GUVERNUL REPUBLICII MOLDOVA

ПРАВИТЕЛЬСТВО РЕСПУБЛИКИ МОЛДОВА

H O T Ă R Î R E
cu privire la Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020

nr. 811 din 29.10.2015

Monitorul Oficial nr.306-310/905 din 13.11.2015

* * *

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 şi completările ulterioare, Guvernul

HOTĂRĂŞTE:

1. Se aprobă Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (se anexează).

2. Ministerele şi alte autorităţi administrative centrale vor prezenta Ministerului Tehnologiei Informaţiei şi Comunicaţiilor semestrial, pînă la data de 1 august şi 1 februarie, informaţia despre executarea Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, conform responsabilităţilor stabilite în acesta.

3. Ministerul Tehnologiei Informaţiei şi Comunicaţiilor va generaliza informaţia recepţionată şi va prezenta Guvernului semestrial, pînă la data de 1 septembrie şi 1 martie, raportul despre executarea Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020.

4. Monitorizarea şi coordonarea procesului de realizare a Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 se pun în sarcina Ministerului Tehnologiei Informaţiei şi Comunicaţiilor.

PRIM-MINISTRU INTERIMAR **Gheorghe BREGA**

Contrasemnează:
Ministrul tehnologiei informaţiei şi comunicaţiilor **Pavel Filip**
Ministrul afacerilor interne **Oleg Balan**
Ministrul apărării **Anatolie Şalaru**

Nr.811. Chişinău, 29 octombrie 2015.

Aprobat
prin Hotărîrea Guvernului
nr.811 din 29 octombrie 2015

PROGRAMUL NAŢIONAL
de securitate cibernetică a Republicii Moldova pentru anii 2016-2020

I. DISPOZIŢII GENERALE

1. Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 (în continuare – *Program*) are drept scop crearea unui sistem de management al securităţii cibernetice a Republicii Moldova prin securizarea serviciilor societăţi informaţionale,

contribuind astfel la dezvoltarea unei economii bazate pe cunoaştere, ceea ce, la rîndul său, va stimula creşterea gradului de competitivitate economică şi de coeziune socială, precum şi va asigura crearea de noi locuri noi de muncă.

2. Termenii utilizaţi în Program au următoarele semnificaţii:

1) *ameninţare cibernetică* – circumstanţă sau eveniment care constituie un pericol potenţial la adresa securităţii cibernetice;

2) *apărare cibernetică* – acţiuni desfăşurate în scopul protecţiei, monitorizării, analizării, detectării, contracarării agresiunilor şi asigurării răspunsului oportun la ameninţările asupra infrastructurilor cibernetice destinate apărării naţionale;

3) *atac cibernetic* – acţiune ostilă, desfăşurată în spaţiul cibernetic, de natură să afecteze securitatea cibernetică;

4) *audit de securitate cibernetică* – evaluare sistemică, detaliată, măsurabilă şi tehnică a modului în care politicile de securitate cibernetică sînt aplicate la nivelul infrastructurilor cibernetice, cu emiterea de recomandări pentru minimizarea riscurilor identificate;

5) *incident cibernetic* – eveniment survenit în spaţiul cibernetic ale cărui consecinţe afectează securitatea cibernetică;

6) *eveniment survenit în spaţiul cibernetic* – acţiune desfăşurată în spaţiul cibernetic care are drept consecinţă modificarea stării infrastructurilor cibernetice;

7) *infrastructuri cibernetice* – infrastructuri din domeniul tehnologiei informaţiei şi comunicaţiei, constînd din sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice;

8) *infrastructuri cibernetice de interes naţional* (ICIN) – infrastructuri cibernetice care susţin servicii publice sau de interes public, precum şi servicii ale societăţii informaţionale a căror afectare poate aduce atingere securităţii naţionale ori prejudicii grave statului sau cetăţenilor acestuia;

9) *management al identităţii* – metode de validare a identităţii persoanelor atunci cînd acestea accesează anumite infrastructuri cibernetice;

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

11) *operaţii în reţelele de calculatoare* – proces complex de planificare, coordonare, sincronizare, armonizare şi desfăşurare a acţiunilor în spaţiul cibernetic pentru protecţia, controlul şi utilizarea reţelelor de calculatoare, în scopul obţinerii superiorităţii informaţionale, concomitent cu neutralizarea capabilităţilor adversarului;

12) *rezilienţă a infrastructurilor cibernetice* – capacitate a componentelor infrastructurilor cibernetice de a rezista unui incident sau unui atac cibernetic şi de a reveni în starea de normalitate;

13) *risc de securitate în spaţiul cibernetic* – probabilitate ca o ameninţare să se materializeze, exploatînd o anumită vulnerabilitate specifică infrastructurilor cibernetice;

14) *securitate cibernetică* – stare de normalitate rezultată în urma aplicării unui ansamblu complex de măsuri proactive şi reactive prin care în spaţiul cibernetic se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a sistemelor şi resurselor informaţionale, a serviciilor publice şi private. Măsurile proactive şi reactive includ politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protecţie a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor;

15) *spaţiu cibernetic* – mediu virtual, generat de infrastructurile cibernetice, incluzînd conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acest mediu;

16) *vulnerabilitate în spaţiul cibernetic* – ineficacitate în proiectarea şi implementarea infrastructurilor cibernetice sau a măsurilor de securitate aferente, care poate fi exploatată de către o ameninţare.

Alţi termeni din Program sînt utilizaţi în sensul definit de Legea nr.20-XVI din 3 februarie 2009 privind prevenirea şi combaterea criminalităţii informatice, Legea comunicaţiilor electronice nr.241-XVI din 15 noiembrie 2007 şi Legea nr.467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat.

3. Conceptul securităţii cibernetice se bazează pe următoarele principii:

1) *protecţia drepturilor şi libertăţilor fundamentale ale omului.* Asigurarea securităţii cibernetice poate fi adecvată şi eficientă doar în cazul în care se bazează pe drepturile şi libertăţile fundamentale ale omului, inclusiv pe valorile general umane. Nici un proces de transfer, procesare sau stocare de date, inclusiv cu caracter personal, comercial şi confidenţial, nu poate fi asigurat fără utilizarea sistemelor informaţionale, a reţelelor şi serviciilor de comunicaţii electronice securizate. Orice tratare a informaţiilor efectuată în scopul asigurării securităţii cibernetice trebuie să fie conformă cadrului legal şi tratatelor la care Republica Moldova este parte;

2) *accesul pentru toţi.* Accesul sigur şi liber la internet şi la resursele acestuia este un drept al fiecărei persoane. Accesibilitatea limitată sau lipsa accesului, precum şi analfabetismul digital constituie dezavantaje atît pentru cetăţeni, cît şi pentru autorităţi;

3) *reziliența cibernetică.* Sesizarea preventivă sau anticipată a ameninţărilor şi atacurilor cibernetice, a altor evenimente survenite în spaţiul cibernetic este esenţială din cauza caracterului lor transfrontalier şi materializării asimetrice. Astfel, acestea urmează a fi depistate, pentru a elimina sau a diminua efectele care pot afecta starea de normalitate a securităţii cibernetice. Ameninţările cibernetice apar ca urmare a exploatării unor vulnerabilităţi. Mediul de ameninţări şi vulnerabilităţi este extrem de fluid şi dinamic: ameninţările pot apărea în decurs de zile sau chiar ore. Avînd în vedere acest mediu specific, responsabilii şi coordonatorii de securitate cibernetică trebuie să îl monitorizeze continuu, să depisteze ameninţările cibernetice şi să consulte permanent sursele recunoscute de informare ale companiilor-lider în domeniul securităţii cibernetice, experţii din mediul academic şi diverse publicaţii;

4) *administrare multiparticipativă.* Atît la nivel local sau naţional, cît şi la nivel regional sau global, spaţiul cibernetic nu poate fi ţinut sub control de o singură entitate. În spaţiul cibernetic nu pot fi fixate frontiere analogic frontierelor dintre unităţile administrativ-teritoriale sau dintre state. Astfel, pentru a asigura reziliența cibernetică, autorităţile publice şi sectorul privat trebuie să-şi dezvolte abilităţile necesare şi să coopereze în mod eficient între ele. Prin administrare multiparticipativă şi acţiuni comune, autorităţile publice şi sectorul privat pot să combată cu succes riscurile şi ameninţările cibernetice, pot contribui cu un răspuns coordonat şi eficient la evenimentele survenite în spaţiul cibernetic, care au dimensiuni naţionale şi transfrontaliere;

5) *responsabilitatea comună şi răspunderea personalizată pentru asigurarea securităţii cibernetice.* Dependenţa crescîndă a activităţilor umane de tehnologiile informaţiei şi comunicaţiei implică vulnerabilităţi care urmează a fi identificate, analizate minuţios şi eliminate sau diminuate, în funcţie de pericolul potenţial la adresa securităţii cibernetice. Toate părţile implicate în executarea activităţilor de asigurare a securităţii cibernetice, fie că sînt autorităţi publice, fie că aparţin sectorului privat sau sînt doar simpli cetăţeni, trebuie să recunoască această responsabilitate comună şi răspundere personalizată, să întreprindă acţiuni proprii şi comune de protecţie, să contribuie la consolidarea securităţii cibernetice şi apărării cibernetice în conformitate cu cadrul legal.

II. SITUAŢIA ACTUALĂ ŞI IDENTIFICAREA PROBLEMEI DE BAZĂ

4. Dezvoltarea accelerată a tehnologiilor informaţiei şi de comunicaţii moderne ridică la un alt nivel abordarea ameninţărilor, riscurilor şi vulnerabilităţilor într-o societate informaţională. În prezent, la nivel mondial, atacurile cibernetice capătă o frecvenţă, o complexitate şi o amploare

din ce în ce mai mari, aducînd pagube enorme sectorului guvernamental, celui privat şi cetăţenilor, ca urmare a caracterului lor asimetric. Accesarea neautorizată a reţelelor şi serviciilor de comunicaţii electronice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice, restricţionarea ilegală a accesului la aceste date şi spionajul cibernetic constituie constrîngeri la nivel global. Ameninţările şi riscurile, atacurile şi incidentele cibernetice, precum şi alte evenimente survenite în spaţiul cibernetic se materializează prin exploatarea vulnerabilităţilor de natură umană, tehnică şi procedurală. Prejudiciile economice provenite din exploatarea unor asemenea vulnerabilităţi sînt destul de semnificative.

5. Astfel, potrivit rapoartelor Norton[1] pentru anii 2012 şi 2013, costul global al criminalităţii cibernetice este în creştere. Pierderile globale au constituit în anul 2013 circa 113 miliarde dolari SUA faţă de 110 miliarde dolari SUA în 2012, iar pierderile în medie pe o victimă au fost de 298 dolari SUA în 2013 faţă de 197 dolari SUA în anul 2012. Potrivit datelor din aceleaşi rapoarte, sîntem supuşi în permanenţă unor riscuri majore la accesarea reţelelor wi-fi neprotejate. Este destul de mare riscul accesării neautorizate a poştei electronice personale (54% în anul 2013 faţă de 64% în anul 2012) ca urmare a interceptării parolei de accesare, precum şi riscul accesării neautorizate a paginilor personale ale utilizatorilor reţelelor sociale (56% în anul 2013 faţă de 63% în anul 2012). Este destul de ridicat şi riscul în comerţul electronic, efectuat prin magazine online, accesate prin intermediul reţelelor wi-fi neprotejate (29% în anul 2013 faţă de 31% în anul 2012). A crescut riscul accesării neautorizate a conturilor bancare în urma efectuării operaţiunilor prin intermediul reţelelor wi-fi neprotejate, care în anul 2013 a crescut la 29% faţă de 24% în anul 2012. Accesarea conturilor bancare prin intermediul reţelelor wi-fi neprotejate sporeşte considerabil riscul interceptării datelor de acces şi, prin urmare, al accesării neautorizate ulterioare a acestora în scopuri criminale.

[1] https://www.symantec.com

6. Din cauza ratei destul de ridicate a riscurilor de accesare sus-menţionate, precum şi a altor riscuri cibernetice specifice, în anul 2013 numărul victimelor care au suferit în urma unor fraude, atacuri şi incidente cibernetice a constituit circa 379 milioane, faţă de 558 milioane în anul 2012. Astfel, în anul 2013 au fost afectaţi 64% dintre proprietarii dispozitivelor mobile, 63% dintre utilizatorii reţelelor sociale, 68% dintre utilizatorii reţelelor wi-fi publice, 65% dintre părinţii copiilor şi 68% dintre pieţele emergente. În pofida numărului foarte mare de victime, doar o parte dintre utilizatorii internetului conştientizează că dispozitivele lor electronice (telefoane mobile, tablete, laptopuri, calculatoare etc.) pot fi supuse unor atacuri cibernetice la conectarea la internet, al căror impact poate fi diminuat semnificativ dacă se respectă cele mai simple recomandări de siguranţă. Acest fapt favorizează considerabil creşterea criminalităţii cibernetice (informatice) prin exploatarea vulnerabilităţilor de natură umană.

7. Pînă în prezent nu a fost efectuat nici un audit de securitate cibernetică, nu există studii sau rapoarte care ar reflecta în detalii situaţia privind criminalitatea informatică în Republica Moldova, ameninţările şi riscurile cibernetice, atacurile şi incidentele cibernetice, alte evenimente survenite în spaţiul cibernetic, numărul victimelor şi prejudiciile economice ale materializării acestora.

8. Unica sursă oficială de date statistice privind criminalitatea informatică este Registrul de evidenţă a infracţiunilor, a cauzelor penale, a persoanelor care au săvîrşit infracţiuni şi a materialelor cu privire la infracţiuni din cadrul Sistemului informaţional integral automatizat de evidenţă a infracţiunilor, a cauzelor penale şi a persoanelor care au săvîrşit infracţiuni. Potrivit informaţiei din Sistemul informaţional automatizat „Registrul informaţiei criminalistice şi criminologice", prezentate de Ministerul Afacerilor Interne, începînd cu anul 2013 şi pînă în august 2015 inclusiv au fost înregistrate 72 de infracţiuni informatice pe art.259-261[1] şi art.208[1] ale Codului penal al Republicii Moldova, cu un prejudiciu material estimat la circa 21588 mii lei. În particular, ca urmare a activităţilor Procuraturii Generale şi Inspectoratului General al Poliţiei, au fost înregistrate în anul 2013 – 23 de infracţiuni, cu un prejudiciu de circa 14139 mii lei, în anul 2014 – 24 de infracţiuni, cu un prejudiciu de circa 1323 mii lei, iar în primele 8 luni ale

anului 2015 – 25 de infracţiuni, cu un prejudiciu de circa 6126 mii lei. Concomitent, în aceeaşi perioadă de timp au fost înregistrate 57 de încălcări ale dreptului de autor şi drepturilor conexe, cu valoarea totală a amenzilor aplicate de circa 99 mii lei. Cu toate că datele din Registrul informaţiei criminalistice şi criminologice nu sînt încă complete şi nu reflectă toate clasele de infracţiuni şi contravenţii în sensul Convenţiei Consiliului Europei de la Budapesta privind criminalitatea informatică, se poate constata că numărul infracţiunilor şi contravenţiilor informatice este în creştere.

9. Totodată, conform datelor Centrului de Telecomunicaţii Speciale, numărul atacurilor cibernetice asupra serverelor web a crescut în anul 2014 faţă de anul 2013 cu circa 26%, iar vulnerabilităţile porturilor deschise au sporit cu circa 385%. Posibilităţile de infectare a calculatoarelor cu viruşi informatici au crescut cu circa 27%. Numărul incidentelor asupra poştei electronice guvernamentale s-a micşorat în 2014 faţă de 2013 cu circa 1%. Concomitent, s-a micşorat ponderea acestor incidente în totalul atacurilor cibernetice. În 2014 această pondere s-a diminuat la 40%, faţă de 51% în 2013.

10. Pericolul major de materializare a acestor evenimente survenite în spaţiul cibernetic, în care nu există frontiere, a impus ca pe agenda unui şir de ţări, începînd cu anul 2009, să fie inclusă ca subiect dominant problema securităţii cibernetice. Deja 56 de state din lume dispun de documente de politici[2] aprobate în domeniul securităţii cibernetice, inclusiv 21 de state ale Uniunii Europene. 37 de state din lume au aprobat documentele de politici pe parcursul anilor 2013-2015, inclusiv 14 state – în 2015.

---

[2] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world.

11. Cadrul legal intern al acestor ţări se ajustează corespunzător prevederilor Convenţiei Consiliului Europei privind criminalitatea informatică, adoptate la Budapesta la 23 noiembrie 2001, ţinîndu-se cont de Recomandările Uniunii Internaţionale a Telecomunicaţiilor referitoare la securitatea cibernetică.

12. Republica Moldova a ratificat Convenţia Consiliului Europei privind criminalitatea informatică prin Legea nr.6-XVI din 2 februarie 2009. Totodată, a fost adoptată Legea nr.20-XVI din 3 februarie 2009 privind prevenirea şi combaterea criminalităţii informatice, au fost operate modificări şi completări la Codul penal în corespundere cu prevederile Convenţiei ratificate, însă prevederile de ordin procedural ale acesteia, precum şi cele ce ţin de dezvoltarea punctului de contact al reţelei 24/7 nu au fost încă implementate.

13. În baza analizei efectuate a fost identificată problema de bază – lipsa unui sistem de management al securităţii cibernetice, în cadrul căruia să se efectueze coordonat planificarea şi utilizarea resurselor disponibile, identificarea vulnerabilităţilor şi riscurilor în urma auditului de securitate cibernetică, a intervenţiilor necesare pentru diminuarea impactului dăunător al criminalităţii, atacurilor şi incidentelor cibernetice asupra dezvoltării sigure a societăţii informaţionale. Acest sistem urmează să fie extins în toate sferele vieţii sociale, economice şi politice. Acesta trebuie să fie creat şi implementat de către entităţile vizate din domeniul public şi cel privat.

14. Lipsa unui sistem de management al securităţii cibernetice a Republicii Moldova generează şi lipsa datelor statistice complete, veritabile, actualizate şi structurate, ceea ce, la rîndul său, impune unele limitări în analiza efectuată şi identificarea de soluţii optime. De rezultatul soluţionării problemei de bază depinde eficienţa măsurilor întreprinse în vederea dezvoltării unei societăţii informaţionale securizate în Republica Moldova, avansării tehnologice şi ştiinţifice, participării active a cetăţenilor la viaţa socială şi culturală, precum şi dinamica de creştere economică a ţării.

15. Pînă în prezent nu există un cadru legal privind delimitarea şi armonizarea competenţelor şi responsabilităţilor instituţiilor statului şi celor private în domeniul securităţii cibernetice, nu se aplică mecanismul obligatoriu de audit al securităţii cibernetice în cadrul instituţiilor publice şi private, prin care pot fi identificate vulnerabilităţile, riscurile şi

ameninţările cibernetice în scopul prevenirii sau diminuării, prin măsuri speciale, a impactului atacurilor, incidentelor şi altor evenimente survenite în spaţiul cibernetic, a căror origine este dificil de stabilit.

16. În afara reglementărilor legislative, normative şi tehnico-normative, persistă o serie de probleme specifice ce ţin de asigurarea securităţii cibernetice a Republicii Moldova şi care sînt părţi componente ale problemei de bază identificate mai sus:

1) nu este asigurată siguranţa deplină la procesarea, stocarea şi accesarea datelor publice, indiferent de clasificarea acestora;

2) securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice nu sînt ajustate la standardele şi recomandările Uniunii Europene, Uniunii Internaţionale a Telecomunicaţiilor, la prevederile Acordului de Asociere între Republica Moldova şi Uniunea Europeană;

3) nu există capacităţi suficiente de prevenire şi reacţie urgentă la nivel naţional (CERT), ţinînd cont de caracterul asimetric al atacurilor şi incidentelor cibernetice;

4) cadrul legislativ-normativ naţional nu este armonizat integral la prevederile Convenţiei Consiliului Europei privind criminalitatea informatică, instituţiile vizate nu dispun de competenţe clare privind asigurarea securităţii cibernetice;

5) dispunem de capacităţi reduse de apărare cibernetică ca urmare a caracterului asimetric al atacurilor cibernetice;

6) nu sînt asigurate educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice;

7) există o insuficienţă a cooperării şi interacţiunii internaţionale privind identificarea riscurilor, vulnerabilităţilor, altor evenimente survenite în spaţiul cibernetic global şi prevenirea ameninţărilor şi atacurilor cibernetice transfrontaliere.

17. Soluţionarea problemei de bază, inclusiv a problemelor specifice, presupune intervenţii în cadrul legislativ şi instituţional, în cadrul normativ şi tehnico-normativ, în pregătirea continuă şi certificarea specialiştilor în domeniul securităţii cibernetice, auditului de securitate cibernetică a entităţilor care deţin infrastructuri cibernetice, sisteme informaţionale şi reţele de comunicaţii electronice, inclusiv a celor care prestează servicii informatice şi de comunicaţii electronice.

18. Totodată, soluţionarea problemelor identificate este în concordanţă cu obiectivul general orizontal privind asigurarea securităţii cibernetice stipulat în Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”, aprobată prin Hotărîrea Guvernului nr.857 din 31 octombrie 2013, cu prevederile Acordului de Asociere între Republica Moldova şi Uniunea Europeană, ratificat prin Legea nr.112 din 2 iulie 2014, precum şi cu noua viziune a Strategiei securităţii naţionale a Republicii Moldova.

III. OBIECTIVELE PROGRAMULUI

19. Obiectivul principal al Programului, stabilit în urma analizei efectuate şi identificării problemei de bază, este crearea şi implementarea unui sistem de management al securităţii cibernetice a Republicii Moldova care să asigure entităţilor vizate din domeniul public şi cel privat planificarea şi utilizarea resurselor disponibile, identificarea intervenţiilor necesare pentru diminuarea impactului dăunător al criminalităţii, atacurilor şi incidentelor cibernetice asupra dezvoltării sigure a societăţii informaţionale.

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 şi accesarea în siguranţă a datelor, inclusiv a datelor de interes public;

2) securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice;

3) dezvoltarea capacităţilor de prevenire şi reacţie urgentă la nivel naţional (reţeaua CERT naţională);

4) prevenirea şi combaterea criminalităţii informatice;

5) consolidarea capacităţilor de apărare cibernetică;
6) educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice;
7) cooperarea şi interacţiunea internaţională în sferele ce ţin de securitatea cibernetică.

IV. ACŢIUNILE CE URMEAZĂ A FI ÎNTREPRINSE PENTRU REALIZAREA OBIECTIVELOR

21. Pentru realizarea obiectivelor formulate în capitolul precedent au fost identificate, împreună cu autorităţile vizate, o serie de acţiuni ce urmează a fi executate, care – pentru comoditate şi în corespundere cu obiectivele specifice – au fost sistematizate într-un Plan de acţiuni privind implementarea Programului naţional de securitate cibernetică a Republicii Moldova (în continuare – *Plan de acţiuni*).

22. Conform Planului de acţiuni, anexă la prezentul Program, obiectivul specific „Procesarea, stocarea şi accesarea în siguranţă 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 informaţie, analiza şi elaborarea propunerilor de aplicare la nivel naţional a standardelor ce ţin de procesarea, stocarea şi accesarea în siguranţă a datelor, elaborarea unei metodologii pentru evaluarea vulnerabilităţilor sistemelor informaţionale în baza standardelor prestabilite, elaborarea cerinţelor minime obligatorii de securitate cibernetică, certificarea specialiştilor, efectuarea auditului de securitate cibernetică şi elaborarea planurilor de înlăturare a vulnerabilităţilor depistate, executarea altor măsuri, conform Planului de acţiuni.

23. Obiectivul specific „Securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice" va fi realizat prin armonizarea legislaţiei din domeniul comunicaţiilor electronice la directivele-cadru UE din domeniu, stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii şi integrităţii reţelelor şi serviciilor de comunicaţii electronice, raportarea incidentelor cu impact asupra acestor reţele şi servicii, aplicarea la nivel naţional a standardelor europene şi internaţionale ce ţin de protecţia şi securitatea reţelelor de comunicaţii electronice, executarea altor măsuri, conform Planului de acţiuni.

24. Obiectivul specific „Dezvoltarea capacităţilor de prevenire şi reacţie urgentă la nivel naţional (reţeaua CERT naţională)" va fi realizat prin crearea Centrului naţional de reacţie la incidentele de securitate cibernetică (CERT) şi a centrelor departamentale în autorităţile publice centrale, autorităţile publice locale, alte entităţi ce deţin sisteme informaţionale de stat, stabilirea obligaţiilor de raportare şi evidenţă operativă obligatorie a incidentelor de securitate cibernetică pentru autorităţile administraţiei publice centrale şi locale şi mediul de afaceri din domeniul tehnologiei informaţiei şi comunicaţiilor, elaborarea şi aplicarea unor metode de prevenire anticipată a incidentelor de securitate cibernetică în Republica Moldova, desfăşurarea unor exerciţii şi antrenamente de consolidare a capacităţilor de reacţie la incidentele şi atacurile cibernetice cu blocarea acestora, executarea altor măsuri, conform Planului de acţiuni.

25. Obiectivul specific „Prevenirea şi combaterea criminalităţii informatice" va fi realizat prin elaborarea proiectelor de legi pentru armonizarea continuă a legislaţiei penale, contravenţionale şi procesuale la prevederile Convenţiei europene privind criminalitatea informatică şi la deciziile Comitetului acestei Convenţii, ratificarea Protocolului adiţional la această Convenţie, ajustarea legislaţiei şi statisticii naţionale la prevederile Convenţiei Consiliului Europei pentru protecţia copiilor împotriva exploatării şi abuzurilor sexuale şi Protocolului adiţional la această Convenţie, consolidarea capacităţilor de prevenire şi combatere a criminalităţii informatice în cadrul Procuraturii Generale, Serviciului de Informaţii şi Securitate, Inspectoratului General al Poliţiei al Ministerului Afacerilor Interne, instruirea angajaţilor organelor de drept în domeniul securităţii cibernetice conform recomandărilor proiectului EAP al Consiliului Europei, executarea altor măsuri, conform Planului de acţiuni.

26. Obiectivul specific „Consolidarea capacităţilor de apărare cibernetică" va fi realizat prin stabilirea autorităţilor responsabile şi asigurarea cooperării dintre acestea pe timp de pace, în situaţii de criză, asediu şi război în cadrul spaţiului cibernetic, elaborarea compartimentului de

apărare cibernetică a Republicii Moldova ca parte componentă a Strategiei securităţii informaţionale a Republicii Moldova, instruirea în domeniul securităţii cibernetice a personalului din sfera securităţii şi apărării naţionale, dezvoltarea capabilităţilor militare de protecţie a infrastructurii şi serviciilor critice ce ţin de apărarea naţională, executarea altor măsuri, conform Planului de acţiuni.

27. Obiectivul specific „Educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice" va fi realizat prin crearea unui laborator de securitate cibernetică, completarea curriculumului de învăţământ cu studierea materiei din domeniul securităţii cibernetice, elaborarea şi implementarea conceptului campaniilor de informare şi conştientizare a riscurilor din spaţiul cibernetic, stabilirea cerinţelor de competenţă în domeniul securităţii cibernetice pentru personalul din sectorul public şi privat, evidenţa, instruirea, evaluarea şi certificarea acestui personal, organizarea şi efectuarea trainingurilor şi workshopurilor în domeniul securităţii cibernetice pentru personalul instituţiilor deţinătoare de elemente ale infrastructurii cibernetice critice, executarea altor măsuri, conform Planului de acţiuni.

28. Obiectivul specific „Cooperarea şi interacţiunea internaţională în sferele ce ţin de securitatea cibernetică" va fi realizat prin crearea unui Centru de excelenţă pentru cercetare şi dezvoltare în domeniul securităţii cibernetice, stabilirea şi dezvoltarea relaţiilor cu comunitatea internaţională de cercetare în domeniile specifice ce stau la baza securităţii cibernetice, dezvoltarea cooperării dintre sectorul public şi cel privat privind identificarea soluţiilor comune de securitate cibernetică, implementarea măsurilor de evaluare a ameninţărilor şi riscurilor faţă de vulnerabilităţile cibernetice identificate, încheierea acordurilor de cooperare internaţională cu echipele de tip CERT europene, nord-atlantice şi naţionale din alte ţări, executarea altor măsuri, conform Planului de acţiuni.

V. ETAPELE, TERMENELE ŞI RESPONSABILII DE IMPLEMENTARE

29. Programul nu prevede implementarea pe etape. Însă după fiecare an de implementare se va realiza evaluarea intermediară, în cadrul căreia se vor analiza şi se vor compara rezultatele intermediare cu cele scontate, se va stabili nivelul de implementare a Programului. Ca urmare a concluziilor din Informaţia de raportare a monitorizării şi evaluării (IRME), se vor propune, în caz de necesitate, ajustări ale obiectivelor şi/sau ale rezultatelor preconizate, acţiuni noi, actualizarea Programului şi/sau a Planului de acţiuni.

30. În Planul de acţiuni, anexat la Program, acţiunile sînt grupate conform obiectivelor specifice care trebuie realizate. În rubricile respective ale Planului de acţiuni sînt stabiliţi responsabilii de executarea acţiunilor, coexecutorii şi termenele de executare pentru obţinerea rezultatului scontat. Prima instituţie din lista responsabililor se consideră „responsabil principal" de executarea acţiunii, care dirijează activităţile coexecutorilor şi ale celorlalţi responsabili, atrage partenerii de dezvoltare pentru a obţine rezultatul scontat în termenul stabilit pentru acţiune.

VI. ESTIMAREA GENERALĂ A COSTURILOR ŞI REZULTATELE SCONTATE

31. La rubricile respective din Planul de acţiuni sînt indicate rezultatele scontate şi costurile estimative de realizare a fiecărei acţiuni aparte pentru obţinerea acestor rezultate. Sursele de finanţare includ contribuţia partenerilor de dezvoltare şi alocările bugetare.

32. Astfel, costurile estimative pentru obţinerea rezultatelor scontate, totalizate pe acţiunile din cadrul fiecărui obiectiv al Programului, sînt următoarele:

1) procesarea, stocarea şi accesarea în siguranţă a datelor, inclusiv a datelor de interes public – circa 9504 mii lei;

2) securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice – circa 1944 mii lei;

3) dezvoltarea capacităţilor de prevenire şi reacţie urgentă la nivel naţional (reţeaua CERT naţională) – circa 49608 mii lei;

4) prevenirea şi combaterea criminalităţii informatice – circa 2916 mii lei;

5) consolidarea capacităţilor de apărare cibernetică – circa 2232 mii lei;

6) educaţia, formarea şi informarea continuă în domeniul securităţii cibernetice – circa 10089 mii lei;

7) cooperarea şi interacţiunea internaţională în sferele ce ţin 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 securităţii cibernetice a Republicii Moldova, creat şi implementat în entităţile vizate din domeniul public şi cel privat, care va asigura planificarea şi utilizarea resurselor disponibile, identificarea intervenţiilor necesare pentru diminuarea impactului dăunător al criminalităţii, atacurilor şi incidentelor cibernetice asupra dezvoltării sigure a societăţii informaţionale. Acest sistem urmează a fi extins în toate sferele vieţii sociale, economice şi politice din ţară.

VII. INDICATORII DE PROGRES ŞI PERFORMANŢĂ

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

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

IR2 – ponderea rapoartelor (informaţiilor) de monitorizare şi evaluare realizate, calculată în % din numărul total al acestora prevăzute în Program;

IR3 – numărul acţiunilor din Planul de acţiuni realizate (înainte de, după şi în termenele prestabilite);

IR4 – numărul recomandărilor privind evitarea riscurilor şi diminuarea vulnerabilităţilor cibernetice;

IR5 – numărul prescripţiilor tehnice şi proiectelor standardelor de securitate cibernetică elaborate;

IR6 – numărul entităţilor care au beneficiat de instruirea angajaţilor în asigurarea securităţii cibernetice, numărul persoanelor care au beneficiat de această instruire;

IR7 – numărul entităţilor care au beneficiat de audit extern/intern de securitate cibernetică în scopul identificării la nivel de entitate a riscurilor şi vulnerabilităţilor cibernetice;

IR8 – ponderea autorităţilor administraţiei publice care aplică politici proprii de securitate cibernetică internă;

IR9 – ponderea autorităţilor administraţiei publice centrale care au creat propriul CERT departamental în reţeaua CERT naţională;

IR10 – numărul entităţilor participante în Sistemul de management al securităţii cibernetice a Republicii Moldova;

IR11 – numărul de cazuri penale şi contravenţionale ce ţin de criminalitatea informatică înregistrate în Sistemul informaţional automatizat „Registrul informaţiei criminalistice şi criminologice”, numărul persoanelor care au săvîrşit aceste infracţiuni şi/sau contravenţii, numărul victimelor, volumul prejudiciului adus victimelor şi volumul amenzilor aplicate;

IR12 – numărul cercetărilor şi studiilor efectuate în domeniul securităţii cibernetice;

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

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

IR15 – numărul recomandărilor practice de sensibilizare a populaţiei despre riscurile şi vulnerabilităţile cibernetice, asigurarea la domiciliu a securităţii cibernetice;

IR16 – numărul de campanii informative organizate de instituţiile vizate în domeniul securităţii cibernetice;

IR17 – numărul informaţiilor (rapoarte de monitorizare şi evaluare, note informative etc.) publicate pe pagina web oficială a Ministerului Tehnologiei Informaţiei şi Comunicaţiilor.

35. Pentru a stabili progresul şi performanţa implementării curente şi finale a Programului, indicatorii de rezultat periodic vor fi comparaţi cu indicatorii din Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”, cu rezultatele curente de realizare a Acordului de Asociere între Republica Moldova şi Uniunea Europeană, cu Recomandările Uniunii Internaţionale a Telecomunicaţiilor şi cu recomandările partenerilor de dezvoltare.

VIII. PROCEDURILE DE RAPORTARE ŞI EVALUARE

36. Procedurile de raportare şi evaluare sînt orientate spre maximizarea efectelor obţinute de la implementarea Programului în corespundere cu rezultatele scontate indicate la rubrica „Indicatori de rezultat” din Planul de acţiuni.

37. Procesul de implementare a Programului este însoţit de monitorizarea permanentă la nivel instituţional, naţional şi internaţional a realizării acţiunilor propuse şi a rezultatelor real obţinute pentru ca, în caz de necesitate, să fie operate modificările respective în politicile publice promovate şi acţiunile întreprinse, precum şi de corelarea obiectivelor şi a acţiunilor din Planul de acţiuni cu rezultatele aşteptate de la implementarea Programului, în scopul efectuării unei evaluări cît mai corecte a modului de implementare a Programului.

38. În cadrul procesului de monitorizare se elaborează Informaţia de raportare a monitorizării şi evaluării, care include date relevante privind rezultatele realizării obiectivelor Programului şi executării acţiunilor respective din Planul de acţiuni, corelate cu rezultatele implementării Strategiei naţionale de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”. La această informaţie se anexează rapoarte de progres, rapoarte de evaluare şi/sau note informative, cu concluzii şi propuneri. În particular, procesul de monitorizare şi evaluare este orientat să contribuie la analiza situaţiei curente şi a tendinţelor în realizarea obiectivelor Programului, la analiza realizării Planului de acţiuni şi la evaluarea corectă a rezultatelor curente şi finale obţinute faţă de rezultatele scontate.

39. La nivelul organismelor internaţionale donatoare (partenerilor de dezvoltare), care finanţează anumite etape, părţi componente sau seturi de activităţi din cadrul Programului, raportarea şi monitorizarea se va conforma cerinţelor acestora. Rapoartele periodice de progres, notele informative şi rapoartele de evaluare vor fi elaborate în formatul agreat de respectiva instituţie financiară donatoare şi Guvern.

40. La nivel naţional, procedurile de raportare şi evaluare se efectuează de Ministerul Tehnologiei Informaţiei şi Comunicaţiilor în baza Informaţiei de raportare a monitorizării şi evaluării prezentate semestrial de responsabilii principali de executarea acţiunilor din Planul de acţiuni. Pentru fiecare an de implementare, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, în colaborare cu responsabilii principali specificaţi în Planul de acţiuni şi alte instituţii interesate, elaborează Raportul anual de evaluare a implementării Programului, care se prezintă Guvernului şi Consiliul intersectorial de securitate cibernetică pînă la data de 1 martie a anului următor. În funcţie de caz, Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, în baza rezultatelor evaluării intermediare sau semestriale, va înainta spre examinare şi aprobare proiecte de hotărîri ale Guvernului privind actualizarea Programului şi/sau a Planului de acţiuni.

41. La nivel instituţional, procedurile de raportare şi evaluare se efectuează semestrial de instituţiile responsabile de acţiunile din Planul de acţiuni. Principala instituţie responsabilă de executarea acţiunii întocmeşte Informaţia de raportare a monitorizării şi evaluării privind realizarea acţiunii de care este responsabilă şi prezintă această informaţie Ministerului Tehnologiei Informaţiei şi Comunicaţiilor pînă la data de 1 august şi 1 februarie a semestrului următor. În caz de necesitate, principala instituţie responsabilă de executarea acţiunii instituie un grup de lucru din reprezentanţii instituţiilor responsabile şi coexecutoare a acţiuni, partenerilor de dezvoltare, altor instituţii de profil, în scopul organizării şi executării eficiente a acţiunii în cauză, conform unui plan de lucru aprobat. Faptul instituirii grupului de lucru şi aprobării planului de lucru privind executarea acţiunii se va reflecta în Informaţia de raportare a monitorizării şi evaluării.

42. Evaluarea se efectuează prin compararea rezultatelor real obţinute faţă de cele scontate pentru perioada respectivă de raportare. După caz, evaluarea poate fi efectuată prin cercetări şi studii, în colaborare cu instituţiile interesate specificate în Planul de acţiuni.

43. După fiecare an de implementare a Programului se efectuează evaluarea intermediară, iar la sfîrşitul implementării acestuia – evaluarea finală. În cadrul evaluării intermediare se analizează rezultatele intermediare în comparaţie cele scontate. Ca urmare a concluziilor şi propunerilor din Raportul de evaluare a implementării Programului, în caz de necesitate, se propun ajustări ale obiectivelor şi/sau ale rezultatelor preconizate, acţiuni noi, actualizarea Programului şi/sau a Planului de acţiuni.

44. La sfîrşitul anului 2020 va fi elaborat Raportul de evaluare finală a implementării Programului, în care se va reflecta realizarea obiectivelor Programului, executarea acţiunilor prevăzute în Planul de acţiuni, inclusiv impactul implementării Programului asupra securităţii cibernetice a Republicii Moldova. Raportul final va include concluzii şi propuneri privind dezvoltarea şi extinderea rezultatelor implementării în alte sfere ale vieţii sociale, economice şi politice din ţară.

45. Ministerul Tehnologiei Informaţiei şi Comunicaţiilor informează publicul despre implementarea Programului prin plasarea pe site-ul său oficial a comunicatelor de presă privind activităţile de implementare a Programului, privind rezultatele semestriale, anuale şi finale obţinute la implementarea acestuia, precum şi prin oferirea informaţiilor relevante partenerilor din ţară şi de peste hotare.

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

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

2) să se angajeze într-un dialog social cu Guvernul, în special cu Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, cu alte organe administrative centrale şi să ofere soluţii noi de sporire a eficienţei implementării Programului.

Anexă
la Programul naţional de securitate
cibernetică a Republicii Moldova
pentru anii 2016-2020

PLANUL DE ACŢIUNI
privind implementarea Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020

Nr. d/o.	Acţiuni	Instituţii responsabile	Parteneri	Termene şi/sau perioade de executare	Indicatori de rezultat	Surse de finanţare, costuri estimative, lei
1	**2**	**3**	**4**	**5**	**6**	**7**
1.	**Procesarea, stocarea şi accesarea în siguranţă a datelor, inclusiv a datelor de interes public**. Costul estimativ – 9504 mii lei					
1.1.	Asigurarea ajustării cadrului normativ-legislativ privind securitatea cibernetică a Republicii Moldova, care va prevedea: a) definirea termenilor	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Serviciul de Informaţii şi Securitate	Cancelaria de Stat; Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală; Agenţia Naţională de	2016-2017	Proiect de act legislativ elaborat şi remis spre examinare Guvernului	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor

	(noţiunilor) din domeniul securităţii cibernetice; b) delimitarea pe domenii a competenţelor; c) stabilirea organului cu funcţii de monitorizare a respectării cerinţelor de securitate cibernetică; d) desemnarea organului responsabil de controlul implementării rezultatelor auditului de securitate cibernetică; e) obligaţiile deţinătorilor sistemelor informaţionale de stat privind efectuarea periodică a auditului acestor sisteme, cu stabilirea periodicităţii, nivelelor, obligaţiilor de prezentare a raportului către organul competent; f) sancţiuni pentru nerespectarea deciziei auditului privind conformitatea cu cerinţele minime obligatorii de securitate cibernetică; g) responsabilitatea personală pentru asigurarea securităţii cibernetice; h) introducerea în autorităţile publice a funcţiei de coordonator de securitate cibernetică, inclusiv atribuţiile principale ale acestuia; i) formarea Consiliului intersectorial de securitate cibernetică (cu funcţie de coordonare a activităţilor de securitate cibernetică)		Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal			de dezvoltare. Costul estimativ – 2592 mii
1.2.	Clasificarea tipurilor de informaţie, cu excepţia secretului de	Ministerul Tehnologiei Informaţiei şi	Serviciul de Informaţii şi Securitate;	2016	Clasificare aprobată	Bugetul instituţiilor, în limitele

	stat	Comunicaţiilor	Ministerul Afacerilor Interne; Procuratura Generală; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal; Centrul de Telecomunicaţii Speciale			alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
1.3.	Analiza şi elaborarea propunerilor de aplicare la nivel naţional a standardelor ce ţin de procesarea, stocarea şi accesarea sigură a datelor conform clasificării tipurilor de informaţie, examinate în cadrul comitetelor tehnice de standardizare CT 28 „Tehnologia informaţiei” şi CT 29 „Comunicaţii electronice”	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Agenţia Naţională de Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei	Institutul Naţional de Standardizare; Centrul de Telecomunicaţii Speciale; Ministerul Afacerilor Interne; Ministerul Apărării; Serviciul de Informaţii şi Securitate; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal; comitetele tehnice de standardizare CT 28 „Tehnologia informaţiei” şi CT 29 „Comunicaţii electronice”	2016-2017	Propuneri de aplicare a standardelor europene şi internaţionale ce ţin de procesarea, stocarea şi accesarea în siguranţă a datelor	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 216 mii
1.4.	Elaborarea unei metodologii pentru evaluarea vulnerabilităţilor sistemelor informaţionale de stat în baza standardelor identificate, transpuse şi aprobate	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Serviciul de Informaţii şi Securitate; Agenţia Naţională de Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei	Institutul Naţional de Standardizare; Cancelaria de Stat; Ministerul Afacerilor Interne; Ministerul Apărării; comitetele tehnice de standardizare CT 28 „Tehnologia informaţiei” şi CT 29 „Comunicaţii electronice”	2016-2017	Metodologie elaborată şi aprobată prin hotărîre de Guvern	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
1.5.	Elaborarea cerinţelor minime obligatorii de securitate cibernetică	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Ministerul Apărării; Ministerul Afacerilor Interne; Agenţia Naţională de Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei; Serviciul de Informaţii şi Securitate; Centrul de Telecomunicaţii Speciale; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	2016-2017	Cerinţe minime obligatorii de securitate cibernetică aprobate de Guvern	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
1.6.	Certificarea specialiştilor reieşind din standardele şi	Ministerul Tehnologiei Informaţiei şi	Cancelaria de Stat; Serviciul de Informaţii şi	2016-2018	Număr de autorităţi ale administraţiei	Bugetul instituţiilor, în limitele

	metodologia identificate şi cerinţele minime obligatorii de securitate cibernetică aprobate	Comunicaţiilor	Securitate; Procuratura Generală; Ministerul Afacerilor Interne; Ministerul Apărării		publice centrale şi locale, alte entităţi deţinătoare de sisteme informaţionale de stat pentru care au fost certificaţi specialişti; număr de specialişti certificaţi	alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 864 mii
1.7.	Identificarea şi planificarea în bugetele instituţiilor a mijloacelor financiare necesare pentru efectuarea auditului securităţii cibernetice în baza metodologiei aprobate	Ministerul Finanţelor; autorităţile administraţiei publice centrale şi locale, deţinătorii sistemelor informaţionale de stat	Cancelaria de Stat; Ministerul Afacerilor Interne; Procuratura Generală; Ministerul Apărării; Serviciul de Informaţii şi Securitate	2016	Mijloace financiare alocate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ nu este identificat
1.8.	Efectuarea unui audit în autorităţile administraţiei publice centrale şi locale, în alte entităţi deţinătoare de sisteme informaţionale de stat, cu scopul identificării vulnerabilităţilor şi corespunderii la cerinţele minime obligatorii de securitate cibernetică	Autorităţile administraţiei publice centrale şi locale, deţinătorii sistemelor informaţionale de stat	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	2017-2020	Număr de entităţi în care a fost efectuat auditul	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 864 mii
1.9.	Elaborarea planului de înlăturare a vulnerabilităţilor conform recomandărilor auditului şi executarea acestuia prin responsabilitate personalizată în cadrul autorităţilor administraţiei publice centrale şi locale, altor entităţi deţinătoare de sisteme informaţionale de stat	Autorităţile administraţiei publice centrale şi locale, deţinătorii sistemelor informaţionale de stat	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	2016-2018	Număr de entităţi care au raportat despre realizarea planului de înlăturare a vulnerabilităţilor	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 1296 mii
1.10.	Elaborarea şi implementarea metodologiei de marcare a informaţiei furnizate prin sistemul care conţine date cu caracter personal cu utilizarea „mărcii temporale”	Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Centrul de Telecomunicaţii	2016-2019	Metodologie elaborată şi implementată	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ –

			Speciale			216 mii
2.11.	Elaborarea şi implementarea actelor legislative necesare pentru introducerea măsurilor de securitate şi standardelor obligatorii în companiile din domeniul tehnologiei informaţiei şi comunicaţiilor, cu stabilirea unor cerinţe minime de securitate a sistemelor informaţionale de stat şi a informaţiilor din aceste sisteme	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Agenţia Naţională de Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei	Cancelaria de Stat; Ministerul Apărării; Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne	2017	Acte legislative elaborate şi remise spre examinare Guvernului	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
2.	**Securitatea şi integritatea reţelelor şi serviciilor de comunicaţii electronice**. Costul estimativ – 1944 mii lei					
2.1.	Armonizarea legislaţiei din domeniul comunicaţiilor electronice la directivele-cadru UE din domeniu	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Agenţia Naţională de Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Ministerul Apărării; Centrul de Telecomunicaţii Speciale; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	2016	Proiect de lege elaborat şi remis spre examinare Guvernului	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 216 mii
2.2.	Stabilirea măsurilor minime de securitate ce trebuie luate de către furnizori pentru asigurarea securităţii, non-repudierii şi integrităţii reţelelor şi/sau serviciilor de comunicaţii electronice şi raportarea incidentelor cu impact semnificativ asupra acestora	Agenţia Naţională de Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	2016-2017	Proiect de act normativ aprobat prin Decizia consiliului de administrare al Agenţiei Naţionale de Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
2.3.	Analiza şi transpunerea la nivel naţional a standardelor europene şi internaţionale ce ţin de protecţia şi securitatea reţelelor de comunicaţii electronice şi înaintarea spre adoptare către Institutul Naţional de Standardizare	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Institutul Naţional de Standardizare; Comitetul tehnic de standardizare CT 29 „Comunicaţii electronice”	2016-2017	Standarde adoptate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
2.4.	Efectuarea unui studiu cu privire la modificarea legislaţiei	Serviciul de Informaţii şi Securitate	Ministerul Tehnologiei Informaţiei şi	2016-2017	Studiu elaborat	Bugetul instituţiilor, în limitele

	în domeniul comunicaţiilor electronice în vederea eliminării sau diminuării numărului abonaţilor serviciilor de comunicaţii electronice depersonalizaţi		Comunicaţiilor; Procuratura Generală; Ministerul Afacerilor Interne; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal			alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
2.5.	Dezvoltarea în continuare a reţelei de comunicaţii speciale a autorităţilor administraţiei publice pe întreg teritoriul Republicii Moldova	Cancelaria de Stat; Serviciul de Informaţii şi Securitate; Centrul de Telecomunicaţii Speciale	Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Conform planului aprobat de Guvern	Număr de oraşe cuprinse de reţeaua de telecomunicaţii speciale	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
3.	**Crearea centrului de reacţie la incidente cibernetice la nivel naţional (reţeaua CERT naţională)**. Costul estimativ – 49608 mii lei					
3.1.	Crearea Centrului naţional de reacţie la incidentele de securitate cibernetică (CERT)	Cancelaria de Stat; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate	Procuratura Generală; Centrul de Telecomunicaţii Speciale; Ministerul Apărării	2016	Centru naţional creat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 29700 mii
3.2.	Crearea unui sistem naţional de alerte şi informare în timp real despre incidentele de securitate cibernetică	Cancelaria de Stat; Centrul de Telecomunicaţii Speciale	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală	2016-2017	Sistem funcţional creat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 594 mii
3.3.	Crearea centrelor de reacţie la incidentele de securitate cibernetică departamentale în autorităţile administraţiei publice centrale şi locale, în alte entităţi deţinătoare de sisteme informaţionale de stat	Autorităţile administraţiei publice centrale şi locale, deţinătorii sistemelor informaţionale de stat		2016-2017	Număr de centre departamentale create	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 14850 mii
3.4.	Stabilirea obligaţiilor pentru autorităţile	Cancelaria de Stat	Serviciul de Informaţii şi	2016-2017	Obligaţii aprobate	Bugetul instituţiilor,

	administraţiei publice centrale şi locale şi mediul de afaceri din domeniul tehnologiei informaţiei şi comunicaţiilor privind raportarea operativă obligatorie a incidentelor de securitate cibernetică în baza unui mecanism de schimb de date şi rolurile bine definite		Securitate; Ministerul Afacerilor Interne; Ministerul Apărării; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Procuratura Generală; Centrul de Telecomunicaţii Speciale; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal			în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
3.5.	Organizarea unei baze de date cu acces al autorităţilor responsabile privind ameninţările, vulnerabilităţile şi incidentele de securitate cibernetică identificate sau raportate, tehnicile şi tehnologiile folosite pentru atacuri, bunele practici pentru protecţia domeniului tehnologiei informaţiei şi comunicaţiilor	Cancelaria de Stat	Procuratura Generală; Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate; Ministerul Apărării; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Centrul de Telecomunicaţii Speciale; Banca Naţională a Moldovei; Inspectoratul Fiscal Principal de Stat; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	Permanent	Sistem creat în conformitate cu concepţia aprobată	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 1800 mii
3.6.	Desfăşurarea exerciţiilor şi antrenamentelor comune de consolidare a capacităţilor de reacţie la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate	Cancelaria de Stat; Serviciul de Informaţii şi Securitate; Centrul de Telecomunicaţii Speciale	Ministerul Apărării; Ministerul Afacerilor Interne; Procuratura Generală; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Permanent	Număr de exerciţii organizate; număr de antrenamente efectuate; capacitate ridicată a reacţiei la ameninţările cibernetice	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 900 mii
3.7.	Consolidarea capacităţilor echipei Centrului naţional de reacţie la incidentele de securitate cibernetică pentru a asigura analiza strategică a incidentelor de securitate şi coordonarea acţiunilor de răspuns la	Cancelaria de Stat; Centrul de Telecomunicaţii Speciale	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală	2016-2018	Capacităţi îmbunătăţite	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 900 mii

	incidente de securitate în sectorul public, privat şi academic, inclusiv prin organizarea trainingurilor de către experţi calificaţi					
3.8.	Elaborarea mecanismelor (modelelor) de prevenire timpurie a incidentelor de securitate cibernetică în Republica Moldova, inclusiv în baza parteneriatelor public-private	Cancelaria de Stat; Centrul de Telecomunicaţii Speciale	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Ministerul Apărării	2016-2018	Metode (modele) de prevenire timpurie a incidentelor de securitate cibernetice	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
4.	**Prevenirea şi combaterea criminalităţii informatice.** Costul estimativ – 2916 mii lei					
4.1.	Elaborarea proiectului de lege privind modificarea şi completarea legislaţiei penale şi contravenţionale pentru prevenirea şi combaterea crimelor informatice în scopul armonizării continue a acesteia la prevederile Convenţiei Europene privind criminalitatea informatică şi la deciziile Comitetului acestei Convenţii	Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate; Procuratura Generală	Ministerul Apărării; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	2016	Proiect de lege privind modificarea şi completarea Codului penal, Codului de procedură penală şi Codului contravenţional elaborat şi remis spre examinare Guvernului	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul nu este estimat
4.2.	Instruirea angajaţilor organelor de drept, specialiştilor certificaţi în domeniul securităţii cibernetice privind: a) depistarea, investigarea, urmărirea penală şi judecarea infracţiunilor informatice; b) legătura dintre criminalitatea informatică, crima organizată, infracţiunile economice şi alte categorii de infracţiuni	Institutul Naţional de Justiţie	Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate; Procuratura Generală	2016-2020	Număr de instruiri efectuate; număr de persoane instruite	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 900 mii
4.3.	Implementarea recomandărilor Consiliului Europei, în special ale proiectului EAP privind instruirea personalului organelor	Institutul Naţional de Justiţie; Academia „Ştefan cel Mare” a Ministerului Afacerilor Interne	Procuratura Generală; Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate;	2016	Curriculum elaborat şi implementat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor

	de drept		Universitatea Tehnică a Moldovei; Universitatea de Stat din Moldova			de dezvoltare. Costul estimativ – 900 mii
4.4.	Elaborarea şi aprobarea proiectului de lege privind ratificarea protocolului adiţional la Convenţia Consiliului Europei privind criminalitatea informatică	Ministerul Afacerilor Interne	Cancelaria de Stat; Serviciul de Informaţii şi Securitate; Procuratura Generală; Ministerul Afacerilor Externe şi Integrării Europene	2016	Proiect de lege elaborat şi remis spre examinare Guvernului	Bugetul instituţiilor, în limitele alocaţiilor aprobate. Costul nu este estimat
4.5	Ajustarea legislaţiei naţionale la prevederile Convenţiei Consiliului Europei pentru protecţia copiilor împotriva exploatării şi abuzurilor sexuale şi a Protocolului adiţional la Convenţie (Lanzarote, 25 octombrie 2007)	Ministerul Afacerilor Interne	Procuratura Generală	2016-2017	Proiect de lege elaborat şi transmis spre examinare Guvernului	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul nu este estimat
4.6.	Efectuarea unui studiu pentru perfecţionarea cadrului normativ în domeniul prevenirii şi combaterii crimelor informatice	Procuratura Generală; Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate	Cancelaria de Stat; Ministerul Justiţiei; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Centrul de Telecomunicaţii Speciale; Ministerul Apărării	2016	Proiect de modificare a cadrului normativ elaborat şi remis spre examinare Guvernului	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 216 mii
4.7.	Consolidarea în cadrul Procuraturii Generale, Serviciului de Informaţii şi Securitate şi Inspectoratului General al Poliţiei al Ministerului Afacerilor Interne a capacităţilor pentru prevenirea şi combaterea criminalităţii informatice şi, după caz, formularea unor propuneri de modificare a cadrului normativ şi crearea unui laborator de testare şi expertiză	Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate; Procuratura Generală		2016-2019	Capacităţi instituţionale dezvoltate cu formularea, după caz, a unor propuneri de modificare a cadrului normativ	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 900 mii
5.	**Consolidarea capacităţilor de apărare cibernetică**. Costul estimativ – 2232 mii lei					
5.1.	Elaborarea	Serviciul de	Procuratura	2016	Compartiment	Bugetul

	compartimentului de apărare cibernetică a Republicii Moldova, ca parte componentă a Strategiei securităţii informaţionale a Republicii Moldova	Informaţii şi Securitate; Ministerul Apărării; Ministerul Afacerilor Interne	Generală		elaborat şi prezentat pentru a fi inclus în Strategia securităţii informaţionale a Republicii Moldova	instituţiilor, în limitele alocaţiilor aprobat; resursele partenerilor de dezvoltare. Costul nu este estimat
5.2.	Stabilirea autorităţilor responsabile şi cooperarea reciprocă pe timp de pace, în situaţii de criză, asediu şi război în cadrul spaţiului cibernetic	Serviciul de Informaţii şi Securitate; Ministerul Apărării; Ministerul Afacerilor Interne	Cancelaria de Stat; Centrul de Telecomunicaţii Speciale; Ministerul Educaţiei; Ministerul Finanţelor; Ministerul Economiei; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Procuratura Generală	2016-2017	Proiect de act legislativ aprobat şi prezentat Parlamentului spre adoptare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
5.3.	Valorificarea oportunităţilor spaţiului cibernetic pentru promovarea intereselor, valorilor şi obiectivelor naţionale în spaţiul cibernetic	Serviciul de Informaţii şi Securitate; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală, Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	2016-2018	Politici elaborate şi aprobate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul nu este estimat
5.4.	Dezvoltarea capabilităţilor militare de protecţie a infrastructurii şi serviciilor critice destinate apărării naţionale	Ministerul Apărării	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	2016-2017	Capabilităţi dezvoltate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 900 mii
5.5.	Stabilirea programelor de conştientizare şi educare a personalului destinat securităţii şi apărării naţionale în domeniul securităţii cibernetice	Serviciul de Informaţii şi Securitate; Ministerul Apărării	Ministerul Afacerilor Interne; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Ministerul Educaţiei	2016-2017	Personal instruit	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 900 mii
5.6.	Stabilirea relaţiilor de cooperare cu	Serviciul de Informaţii şi	Ministerul Afacerilor Interne;	2016-2018	Proceduri de cooperare stabilite	Bugetul instituţiilor,

	instituţiile naţionale şi cele internaţionale din domeniu	Securitate; Ministerul Apărării	Ministerul Afacerilor Externe şi Integrării Europene; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor			în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul nu este estimat
6.	**Educarea şi informarea continuă în domeniul securităţii cibernetice**. Costul estimativ – 10089 mii lei					
6.1.	Elaborarea conceptului campaniilor de informare şi conştientizare despre riscurile spaţiului cibernetic	Cancelaria de Stat; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Ministerul Afacerilor Interne; Procuratura Generală; Serviciul de Informaţii şi Securitate; Centrul de Telecomunicaţii Speciale; Centrul de Guvernare Electronică; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	2016-2017	Concept al campaniilor de informare aprobat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 900 mii
6.2.	Completarea curriculumului de învăţământ în domeniul securităţii cibernetice	Ministerul Educaţiei	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Centrul de Guvernare Electronică; Universitatea Tehnică a Moldovei; Universitatea de Stat din Moldova; Centrul Naţional pentru Protecţia Datelor cu Caracter Personal	2016-2018	Curriculum aprobat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 432 mii
6.3.	Crearea unui portal cu anunţarea operativă a pericolelor din spaţiul cibernetic (digital)	Cancelaria de Stat; Centrul de Telecomunicaţii Speciale	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	2016-2018	Portal funcţional creat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 900 mii
6.4.	Stabilirea cerinţelor de competenţă în domeniul securităţii cibernetice pentru personalul din sectorul public şi privat, precum şi organizarea procesului de instruire, evaluare şi certificare a specialiştilor pentru	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Procuratura Generală; Centrul de Telecomunicaţii Speciale; Ministerul Apărării	2016-2018	Număr de specialişti certificaţi	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ –

	acest domeniu					432 mii
6.5.	Organizarea şi efectuarea trainingurilor şi workshopurilor în domeniul securităţii cibernetice pentru personalul din sectorul public şi privat, deţinătorii de elemente de infrastructură critică	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Centrul de Telecomunicaţii Speciale	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Procuratura Generală; Ministerul Apărării; Centrul de Guvernare Electronică; Universitatea Tehnică a Moldovei; Universitatea de Stat din Moldova	Permanent	Număr de traininguri şi workshopuri efectuate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul nu este estimat
6.6.	Crearea unui laborator de securitate cibernetică	Centrul de Telecomunicaţii Speciale; Universitatea Tehnică a Moldovei	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Ministerul Apărării	2016-2018	Laborator creat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 7425 mii
7.	**Cooperarea şi interacţiunea internaţională în domeniul securităţii cibernetice**. Costul estimativ – 648 mii lei					
7.1.	Încheierea acordurilor de cooperare cu alte echipe naţionale de răspuns la incidentele legate de securitatea cibernetică (CERT), precum şi US –CERT, europene şi nord-atlantice (NATO NCERT)	Cancelaria de Stat; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Ministerul Apărării	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Procuratura Generală	2016-2018	Număr de acorduri încheiate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul nu este estimat
7.2.	Elaborarea unei platforme de coordonare şi consultare în ceea ce priveşte evaluarea ameninţărilor cibernetice şi identificarea soluţiilor	Cancelaria de Stat; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Serviciul de Informaţii şi Securitate; Ministerul Afacerilor Interne; Ministerul Apărării; Procuratura Generală; Centrul de Telecomunicaţii Speciale	2016-2018	Platformă de coordonare şi consultare elaborată şi aprobată	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul estimativ – 648 mii
7.3.	Dezvoltarea cooperării cu sectorul privat (identificarea unor aplicaţii necesare implementării măsurilor de securitate; înfiinţarea	Cancelaria de Stat; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor	Ministerul Afacerilor Interne; Serviciul de Informaţii şi Securitate; Agenţia Naţională de Reglementare în	2016-2019	Număr de aplicaţii identificate; număr de puncte de contact; sistem modern de transmitere a solicitărilor;	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor

	de puncte de contact în vederea asigurării solicitării unor date şi informaţii conform prevederilor legale şi stabilirea unui sistem modern de transmitere a solicitărilor; realizarea de întruniri periodice în cadrul unor forumuri de dezbateri pentru cunoaşterea mai bună a situaţiei operative şi pentru înţelegerea nevoilor fiecărei instituţii)		Comunicaţii Electronice şi Tehnologia Informaţiei; Procuratura Generală		număr de întruniri realizate	de dezvoltare. Costul nu este estimat
7.4.	Promovarea intereselor naţionale de securitate cibernetică în formatele internaţionale de cooperare la care participă Republica Moldova	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Ministerul Afacerilor Interne; Ministerul Apărării; Serviciul de Informaţii şi Securitate; Procuratura Generală	Ministerul Afacerilor Externe şi Integrării Europene; Cancelaria de Stat; Centrul de Telecomunicaţii Speciale; Centrul de Guvernare Electronică	Permanent	Interese naţionale promovate în formate internaţionale de cooperare	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul nu este estimat
7.5.	Promovarea cooperării dintre universităţile din Moldova şi liderii mondiali în instruirea şi certificarea în domeniul securităţii cibernetice, cum ar fi (ISC) 2, ISACA, SANS	Ministerul Educaţiei	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; universităţile din Republica Moldova	Permanent	Număr de întruniri realizate	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de dezvoltare. Costul nu este estimat
7.6.	Stabilirea şi dezvoltarea relaţiilor cu comunitatea internaţională de cercetare în domeniile specifice care stau la baza securităţii cibernetice	Ministerul Educaţiei; Academia de Ştiinţe a Moldovei	Ministerul Afacerilor Externe şi Integrării Europene; Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Institutul Dezvoltării Societăţii Informaţionale	2016-2019	Număr de relaţii stabilite	Bugetul instituţiilor, în limitele alocaţiilor aprobate, resursele partenerilor de dezvoltare. Costul nu este estimat
7.7.	Stabilirea şi dezvoltarea relaţiilor cu liderii mondiali în domeniul securităţii cibernetice pentru a crea un Centru de excelenţă pentru cercetare şi dezvoltare	Ministerul Educaţiei	Ministerul Tehnologiei Informaţiei şi Comunicaţiilor; Academia de Ştiinţe a Moldovei; Institutul Dezvoltării	2016-2018	Centru de excelenţă creat	Bugetul instituţiilor, în limitele alocaţiilor aprobate; resursele partenerilor de

	în Republica Moldova		Societăţii Informaţionale			dezvoltare. Costul nu este estimat

_____

Hotărîrile Guvernului

811/29.10.2015 Hotărîre cu privire la Programul naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 *//Monitorul Oficial 306-310/905, 13.11.2015*