejudiciu de circa 6126 mii lei. Concomitent, în aceeași perioadă de timp, au fost înregistrate 57 de contravenții de încălcare a dreptului de autor și a drepturilor conexe, cu valoarea totală a amenziilor aplicate de circa 99 mii lei. Cu toate că datele din Registrul informației criminalistice și criminologice încă nu sunt complete și nu reflectă toate clasele de infracțiuni și contravenții în sensul Convenției Consiliului Europei de la Budapesta

privind criminalitatea informatică, deja se constată că tendința săvîrsirii infracțiunilor și contravențiilor informatici este în creștere.

9. Totodată, conform datelor Centrului de Telecomunicații Speciale, numărul atacurilor cibernetice asupra serverelor WEB a crescut în anul 2014 față de anul 2013 cu circa 26%, iar vulnerabilitățile porturilor deschise au sporit cu circa 385%. Posibilitățile de infectare a calculatoarelor cu virusi informatici au crescut cu circa 27%. Numărul incidentelor asupra poștei electronice guvernamentale s-a micșorat în 2014 față de 2013 cu circa 1%. Concomitent, s-a micșorat și ponderea acestor incidente din totalul atacurilor cibernetice. În 2014 această pondere s-a diminuat la 40% față de 51% în 2013.

10. Pericolul major de materializare a acestor evenimente survenite în spațiul cibernetic, în care nu există frontiere, a impus ca pe agenda unui sir de țări, începînd cu anul 2009, să fie inclusă ca subiect dominant problema securității cibernetice. Deja 56 de state din lume dispun de documente de politici<sup>2</sup> aprobată în domeniul securității cibernetice, inclusiv 21 de state ale Uniunii Europene. 37 de state din lume, au aprobat documentele sale de politici pe parcursul anilor 2013-2015, inclusiv 14 state – în 2015.

11. Cadrul legal intern al acestor țări se ajustează corespunzător prevederilor Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, ținîndu-se cont de Recomandările Uniunii Internaționale a Telecomunicațiilor referitoare la securitatea cibernetică.

12. Republica Moldova a ratificat Convenția Consiliului Europei privind criminalitatea informatică prin Legea nr.6-XVI din 02.02.2009. Totodată, a fost adoptată Legea nr.20-XVI din 03.02.2009 privind prevenirea și combaterea criminalității informatici, au fost introduse modificări și completări în Codul penal în corespondere cu prevederile Convenției ratificate, însă prevederile Convenției de ordin procedural, precum și celor ce țin de dezvoltarea punctului de contact al retelei 24/7 încă nu sunt implementate.

13. Urmare analizei efectuate este identificată problema de bază – lipsa unui sistem de management al securității cibernetice, în cadrul căruia să se efectueze coordonat planificarea și utilizarea resurselor disponibile, identificarea vulnerabilităților și riscurilor în urma auditului de securitate cibernetică, a intervențiilor necesare pentru diminuarea impactului dăunător al criminalității, atacurilor și incidentelor cibernetice asupra dezvoltării sigure a societății informaționale. Acest sistem urmează să fie extins în toate sferele vieții sociale, economice și politice din țară. Aceasta trebuie să fie creat și implementat de către entitățile vizate din domeniul public și cel privat.

14. Lipsa unui sistem de management al securității cibernetice a Republicii Moldova generează și lipsa datelor statistice complete, veritabile, actualizate și structurate, care la rîndul său impune unele limitări în analiza efectuată și identificarea de soluții optime. De rezultatul soluționării problemei de bază identificate, depinde eficiența măsurilor întreprinse în vederea dezvoltării unei societăți informaționale securizate în Republica Moldova, avansării tehnologice și științifice, participării active a cetățenilor la viața socială și culturală, precum și dinamica de creștere economică a țării.

<sup>2</sup> Sursa <https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world>

15. Pînă în prezent nu există un cadru legal privind delimitarea și armonizarea competențelor și responsabilităților instituțiilor statului și celor private în domeniul securității cibernetice, nu se aplică mecanismul obligatoriu de audit al securității cibernetice în cadrul instituțiilor publice și private, prin care pot fi identificate vulnerabilitățile, riscurile și amenințările cibernetice în scopul prevenirii sau diminuării prin măsuri speciale a impactului atacurilor, incidentelor și altor evenimente survenite în spațiul cibernetic, originea cărora este dificil de stabilit.

16. În afara reglementărilor legislative, normative și tehnico-normative, persistă un șir de probleme specifice ce țin de asigurarea securității cibernetice a Republicii Moldova și care sunt părți componente ale problemei de bază identificată mai sus:

1) Nu este asigurată o siguranță deplină la procesarea, stocarea și accesarea datelor publice, indiferent de clasificarea acestora;

2) Securitatea și integritatea rețelelor și serviciilor de comunicații electronice nu sunt ajustate la standardele și recomandările Uniunii Europene, Uniunii Internaționale a Telecomunicațiilor, la prevederile Acordului de Asociere între Republica Moldova și Uniunea Europeană;

3) Capacități insuficiente de prevenire și reacție urgentă la nivel național (CERT), urmare caracterului asimetric al atacurilor și incidentelor cibernetice;

4) Cadrului legislativ-normativ național nu este integral armonizat la prevederile Convenției Consiliului Europei privind criminalitatea informatică, instituțiile vizate nu dispun de competențe clare privind asigurarea securității cibernetice;

5) Capacități reduse de apărare cibernetică urmare caracterului asimetric al atacurilor cibernetice;

6) Nu este asigurată educația, formarea și informarea continuă în domeniul securității cibernetice;

7) Insuficiența cooperării și interacțiunii internaționale privind identificarea riscurilor, vulnerabilităților, altor evenimente survenite în spațiul cibernetic global și prevenirea amenințărilor și atacurilor cibernetice transfrontaliere.

17. Soluționarea problemei de bază, inclusiv a problemelor specifice, presupune intervenții în cadrul legislativ și instituțional, în cadrul normativ și tehnico-normativ, în pregătirea continuă și certificarea specialiștilor în domeniul securității cibernetice, auditului de securitate cibernetică a entităților care dețin infrastructuri cibernetice, sisteme informaționale și rețele de comunicații electronice, inclusiv a celor care prestează servicii informative și de comunicații electronice.

18. Totodată, soluționarea problemelor sus identificate este în concordanță cu obiectivul general orizontal privind asigurarea securității cibernetice din cadrul Strategiei naționale de dezvoltare a societății informaționale "Moldova Digitală 2020", aprobată prin Hotărârea Guvernului nr.857 din 31.10.2013, inclusiv cu prevederile Acordului de asociere între Republica Moldova și Uniunea Europeană, ratificat de Parlament prin Legea nr.112 din 02.07.2014, precum și cu noua viziune a Strategiei securității naționale a Republicii Moldova.

### **III. OBIECTIVELE PROGRAMULUI**

19. Obiectivul principal al Programului, urmare analizei efectuate și identificării problemei de bază, este crearea și implementarea unui sistem de management al securității cibernetice a Republicii Moldova care să asigure, entităților vizate din

domeniul public și cel privat, planificarea și utilizarea resurselor disponibile, identificarea intervențiilor necesare pentru diminuarea impactului dăunător al criminalității, atacurilor și incidentelor cibernetice asupra dezvoltării sigure a societății informaționale.

20. Realizarea obiectivului principal al Programului, în conformitate cu problemele specifice identificate în capitolul precedent, se va produce prin realizarea complexă a 7 obiective specifice:

- 1) "Procesarea, stocarea și accesarea sigure a datelor, inclusiv a datelor de interes public";
- 2) "Securitatea și integritatea sigure a rețelelor și serviciilor de comunicații electronice";
- 3) "Dezvoltarea capacitaților de prevenire și reacție urgentă la nivel național (rețeaua CERT națională)";
- 4) "Prevenirea și combaterea criminalității informaticе";
- 5) "Consolidarea capacitaților de apărare cibernetică";
- 6) "Educația, formarea și informarea continuă în domeniul securității cibernetice";
- 7) "Cooperarea și interacțiunea internațională în sferele ce țin de securitatea cibernetică".

#### **IV. ACTIUNILE CE URMEAZĂ A FI ÎNTREPRINSE PENTRU REALIZAREA OBIECTIVELOR**

21. Pentru realizarea obiectivelor, formulate în capitolul precedent, au fost identificate împreună cu autoritățile vizate un sir de acțiuni ce urmează a fi executate, care pentru comoditate și în corespondere cu obiectivele specifice, fiind sistematizate, alcătuiesc un Plan de acțiuni de implementare a Programului național de securitate cibernetică a Republicii Moldova (în continuare – Planul de acțiuni).

22. Conform Planului de acțiuni (a se vedea anexa nr.1 la Program), obiectivul specific de la pct.3.2.1 "Procesarea, stocarea și accesarea sigure a datelor, inclusiv a datelor de interes public" va fi realizat prin asigurarea ajustării cadrului normativ-legislativ privind securitatea cibernetică a Republicii Moldova, clasificarea tipurilor de informație, analiza și elaborarea propunerilor de aplicare la nivel național a standardelor ce țin de procesarea, stocarea și accesarea sigure a datelor, identificarea unei metodologii pentru evaluarea vulnerabilităților sistemelor informaționale în baza standardelor prestabilite, elaborarea cerințelor minime obligatorii de securitate cibernetică, certificarea specialiștilor, efectuarea auditului de securitate cibernetică cu elaborarea planurilor de înlăturare a vulnerabilităților depistate, inclusiv prin executarea altor acțiuni, conform Planului de acțiuni.

23. Obiectivul specific de la pct.3.2.2 "Securitatea și integritatea sigure a rețelelor și serviciilor de comunicații electronice" va fi realizat prin armonizarea legislației din domeniul comunicațiilor electronice la directivele-cadru UE din domeniu, stabilirea măsurilor minime de securitate ce trebuie întreprinse de către furnizori pentru asigurarea securității și integrității rețelelor și serviciilor de comunicații electronice cu raportarea incidentelor cu impact asupra acestor rețele și servicii, aplicarea la nivel național a standardelor europene și internaționale ce țin de protecția și securitatea

rețelelor de comunicații electronice, inclusiv prin executarea altor acțiuni, conform Planului de acțiuni.

24. Obiectivul specific de la pct.3.2.3 "Dezvoltarea capacităților de prevenire și reacție urgentă la nivel național (rețeaua CERT națională)" va fi realizat prin crearea Centrului național de reacție la incidentele de securitate cibernetică (CERT) și CERT-urilor departamentale în autoritățile publice centrale (APC), autoritățile publice locale (APL), alte entități ce dețin sisteme informaționale de stat, stabilirea obligațiunilor de raportare și evidență operativă obligatorie a incidentelor de securitate cibernetică pentru APC, APL și mediul de afaceri din domeniul Tehnologiei Informației și Comunicațiilor (TIC), elaborarea și aplicarea unor metode de prevenire anticipată a incidentelor de securitate cibernetică în Republica Moldova, desfășurarea unor exerciții și antrenamente de consolidare a capacităților de reacție la incidentele și atacurile cibernetice cu blocarea acestora, inclusiv prin executarea altor acțiuni, conform Planului de acțiuni.

25. Obiectivul specific de la pct.3.2.4 "Prevenirea și combaterea criminalității informaticе" va fi realizat prin elaborarea proiectelor de legi pentru armonizarea continuă a legislației penale, contravenționale și procesuale la prevederile Convenției Europene privind criminalitatea informatică și cu deciziile Comitetului acestei Convenții, ratificarea Protocolului adițional la această Convenție, ajustarea legislației și statisticii naționale la prevederile Convenției Consiliului Europei pentru protecția copiilor împotriva exploatarii și abuzurilor sexuale, și Protocolului adițional respectiv la această Convenție, consolidarea capacităților de prevenire și combatere a criminalității informaticе în cadrul Procuraturii Generale (PG), Serviciului de Informații și Securitate (SIS), Inspectoratului General al Poliției (IGP) al Ministerului Afacerilor Interne (MAI), instruirea lucrătorilor organelor de drept în domeniul securității cibernetice conform recomandărilor proiectului EAP al Consiliului Europei, inclusiv prin executarea altor acțiuni, conform Planului de acțiuni.

26. Obiectivul specific de la pct.3.2.5 "Consolidarea capacităților de apărare cibernetică" va fi realizat prin stabilirea autorităților responsabile și cooperare reciprocă pe timp de pace, în situații de criză, asediu și război în cadrul spațiului cibernetic, elaborarea compartimentului de apărare cibernetică a Republicii Moldova ca parte componentă a Strategiei securității informaționale a Republicii Moldova, instruirea în domeniul securității cibernetice a personalului din sfera securității și apărării naționale, dezvoltarea capabilităților militare de protecție a infrastructurii și serviciilor critice ce țin de apărarea națională, inclusiv prin executarea altor acțiuni, conform Planului de acțiuni.

27. Obiectivul specific de la pct.3.2.6 "Educația, formarea și informarea continuă în domeniul securității cibernetice" va fi realizat prin crearea unui laborator de securitate cibernetică, completarea curriculumului de învățămînt cu studierea materiei din domeniul securității cibernetice, elaborarea și implementarea conceptului campaniilor de informare și conștientizare a riscurilor din spațiul cibernetic, stabilirea cerințelor de competență în domeniul securității cibernetice pentru personalul din sectorul public și privat, evidența, instruirea, evaluarea și certificarea acestui personal, organizarea și efectuarea trainingurilor și workshopurilor în domeniul securității

cibernetice pentru personalul instituțiilor deținătoare de elemente ale infrastructurii cibernetice critice, inclusiv prin executarea altor acțiuni, conform Planului de acțiuni.

28. Obiectivul specific de la pct.3.2.7 "Cooperarea și interacțiunea internațională în sferele ce țin de securitatea cibernetică" va fi realizat prin crearea unui Centru de Excelență pentru Cercetare și Dezvoltare în domeniul securității cibernetice, stabilirea și dezvoltarea relațiilor cu comunitatea internațională de cercetare în domeniile specifice ce stau la baza securității cibernetice, dezvoltarea cooperării între sectorul public și cel privat privind identificarea soluțiilor comune de securitate cibernetică, implementarea măsurilor de evaluare a amenințărilor și riscurilor față de vulnerabilitățile cibernetice identificate, încheierea acordurilor de cooperare internațională cu echipele de tip CERT europene, Nord Atlantice și naționale din alte țări, inclusiv prin executarea altor acțiuni, conform Planului de acțiuni.

## **V. ETAPELE, TERMENELE ȘI RESPONSABILII DE IMPLEMENTARE**

29. Programul nu prevede implementarea pe etape. Însă după expirarea fiecărui an de la aprobarea acestuia se va efectua evaluarea intermediară, în cadrul căreia se va analiza și compara rezultatele intermedieare cu cele scontate, se va stabili nivelul de implementare a Programului. Urmare concluziilor din Informația de raportare a monitorizării și evaluării (IRME), în caz de necesitate, se vor propune ajustări ale obiectivelor și/sau ale rezultatelor preconizate, acțiuni noi, actualizarea Programului și/sau a Planului de acțiuni.

30. În Planul de acțiuni, anexat la Program, acțiunile sunt grupate conform obiectivelor specifice care trebuie realizate. În rubricile respective ale Planului de acțiuni sunt stabiliți responsabilii de executarea acțiunilor, coexecutorii și termenele de executare pentru obținerea rezultatului scontat. Prima instituție din lista responsabilităților se consideră "responsabil principal" de executarea acțiunii și care dirijează activitatele coexecutorilor și celorlalți responsabili, atrage partenerii de dezvoltare pentru a obține rezultatul scontat în termenul stabilit pentru acțiune.

## **VI. ESTIMAREA GENERALĂ A COSTURILOR ȘI REZULTATELE SCONTATE**

31. La rubricile respective din Planul de acțiuni (a se vedea anexa nr.1) sunt indicate rezultatele scontate și costurile estimative de realizare a fiecărei acțiuni aparte pentru obținerea acestor rezultate. Sursele de finanțare includ resursele partenerilor de dezvoltare și alocările bugetare.

32. Astfel, costurile estimative, pentru obținerea rezultatelor scontate, totalizate pe acțiunile din cadrul fiecărui obiectiv al Programului sunt după cum urmează:

1) Obiectivul specific "Procesarea, stocarea și accesarea sigure a datelor, inclusiv a datelor de interes public" - circa 9504 mii lei;

2) Obiectivul specific "Securitatea și integritatea sigure a rețelelor și serviciilor de comunicații electronice" - circa 1944 mii lei;

3) Obiectivul specific "Dezvoltarea capacităților de prevenire și reacție urgentă la nivel național (rețeaua CERT națională)" - circa 49608 mii lei;

4) Obiectivul specific "Prevenirea și combaterea criminalității informaticе" - circa 2916 mii lei;

5) Obiectivul specific "Consolidarea capacitaților de apărare cibernetică" - circa 2232 mii lei;

6) Obiectivul specific "Educația, formarea și informarea continuă în domeniul securității cibernetice" - circa 10089 mii lei;

7) Obiectivul specific "Cooperarea și interacțiunea internațională în sferele ce țin de securitatea cibernetică" - circa 648 mii lei.

33. Costul estimativ preliminar de implementare integrală a Programului este de 76941 mii lei. Rezultatul scontat al implementării Programului este un sistem de management al securității cibernetice a Republicii Moldova, creat și implementat în entitățile vizate din domeniul public și cel privat, care va asigura planificarea și utilizarea resurselor disponibile, identificarea intervențiilor necesare pentru diminuarea impactului dăunător al criminalității, atacurilor și incidentelor cibernetice asupra dezvoltării sigure a societății informaționale. Acest sistem urmează a fi extins în toate sferele vieții sociale, economice și politice din țară.

## VII. INDICATORI DE PROGRES ȘI PERFORMANȚĂ

34. Domeniul securității cibernetice, fiind relativ nou în lume, încă nu dispune de indicatorii de progres și performanță recomandați pentru monitorizarea și evaluarea implementării documentelor de politici în acest domeniu. Totodată, pornind de la necesitatea monitorizării și evaluării implementării Programului se vor aplica în complexitate 17 indicatori de rezultat (IR):

IR1 – ponderea elaborării proiectelor de acte legislative și normative, documente de politici și tehnice, calculată în % din numărul total al acestora prevăzute în Planul de acțiuni;

IR2 – ponderea rapoartelor (informațiilor) de monitorizare și evaluare realizate, calculată în % din numărul total al acestora prevăzute în cadrul Programului;

IR3 – numărul acțiunilor din Planul de acțiuni realizate (înainte de, după și în termenele prestabilite);

IR4 – numărul recomandărilor privind evitarea riscurilor și diminuarea vulnerabilităților cibernetice;

IR5 – numărul prescripțiilor tehnice și proiectelor standardelor de securitate cibernetică elaborate;

IR6 – numărul entităților care au beneficiat de instruirea angajaților în asigurarea securității cibernetice, numărul persoanelor care au beneficiat de această instruire;

IR7 – numărul entităților care au beneficiat de audit extern/intern de securitate cibernetică în scopul identificării la nivel de entitate a riscurilor și vulnerabilităților cibernetice;

IR8 – ponderea AAP care aplică politici proprii de securitate cibernetică internă;

IR9 – ponderea AAPC care au creat propriul CERT departamental în rețeaua CERT națională;

IR10 – numărul entităților participante în Sistemul de management al securității cibernetice a Republicii Moldova;

IR11 – numărul de cazuri penale și contravenționale ce țin de criminalitatea informatică înregistrate în Sistemul informațional automatizat (SIA) "Registru informației criminalistice și criminologice" (RICC), numărul persoanelor care au

săvîrșit aceste infracțiuni și/sau contravenții, numărul persoanelor pătimite, volumul prejudiciului adus pătimișilor și volumul amenzilor aplicate;

IR12 – numărul cercetărilor și studiilor efectuate în domeniul securității cibernetice;

IR13 – numărul referatelor/comunicărilor privind securitatea cibernetică făcute public;

IR14 – numărul realizat de seminare, mese rotunde, trainingurilor, workshopurilor și alte evenimente privind securitatea cibernetică, numărul participanților la acestea;

IR15 – numărul recomandărilor practice de sensibilizare a populației despre riscurile și vulnerabilitățile cibernetice, asigurarea la domiciliu a securității cibernetice;

IR16 – numărul de campanii informative organizate de instituțiile vizate în domeniul securității cibernetice;

IR17 – numărul informațiilor (rapoarte de monitorizare și evaluare, note informative etc.) publicate pe pagina web oficială a MTIC.

35. Pentru a stabili progresul și performanța implementării curente și finale a Programului, indicatorii de rezultat periodic se vor compara cu indicatorii din Strategia națională de dezvoltare a societății informaționale "Moldova Digitală 2020", cu rezultatele curente de realizare a Acordului de Asociere între Republica Moldova și Uniunea Europeană, cu Recomandările Uniunii Internaționale a Telecomunicațiilor și cu recomandările partenerilor de dezvoltare.

## **VIII. PROCEDURI DE RAPORTARE ȘI EVALUARE**

36. Procedurile de raportare și evaluare sunt orientate spre maximizarea efectelor obținute de la implementarea Programului în corespondere cu rezultatele scontate indicate la rubrica "Indicator de rezultat" din Planul de acțiuni.

37. Procesul de implementare a Programului este însotit de monitorizarea permanentă la nivel instituțional, național și internațional a realizării acțiunilor propuse și a rezultatelor real obținut pentru ca, în caz de necesitate, să fie operate modificările respective în politicile publice promovate și acțiunile întreprinse, precum și de corelare a obiectivelor și a acțiunilor din Planul de acțiuni cu rezultatele așteptate de la implementarea Programului, în scopul efectuării unei evaluări cât mai corecte a modului de implementare a Programului.

38. În cadrul procesului de monitorizare se elaborează IRME, care include date relevante privind rezultatele realizării obiectivelor Programului și executării acțiunilor respective din Planul de acțiuni, corelate cu rezultatele implementării Strategiei naționale de dezvoltare a societății informaționale "Moldova Digitală 2020". La această IRME se anexează rapoarte de progres, rapoarte de evaluare și/sau note informative, cu concluzii și propuneri. În particular, procesul de monitorizare și evaluare este orientat să contribuie la analiza situației curente și a tendințelor în realizarea obiectivelor Programului, la analiza realizării Planului de acțiuni și evaluarea corectă a rezultatelor curente și finale obținute față de rezultatele scontate.

39. La nivelul organismelor internaționale donatoare (partenerilor de dezvoltare), care finanțează careva etape, părți componente sau seturi de activități din cadrul Programului, raportarea și monitorizarea se va conforma cerințelor acestora.

Rapoartele periodice de progres, notele informative și rapoartele de evaluare se vor elabora în formatul agreat de către respectiva instituție finanțieră donatoare și Guvern.

40. La nivel național, procedurile de raportare și evaluare se efectuează de Ministerul Tehnologiei Informației și Comunicațiilor în baza IRME prezentate semestrial de responsabilii principali de executarea acțiunilor din Planul de acțiuni. Pentru fiecare an de implementare, Ministerul Tehnologiei Informației și Comunicațiilor, în colaborare cu responsabilii principali specificați în Planul de acțiuni și alte instituții interesate, elaborează Raportul anual de evaluare a implementării Programului, care se prezintă Guvernului și Consiliul intersectorial de securitate cibernetică pînă la 1 martie a anului următor. După caz, Ministerul Tehnologiei Informației și Comunicațiilor, în baza rezultatelor evaluării intermediare sau semestriale, va înainta spre examinare și aprobare proiecte a hotărîrilor Guvernului privind actualizarea Programului și/sau a Planului de acțiuni.

41. La nivel instituțional, procedurile de raportare și evaluare se efectuează semestrial de instituțiile responsabile principale de acțiunile din Planul de acțiuni. Instituția responsabilă principală de executarea acțiunii alcătuiește IRME privind realizarea acțiunii de care este responsabilă și prezintă această informație Ministerului Tehnologiei Informației și Comunicațiilor pînă la data de 1 august și 1 februarie a semestrului următor. În caz de necesitate, instituția responsabilă principală de executare a acțiunii va institui un grup de lucru din reprezentanții instituțiilor responsabile și coexecutoare a acțiuni, partenerilor de dezvoltare, altor instituții de profil, în scopul organizării și executării eficiente a acțiunii în cauză, conform unui plan de lucru aprobat. Faptul instituirii grupului de lucru și aprobării planului de lucru privind executarea acțiunii se va reflecta în IRME.

42. Evaluarea se efectuează prin comparare a rezultatelor real obținute față de cele scontate pentru perioada respectivă de raportare. După caz, evaluarea poate fi efectuată prin cercetări și studii, în colaborare cu instituțiile interesate specificate în Planul de acțiuni.

43. După expirarea fiecărui an de la aprobarea Programului se efectuează evaluarea intermediară, iar la sfîrșitul implementării Programului – evaluarea finală. În cadrul evaluării intermediare se analizează rezultatele intermediare în comparație cele scontate. Urmare concluziilor și propunerilor din Raportul de evaluare a implementării Programului, în caz de necesitate, se propun ajustări ale obiectivelor și/sau ale rezultatelor preconizate, acțiuni noi, actualizarea Programului și/sau a Planului de acțiuni.

44. La finele anului 2018 se elaborează Raportul de evaluare finală a implementării Programului în care se va reflecta realizarea obiectivelor Programului, executarea acțiunilor prevăzute în Planul de acțiuni, inclusiv impactul implementării Programului asupra securității cibernetice a Republicii Moldova. Raportul final va include concluzii și propunerile privind dezvoltarea și extinderea rezultatelor implementării în alte sfere ale vieții sociale, economice și politice din țară.

45. Ministerul Tehnologiei Informației și Comunicațiilor informează publicul despre implementarea Programului prin plasarea pe site-ul său oficial a comunicatelor de presă privind activitățile de implementare a Programului, a rezultatelor semestriale,

anuale și finale obținute la implementarea acestuia, precum și diseminarea informațiilor relevante partenerilor din țară și de peste hotare.

46. În procesul de monitorizare, un rol important se atribuie societății civile, care urmează:

1) să participe activ, în calitate de supraveghetor social al îndeplinirii prezentului Program, inclusiv prin generalizarea și diseminarea informațiilor independente privind indicatorii de progres real, precum și prin expunerea experienței avansate acumulate și a neajunsurilor depistate;

2) să se angajeze într-un dialog social cu Guvernul, în special cu Ministerul Tehnologiei Informației și Comunicațiilor, cu alte organe administrative centrale și să ofere soluții noi de sporire a eficienței implementării Programului.

Anexa nr. 1  
la Programul național de securitate cibernetică  
a Republicii Moldova pentru anii 2016-2020

**Planul de acțiuni de implementare  
a Programului național de securitate cibernetică a Republicii Moldova pentru  
anii 2016-2020**

Nr. d/o.	Acțiunea	Instituțiile responsabile	Partenerii	Termenul și/sau perioada de execuțare.	Indicator de rezultat	Surse de finanțare, costuri estimative, în lei
1.	OS "Procesarea, stocarea și accesarea sigură a datelor publice, inclusiv de interes public". Costul estimativ – 9504 mii lei.					
1.01	<p>Asigurarea ajustării cadrului normativ-legislativ privind securitatea cibernetică a Republicii Moldova, care va prevedea:</p> <ul style="list-style-type: none"> <li>a) definirea termenilor (noțiunilor) din domeniul securității cibernetice;</li> <li>b) delimitarea pe domenii a competențelor;</li> <li>c) stabilirea organului cu funcții de monitorizare a respectării cerințelor de securitate cibernetică;</li> <li>d) desemnarea organului responsabil de controlul implementării rezultatelor auditului de securitate cibernetică;</li> <li>e) obligațiile pentru deținătorii sistemelor informaționale de stat, de efectuare periodică a auditului acestor sisteme, cu stabilirea periodicității, nivelelor, cu prezentarea raportului organului competent;</li> <li>f) sancțiuni pentru nerespectarea deciziei auditului privind conformitatea cu cerințele minime obligatorii de securitate</li> </ul>	MTIC, SIS.	CS, MAI, MA, PG, ANRCETI, CNPDCP.	2016-2017	Proiect de act legislativ elaborat și remis spre examinare Guvernului.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 2592 mii.

	cibernetică. g) responsabilitatea personală pentru asigurarea securității cibernetice; h) introducerea în autoritățile publice a funcției de coordonator de securitate cibernetică, inclusiv atribuțiile principale ale acestuia; i) formarea Consiliului Intersectorial de Securitate Cibernetică (cu funcție de coordonare a activităților de securitate cibernetică).					
1.02	Clasificarea tipurilor de informație, cu excepția secretului de stat.	MTIC.	SIS, MAI, PG, CNPDCP, CTS.	2016	Clasificare aprobată.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
1.03	Analiza și elaborarea propunerilor de aplicare la nivel național a standardelor ce țin de procesarea, stocarea și accesarea sigură a datelor conform clasificării tipurilor de informație, examineate în cadrul comitetelor tehnice de standardizare CT 28 "Tehnologia informației" și CT 29 "Comunicații electronice".	MTIC, ANRCETI.	INS, CTS, MAI, MA, SIS, CNPDCP, Comitetele tehnice de standardizare CT 28 "Tehnologia informației" și CT 29 "Comunicații electronice".	2016-2017	Propuneri de aplicare a standardelor europene și internaționale ce țin de procesarea, stocarea și accesarea sigură a datelor.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 216 mii.
1.04	Identificarea unei metodologii pentru evaluarea vulnerabilităților sistemelor informaționale de stat în baza standardelor identificate, transpuse și	MTIC, SIS, ANRCETI.	INS, CS, MAI, MA, Comitetele tehnice de standardizare CT 28	2016-2017	Metodologie identificată și aprobată prin HG.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de

	aprobată.		"Tehnologia informației " și CT 29 "Comunicații electronice" ..			dezvoltare. Costul estimativ – 432 mii.
1.05	Elaborarea cerințelor minime obligatorii de securitate cibernetică.	MTIC.	MA, MAI, ANRCETI, SIS, CTS, CNPDCP.	2016-2017	Cerințe minime obligatorii de securitate cibernetică aprobată de Guvern.	Bugetul instituțiilor, în limita alocațiilor aprobată. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
1.06	Certificarea specialiștilor reieșind din standardele și metodologia identificate și cerințele minime obligatorii de securitate cibernetică aprobată.	MTIC.	CS, SIS, PG, MAI, MA.	2016-2018	Numărul APC, APL, alte entități deținătoare de sisteme informaționale de stat pentru care au fost certificați specialiști. Numărul specialiștilor certificați.	Bugetul instituțiilor, în limita alocațiilor aprobată. Resursele partenerilor de dezvoltare. Costul estimativ – 864 mii.
1.07	Identificarea și planificarea mijloacelor financiare necesare în bugetele instituțiilor pentru efectuarea auditului securității cibernetice în baza metodologiei aprobată.	MF, APC, APL, deținătorii sistemelor informaționale de stat.	CS, MAI, PG, MA, SIS.	2016	Surse și mijloace financiare alocate.	Bugetul instituțiilor, în limita alocațiilor aprobată. Resursele partenerilor de dezvoltare. Costul estimativ nu este identificat.
1.08	Efectuarea unui audit în APC, APL, alte entități deținătoare de sisteme informaționale de stat, cu scopul identificării vulnerabilităților și corespunderii cerințelor minime obligatorii de securitate cibernetică.	APC, APL, deținătorii sistemelor informaționale de stat.	MTIC.	2017-2020	Numărul entităților în care a fost efectuat auditul.	Bugetul instituțiilor, în limita alocațiilor aprobată. Resursele partenerilor de dezvoltare. Costul

						estimativ – 864 mii.
1.09	Elaborarea planului de înlăturare a vulnerabilităților conform recomandărilor auditului și executarea acestuia prin responsabilitate personalizată în cadrul APC, APL, altor entități deținătoare de sisteme informaționale de stat.	APC, APL, deținătorii sistemelor informaționale de stat.	MTIC.	2016-2018	Numărul entităților care au raportat despre realizarea planului de înlăturare a vulnerabilităților.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 1296 mii.
1.10	Elaborarea și implementarea metodologiei de marcarea informației furnizată prin sistemul care conține date cu caracter personal cu utilizarea "mărcii temporale".	CNPDCP.	MTIC, SIS, MAI, CTS.	2016-2019	Metodologie elaborată și implementată.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 216 mii.
1.11	Elaborarea și implementarea actelor legislative necesare pentru introducerea măsurilor de securitate și standardelor obligatorii în companiile TIC cu stabilirea unor cerințe minime de securitate a sistemelor informaționale de stat și a informațiilor din aceste sisteme.	MTIC, ANRCETI.	CS, MA, SIS, MAI.	2017	Acte legislative elaborate și remise spre examinare Guvernului.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
2.	OS "Securitatea și integritatea sigură a rețelelor și serviciilor de comunicații electronice". Costul estimativ – 1944 mii lei.					
2.01	Armonizarea legislației din domeniul comunicațiilor electronice cu directivele- cadru UE din domeniu.	MTIC, ANRCETI.	SIS, MAI, MA, CTS, CNPDCP.	2016	Proiect de lege elaborat și remis spre examinare Guvernului.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 216 mii.
2.02	Stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru	ANRCETI.	MTIC.	2016-2017	Proiect de act normativ aprobat prin Decizia	Bugetul instituțiilor, în limita alocațiilor

	asigurarea securității, non-repudierii și integrității rețelelor și/sau serviciilor de comunicații electronice și raportarea incidentelor cu impact semnificativ asupra acestora.				consiliului de administrare ANRCETI.	aprobată. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
2.03	Analiza și transpunerea la nivel național a standardelor europene și internaționale ce țin de protecția și securitatea rețelelor de comunicații electronice și înaintarea spre adoptare către Institutul Național de Standardizare.	MTIC.	INS, Comitetul tehnic de standardizare CT 29 "Comunicații electronice".	2016-2017	Standarde adoptate.	Bugetul instituțiilor, în limita alocațiilor aprobată. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
2.04	Efectuarea unui studiu cu privire la modificarea legislației în domeniul comunicațiilor electronice în vederea eliminării sau diminuării numărului abonaților serviciilor de comunicații electronice depersonalizați.	SIS.	MTIC, PG, MAI, CNPDCP.	2016-2017	Studiu elaborat.	Bugetul instituțiilor, în limita alocațiilor aprobată. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
2.05	Dezvoltarea în continuare a rețelei de comunicații speciale a autorităților administrației publice pe întreg teritoriul Republicii Moldova.	CS, SIS, CTS.	MAI, MA, PG, MTIC.	Conform planului aprobat de Guvern.	Numărul orașelor cuprinse de rețea de telecomunicații speciale.	Bugetul instituțiilor, în limita alocațiilor aprobată. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
3.	OS "Crearea centrului de reacție la incidente cibernetice la nivel național (rețeaua CERT națională)". Costul estimativ – 49608 mii lei.					
3.01	Crearea Centrului Național de reacție la incidentele de securitate cibernetică (CERT).	CS, MTIC, MAI, SIS.	PG, CTS, MA.	2016	CERT național creat.	Bugetul instituțiilor, în limita alocațiilor aprobată. Resursele partenerilor de dezvoltare. Costul

						estimativ – 29700 mii.
3.02	Crearea unui Sistem pe țară de alerte și informare în timp real despre incidentele de securitate cibernetică	CS, CTS.	SIS, MAI, MA, PG.	2016-2017	Sistem funcțional creat.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 594 mii.
3.03	Crearea CERT-urilor departamentale în APC, APL, alte entități deținătoare de sisteme informative de stat.	APC, APL, deținătorii sistemelor informative de stat.		2016-2017	Numărul de CERT-uri departamentale create.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 14850 mii.
3.04	Stabilirea obligațiunilor pentru APC, APL și mediul de afaceri TIC, privind raportarea operativă obligatorie a incidentelor de securitate cibernetică în baza unui mecanism de schimb de date și rolurile bine definite.	CS.	SIS, MAI, MA, MTIC, PG, CTS, CNPDCP.	2016-2017	Obligațiuni aprobate.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
3.05	Organizarea unei baze de date cu acces al autorităților responsabile privind amenințările, vulnerabilitățile și incidentele de securitate cibernetică identificate sau raportate, tehniciile și tehnologiile folosite pentru atacuri, bunele practici pentru protecția domeniului TICi	CS.	PG, MAI, SIS, MA, MTIC, CTS, BNM, IFPS, CNPDCP.	Permanent.	Sistem creat în conformitate cu concepția aprobată.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 1800 mii.
3.06	Desfășurarea exercițiilor și antrenamentelor comune de consolidare a capacitaților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice	CS, SIS, CTS.	MA, MAI, PG, MTIC.	Permanent.	Numărul de exerciții organizate. Numărul antrenamentelor efectuate. Capacitate	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor

	simulate.				ridicată a reacției la amenințările cibernetice.	de dezvoltare. Costul estimativ – 900 mii.
3.07	Consolidarea capacitaților echipei CERT din Republica Moldova pentru a asigura analiza strategică a incidentelor de securitate și coordonare a acțiunilor de răspuns la incidente de securitate în sectorul public, privat și academic, inclusiv prin organizarea training-urilor de către experti calificați .	CS, CTS.	SIS, MAI, MA, PG.	2016-2018	Capacitatea îmbunătățite.	Bugetul instituțiilor în limita alocațiilor aprobate, Resursele partenerilor de dezvoltare. Costul estimativ – 900 mii.
3.08	Elaborarea mecanismelor (modelelor) de prevenire timpurie a incidentelor de securitate cibernetică în Republica Moldova, inclusiv în baza parteneriatelor public-private.	CS, CTS.	SIS, MAI, MA.	2016-2018	Metode (modele) de prevenire timpurie a incidentelor de securitate cibernetice.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
4. OS "Prevenirea și combaterea criminalității informaticе", Costul estimativ – 2916 mii lei.						
4.01	Elaborarea proiectului de lege privind modificarea și completarea legislației penale și contravenționale pentru prevenirea și combaterea crimelor informaticе în scopul armonizării continue a acestia la prevederile Convenției Europene privind criminalitatea informatică și la deciziile Comitetului acestei Convenții.	MAI, SIS, PG.	MA, MTIC.	2016	Proiectul legii de modificare și completare a Codului penal, Codului de procedură penală și codului contravențional, elaborat și remis spre examinare Guvernului.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este estimat.
4.02	Instruirea lucrătorilor organelor de drept, specialiștilor certificați în domeniul securității cibernetice, privind: a) depistarea, investigarea, urmărirea penală și judecarea	INJ.	MAI, SIS, PG.	2016-2020	Număr de instruiriri efectuate. Număr de persoane instruite.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de

	infracțiunilor informatic; b) legătura dintre criminalitatea informatică, crima organizată, infracțiunile economice și alte categorii de infracțiuni.					dezvoltare. Costul estimativ – 900 mii.
4.03	Implementarea recomandărilor Consiliului Europei, și în special a proiectului EAP privind instruirea personalului organelor de drept.	INJ, Academia MAI.	PG, MAI, SIS, UTM, USM.	2016	Curriculum elaborat și implementat.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 900 mii.
4.04	Elaborarea și aprobarea proiectului de lege privind ratificarea protocolului adițional la Convenția Consiliului Europei privind criminalitatea informatică.	MAI.	CS, SIS, PG, MAEIE.	2016	Proiect de lege elaborat și remis spre examinare Guvernului.	Bugetul instituțiilor în limita alocațiilor aprobate. Costul nu este estimat.
4.05	Ajustarea legislației naționale la prevederile Convenției Consiliului Europei pentru protecția copiilor împotriva exploatarii și abuzurilor sexuale și a Protocolului adițional la Convenția (Lanzarote, 25 X 2007).	MAI.	PG.	2016-2017	Proiect de lege elaborat și transmis spre examinare Guvernului.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este estimat.
4.06	Efectuarea unui studiu pentru perfectarea cadrului normativ în domeniul prevenirii și combaterii crimelor informatic.	PG, MAI, SIS.	CS, MJ, MTIC, CTS, MA.	2016	Proiect de modificare a cadrului normativ, elaborat și remis spre examinare Guvernului.	Bugetul instituțiilor, în limita alocațiilor aprobate., Resursele partenerilor de dezvoltare. Costul estimativ – 216 mii.
4.07	Consolidarea în cadrul Procuraturii Generale, Serviciului de Informații și Securitate și Inspectoratului General	MAI, SIS, PG.		2016-2019	Capacitatea instituționale dezvoltate cu formularea, după caz, a	Bugetul instituțiilor, în limita alocațiilor aprobate.

	al Poliției al MAI a capacitateilor pentru prevenirea și combaterea criminalității informaticе, și după caz, formularea unor propuneri de modificare a cadrului normativ și crearea unui laborator de testare și expertiză.				unor propuneri de modificare a cadrului normativ.	Resursele partenerilor de dezvoltare. Costul estimativ – 900 mii.
5.	OS "Consolidarea capacitateilor de apărare cibernetică". Costul estimativ – 2232 mii lei.					
5.01	Elaborarea compartimentului de apărare cibernetică a RM, ca parte componentă a Strategiei securității informaționale a RM.	SIS, MA, MAI.	PG.	2016	Compartiment elaborat și prezentat pentru a fi inclus în Strategia securității informaționale a RM.	Bugetul instituțiilor, în limita alocațiilor aprobate, Resursele partenerilor de dezvoltare. Costul nu este estimat.
5.02	Stabilirea autorităților responsabile și cooperarea reciprocă pe timp de pace, în situații de criză, asediu și război în cadrul spațiului cibernetic.	SIS, MA, MAI.	CS, CTS, MED, MF, ME, MTIC, PG.	2016-2017	Proiect de act legislativ aprobat și prezentat Parlamentului spre adoptare.	Bugetul instituțiilor, în limita alocațiilor aprobate, Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
5.03	Valorificarea oportunităților spațiului cibernetic pentru promovarea intereselor, valorilor și obiectivelor naționale în spațiul cibernetic.	SIS, MTIC.	MAI, MA, PG, CNPDCP.	2016-2018	Politici elaborate și aprobate.	Bugetul instituțiilor, în limita alocațiilor aprobate, Resursele partenerilor de dezvoltare. Costul nu este estimat.
5.04	Dezvoltarea capacitateilor militare de protecție a infrastructurii și serviciilor critice destinate apărării naționale.	MA.	SIS, MAI, MTIC.	2016-2017	Capabilități dezvoltate.	Bugetul instituțiilor, în limita alocațiilor aprobate, Resursele partenerilor de dezvoltare.

						Costul estimativ – 900 mii.
5.05	Stabilirea programelor de conștientizare și educare a personalului destinat securității și apărării naționale în domeniul securității cibernetice.	SIS, MA.	MAI, MTIC, MEd.	2016-2017	Personal instruit.	Bugetul instituțiilor, în limita alocățiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 900 mii.
5.06	Stabilirea relațiilor de cooperare cu instituțiile naționale și cele internaționale din domeniu.	SIS, MA.	MAI, MAEIE, MTIC.	2016-2018	Proceduri de cooperare stabilite.	Bugetul instituțiilor, în limita alocățiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este estimat.
6.	OS "Educarea și informarea continuă în domeniul securității cibernetice". Costul estimativ – 10089 mii lei.					
6.01	Elaborarea conceptului campaniilor de informare și conștientizare despre riscurile spațiului cibernetic.	CS, MTIC.	MAI, PG, SIS, CTS, CGE, CNPDCP.	2016-2017	Conceptul campaniilor de informare aprobat.	Bugetul instituțiilor, în limita alocățiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 900 mii.
6.02	Completarea curriculumului de învățămînt în domeniul securității cibernetice.	MEd.	MTIC, CGE, UTM, USM, CNPDCP.	2016-2018	Curriculum respectiv aprobat.	Bugetul instituțiilor, în limita alocățiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
6.03	Crearea unui portal cu anunțarea operativă a pericolelor din spațiul cibernetic (digital)	CS, CTS.	MTIC.	2016-2018	Portal funcțional creat.	Bugetul instituțiilor, în limita alocățiilor

						aprobată. Resursele partenerilor de dezvoltare. Costul estimativ – 900 mii.
6.04	Stabilirea cerințelor de competență în domeniul securității cibernetice pentru personalul din sectorul public și privat, și organizarea procesului de instruire, evaluare și certificare a specialiștilor pentru acest domeniu.	MTIC.	SIS, MAI, PG, CTS, MA.	2016-2018	Numărul specialiștilor certificați.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 432 mii.
6.05	Organizarea și efectuarea trainingurilor și workshopurilor în domeniul securității cibernetice pentru personalul din sectorul public și privat, deținătorii de elemente de infrastructură critică.	MTIC, CTS.	SIS, MAI, PG, MA, CGE, UTM, USM.	Permanent.	Numărul trainingurilor și workshopurile efectuate.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este estimat.
6.06	Crearea unui laborator de securitate cibernetică.	CTS, UTM.	MTIC, MA.	2016 - 2018	Laborator creat.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 7425 mii.
7.	OS "Cooperarea și interacțiunea internațională în domeniul securității cibernetice". Costul estimativ – 648 mii lei.					
7.01	Încheierea acordurilor de cooperare cu alte echipe naționale de răspuns la incidentele legate de securitatea cibernetică (CERT), precum și US –CERT, europene și Nord Atlantice (NATO NCERT).	CS, MTIC, MA.	SIS, MAI, PG.	2016-2018	Numărul acordurilor încheiate.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este

						estimat.
7.02	Elaborarea unei platforme de coordonare și consultare în ceea ce privește evaluarea amenințărilor cibernetice și identificarea soluțiilor.	CS, MTIC.	SIS, MAI, MA, PG, CTS.	2016-2018	Platformă de coordonare și consultare elaborată și aprobată.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul estimativ – 648 mii.
7.03	Dezvoltarea cooperării cu sectorul privat (identificarea unor aplicații necesare implementării măsurilor de Securitate; înființarea de puncte de contact în vederea asigurării solicitării unor date și informații conform prevederilor legale și stabilirea unui sistem modern de transmitere a solicitărilor; realizarea de întuniri periodice în cadrul unor forumuri de dezbatere pentru cunoașterea mai bună a situației operative și pentru înțelegerea nevoilor fiecărei instituții).	CS, MTIC.	MAI, SIS, ANRCETI, PG.	2016-2019	Numărul aplicațiilor identificate. Numărul punctelor de contact. Sistem modern de transmitere a solicitărilor. Numărul întunirilor realizate.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este estimat.
7.04	Promovarea intereselor naționale de securitate cibernetică în formate internaționale de cooperare, la care participă Republica Moldova.	MTIC, MAI, MA, SIS, PG.	MAEIE, CS, CTS, CGE.	Permanent.	Formate internaționale de cooperare.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este estimat.
7.05	Promovarea cooperării între universitățile din Moldova cu liderii mondiali în instruirea și certificarea în domeniul securității cibernetice, cum ar fi (ISC) 2, ISACA, SANS.	MEd.	MTIC, Universități le din Republica Moldova.	Permanent.	Numărul întunirilor realizate.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu

						este estimat.
7.06	Stabilirea și dezvoltarea relațiilor cu comunitatea internațională de cercetare în domeniile specifice ce stau la baza securității cibernetice.	MEd, AŞM.	MAEIE, MTIC, IDSI.	2016-2019	Numărul relațiilor stabilite.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este estimat.
7.07	Stabilirea și dezvoltarea relațiilor cu liderii mondiali în domeniul securității cibernetice pentru a crea un Centru de Excelență pentru Cercetare și Dezvoltare în Republica Moldova.	MEd.	MTIC, AŞM, IDSI.	2016-2018	Centru de excelență creat.	Bugetul instituțiilor, în limita alocațiilor aprobate. Resursele partenerilor de dezvoltare. Costul nu este estimat.

Anexa nr. 2  
la Programul național de securitate cibernetică  
a Republicii Moldova pentru anii 2016-2020

**Lista abrevierilor și acronimelor**

CS	– Cancelaria de Stat;
MEd	– Ministerul Educației;
MTIC	– Ministerul Tehnologiei Informației și Comunicațiilor;
AŞM	– Academia de Științe a Moldovei;
MAEIE	– Ministerul Afacerilor Externe și Integrării Europene;
MAI	– Ministerul Afacerilor Interne;
MA	– Ministerul Apărării;
SIS	– Serviciul de Informații și Securitate;
PG	– Procuratura Generală;
CTS	– Î.S. Centrul de Telecomunicații Speciale;
ANRCETI	– Agenția Națională de Reglementare în Comunicații Electronice și Tehnologia Informației;
CNPDCP	– Centrul Național pentru Protecția Datelor cu Caracter Personal;
INS	– Institutul Național de Standardizare;
MF	– Ministerul Finanțelor;
APC	– Autoritățile Publice Centrale;
APL	– Autoritățile Publice Locale;
BNM	– Banca Națională a Moldovei;
IFPS	– Inspectoratul Fiscal Principal de Stat;
INJ	– Institutul Național de Justiție;
UTM	– Universitatea Tehnică din Moldova;
USM	– Universitatea de Stat din Moldova;
CGE	– I.P. Centrul de Guvernare Electronică;
IDSI	– Institutul Dezvoltării Societății Informaționale;
OS	– Obiectiv specific;

Responsabil principal – instituția prima înscrisă în rubrica executorilor acțiunii din Planul de acțiuni.

**NOTĂ INFORMATIVĂ**  
la proiectul hotărîrii Guvernului cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020

Proiectul hotărîrii Guvernului cu privire la Programul național de securitate cibernetică a Republicii Moldova este elaborat de Ministerul Tehnologiei Informației și Comunicațiilor în comun cu autoritățile vizate, încrucișând prevederile Acordului de Asociere între Republica Moldova și Uniunea Europeană, Convenției Consiliului Europei privind criminalitatea informatică, Strategiei securității cibernetice a UE și Recomandărilor Uniunii Internaționale a Telecomunicațiilor referitoare la asigurarea securității cibernetice a rețelelor de comunicații electronice.

Proiectul de Hotărîre se bazează pe Strategia Națională de dezvoltare a societății informaționale "Moldova Digitală 2020", aprobată prin Hotărîrea Guvernului nr.857 din 31.10.2013 și pe Strategia securității naționale a Republicii Moldova, aprobată prin Hotărîrea Parlamentului nr.153 din 15.07.2011, inclusiv pe un cadru legal și funcțional. Totodată, acesta este rezultatul unor abordări sistémice și complexe a acțiunilor necesare pentru asigurarea securității cibernetice a Republicii Moldova, este construit pe cele mai bune practici internaționale și armonizat cu legislația europeană.

Programul național de securitate cibernetică a Republicii Moldova, anexă la proiectul de Hotărîre, include 7 domenii de intervenție:

- 1) procesarea sigură, stocarea și accesarea datelor;
- 2) securitatea și integritatea rețelelor și serviciilor de comunicații electronice;
- 3) capacitate de prevenire și reacție de urgență (CERT);
- 4) prevenirea și combaterea criminalității informaticе;
- 5) consolidarea capacitaților de apărare cibernetică;
- 6) educația și informarea;
- 7) cooperarea și interacțiunea internațională.

Desfășurarea acțiunilor din cadrul domeniilor de intervenție sunt orientate spre implementarea a patru componente-cheie de principiu:

- 1) cerințe minime obligatorii de securitate cibernetică, adoptarea unor standarde naționale de securitate cibernetică privind procesarea, stocarea, transmiterea, păstrarea și accesarea sigură a datelor clasificate corespunzător;
- 2) certificarea și autorizarea specialiștilor și sistemelor informaționale, conform standardelor aprobate;
- 3) efectuarea periodică a auditului de securitate cibernetică a sistemelor informaționale și rețelelor de comunicații electronice în cadrul autorităților publice și altor entități deținătoare de sisteme informaționale de importanță vitală pentru societate;
- 4) prescripții și sancțiuni personalizate, care sunt o consecință inherentă a nerespectării recomandărilor experților.

Totodată, la realizarea și implementarea Programului se vor respecta obligatoriu principiul neutralității tehnologice și principiile europene de securitate cibernetică:

- protecția drepturilor fundamentale, libertății de exprimare, datelor personale și confidențialității;
- accesul pentru toți la informații veridice și protejate;
- reziliența cibernetică a sistemelor;
- administrarea multiparticipativă și partajată a activităților de asigurare a securității cibernetice a sistemelor informaționale și rețelelor de comunicații electronice;
- responsabilitatea comună și personalizată de executare a activităților de asigurare a securității cibernetice.

Implementarea cu succes a proiectului Hotărîrii Guvernului propus spre aprobare, va avea drept rezultat formarea unui *Sistem național funcțional de management al securității cibernetice a Republicii Moldova*, care cu capacitați reale și legale, în strânsă cooperare între autoritățile publice, sectorul privat și organismele europene din domeniu, va permite în dinamică reducerea vulnerabilităților și riscurilor cibernetice, diminuarea pericolelor și atacurilor cibernetice pentru Republica Moldova. Astfel, Republica Moldova va dispune permanent de un spațiu cibernetic deschis, sigur și securizat.

Costul estimativ de implementare a Programului național de securitate cibernetică a Republicii Moldova se estimează la circa 76581 mii lei, inclusiv crearea rețelei CERT național – 49608 mii lei. Finanțarea se va efectua de la Bugetul de stat și resursele partenerilor de dezvoltare.

Proiectul Programului național de securitate cibernetică a Republicii Moldova este elaborat cu suportul experților din Estonia și Coreea de Sud.

Proiectul acestei Hotărîri se propune spre aprobare în contextul cînd pe parcursul ultimilor ani, incidentele cibernetice și criminalitatea informatică, indiferent de frontiere, capătă o frecvență, complexitate și o amploare din ce în ce mai mare, aducînd pagube enorme sectorului guvernamental, privat și cetățenilor.

**Ministru al tehnologiei  
informației și comunicațiilor**



**Pavel FILIP**