



LEGE
privind aprobarea Concepției securității informaționale
a Republicii Moldova

nr. 299 din 21.12.2017

Monitorul Oficial nr.48-57/122 din 16.02.2018

* * *

Parlamentul adoptă prezenta lege ordinară.

Art.1. – Se aprobă Concepția securității informaționale a Republicii Moldova, cuprinsă în anexă.

Art.2. – Guvernul, în comun cu Serviciul de Informații și Securitate al Republicii Moldova, pînă la data de 30 iunie 2018, va elabora și va prezenta Parlamentului spre aprobare programul de măsuri pentru implementarea concepției menționate.

Art.3. – Guvernul, în termen de 6 luni de la data intrării în vigoare a prezentei legi, va elabora și va prezenta spre examinare Strategia securității informaționale a Republicii Moldova și Planul de acțiuni pentru implementarea acesteia.

PREȘEDINTELE PARLAMENTULUI **Andrian CANDU**

Nr.299. Chișinău, 21 decembrie 2017.

Anexă

CONCEPȚIA SECURITĂȚII INFORMAȚIONALE
A REPUBLICII MOLDOVA

Capitolul I
DESCRIEREA SITUAȚIEI ȘI DEFINIREA PROBLEMEI

Secțiunea 1
Descrierea situației

1. Dezvoltarea rapidă a tehnologiei informației și extinderea multisectorială a acesteia reprezintă o caracteristică indispensabilă a societății contemporane, cu efecte diverse de ordin social, politic, militar și economic asupra vieții cotidiene, la nivel de stat, de societate și de persoană. În acest context, întreprinderea unor măsuri necesare pentru asigurarea securității la nivel național presupune un program complex de activități, care au legături directe cu nivelul asigurării securității informaționale a persoanei, a societății și a statului în ansamblu.

2. Evoluarea tehnologiei informației și diversificarea surselor de informare în masă, pe de o parte, creează premise favorabile pentru buna funcționare a societății contemporane, iar, pe de altă parte, facilitează extinderea utilizării de către centrele subversive a mijloacelor de

propagandă și de agresiune mediatică, în scopul destabilizării situației social-politice și al subminării suveranității, independenței și integrității teritoriale ale Republicii Moldova.

3. Creșterea dependenței societății contemporane de globalizarea sistemelor informaționale și a infrastructurilor de comunicații conduce la sporirea vulnerabilității persoanei, a societății și a statului față de amenințările, tot mai accentuate, din domeniile informațional-tehnologic și informațional-mediatic.

4. Măsurile de prevenire, depistare și contracarare a amenințărilor complexe și persistente la adresa securității informaționale pot fi întreprinse doar cu condiția existenței și funcționării unui cadru normativ corespunzător în domeniu, a unor instrumente și metode bine definite, a unor mecanisme de colaborare la nivel național și internațional.

5. Concepția securității informaționale a Republicii Moldova (în continuare – *Concepție*) este determinată de necesitatea protejării intereselor statului, ale societății și ale persoanei, a obiectivelor vitale și de importanță strategică pentru securitatea națională, de necesitatea asigurării protecției informației atribuite la secret de stat, precum și de necesitatea prevenirii și combaterii criminalității informatice.

6. Concepția reprezintă o viziune de ansamblu asupra scopului, obiectivelor, principiilor și direcțiilor de bază ale activității de asigurare a unui nivel înalt al securității informaționale a Republicii Moldova.

7. Securitatea informațională este parte componentă a sistemului național de securitate.

8. Interesele naționale în domeniul securității informaționale sînt: asigurarea respectării drepturilor și libertăților privind accesul la resursele informaționale; dezvoltarea domeniului tehnologiei informației și al comunicațiilor electronice și sporirea utilizării acestora; asigurarea protecției spațiului informațional, a obiectivelor vitale și de importanță strategică, a infrastructurii critice, a informațiilor atribuite la secret de stat și a celor cu accesibilitate limitată; prevenirea, depistarea și contracararea riscurilor și amenințărilor la adresa securității informaționale a Republicii Moldova, precum și protecția spațiului informațional național și a societății în ansamblu de impactul propagandei și al agresiunii mediatice din exterior și din interior.

9. Concepția constituie baza pentru elaborarea Strategiei securității informaționale a Republicii Moldova și a Planului de acțiuni pentru implementarea strategiei respective.

Secțiunea a 2-a

Noțiuni principale

10. În sensul prezentei Concepții, următoarele noțiuni semnifică:
amenințare la adresa securității informaționale – set de condiții, forțe și factori care pun în pericol interesele naționale în domeniul securității informaționale;

amenințare hibridă de securitate – operațiune subversivă și/sau de informație, condusă ori plasată sub comanda unor state, entități nonstatale, organizații, indivizi, care vizează, în mod special, slăbiciunile și vulnerabilitățile unei guvernări suverane, independente și integre;

armă informațională – informație și/sau tehnologie a informației, mijloace de comunicare în mass-media, alte resurse și metode, utilizate la nivel tactic, operativ și strategic în scopul desfășurării unui război informațional;

operațiune psihologică – acțiune planificată pentru transmiterea către publicul larg a mesajelor psihologic distructive, a informațiilor și indicatorilor selectați în funcție de emoții, de motive și de raționamente obiective sau subiective, în scopul influențării comportamentului autorităților, al organizațiilor, al grupurilor și/sau al persoanelor;

politica de asigurare a securității informaționale a Republicii Moldova – ansamblul direcțiilor de activitate a autorităților administrației publice, obligațiilor și responsabilităților acestora privind protecția intereselor naționale în spațiul informațional, stabilit cu respectarea echilibrului dintre interesele persoanei, ale societății și ale statului;

propagandă – acțiune de răspîndire sistematică a informației pentru influențarea atitudinilor, convingerilor și comportamentului persoanelor, pentru susținerea sau compromiterea anumitor instituții, cauze ori persoane prin prezentarea manipulatorie a informației și/sau prin reflectarea selectivă a evenimentelor, în scopul subminării intereselor naționale ale statului;

război informațional – ansamblu de acțiuni desfășurate de către entități statale sau nonstatale în spațiul informațional prin intermediul propagandei, al agresiunii mediatice, al manipulării și al dezinformării, care includ operațiuni digitale, cibernetice și psihologice, în scopul subminării suveranității, independenței și integrității teritoriale ale unui stat;

securitate informațională – stare de protecție a resurselor informaționale, precum și a persoanei, societății și statului, în spațiul informațional;

spațiu informațional – mediu de activitate (digital, cibernetic, mediatic) asociat cu formarea, crearea, transformarea, transmiterea, difuzarea, utilizarea și stocarea informațiilor, care produce efecte la nivel de conștiință individuală și/sau socială, de infrastructură informațională și de informație.

Secțiunea a 3-a

Scopul și obiectivele Concepției

11. Scopul Concepției este asigurarea protecției, în spațiul informațional, a drepturilor și libertăților fundamentale, a democrației și a statului de drept.

12. Obiectivele de bază în domeniul asigurării securității informaționale sînt:

- a) dezvoltarea capacităților de reacție în cazul unor amenințări hibride de securitate;
- b) monitorizarea permanentă și evaluarea periodică a nivelului securității informaționale a Republicii Moldova; identificarea surselor interne și externe de amenințare la adresa securității informaționale, precum și determinarea direcțiilor de activitate prioritare pentru prevenirea și suprimarea amenințărilor respective;
- c) monitorizarea spațiului informațional și depistarea acțiunilor de dezinformare și/sau de informare manipulatorie din interiorul sau exteriorul țării;
- d) crearea condițiilor pentru respectarea drepturilor persoanelor fizice și juridice în cadrul practicării activităților legale în spațiul informațional;
- e) crearea unui sistem integrat de comunicare și evaluare a amenințărilor la adresa securității informaționale și de elaborare a măsurilor operative de răspuns;
- f) coordonarea activității autorităților administrației publice, a instituțiilor publice și private în partea ce ține de exercitarea atribuțiilor privind asigurarea securității informaționale;
- g) dezvoltarea mecanismelor de prevenire, de depistare, de atenuare și de răspuns care ar permite schimbul de informație și asistență mutuală între autoritățile naționale responsabile de asigurarea securității informaționale;
- h) controlul civic (monitorizarea) asupra activității autorităților administrației publice, comisiilor de stat și celor interdepartamentale, altor structuri care exercită atribuții de asigurare a securității informaționale;
- i) dezvoltarea capacităților de prevenire, de depistare și de contracarare a acțiunilor/inacțiunilor care atentează la interesele legale ale persoanei, societății și statului privind securitatea informațională, a acțiunilor de alterare a informațiilor, de propagandă, a acțiunilor extremiste, teroriste și de altă natură care periclitează securitatea informațională;
- j) dezvoltarea mecanismelor de comunicare strategică la nivel național pentru realizarea intereselor naționale ale Republicii Moldova;
- k) dezvoltarea infrastructurii informaționale naționale;
- l) efectuarea cercetărilor științifice aplicative în domeniul securității informaționale;
- m) protecția rețelelor de comunicații speciale ale Republicii Moldova și a informației cu accesibilitate limitată, pentru menținerea funcțiilor vitale ale statului;

- n) asigurarea controlului asupra importului, certificării și utilizării mijloacelor de protecție a informației;
- o) dezvoltarea sistemului de pregătire a cadrelor în domeniul securității informaționale;
- p) asigurarea colaborării internaționale în domeniul securității informaționale;
- q) dezvoltarea capacităților de reziliență informațională și cibernetică;
- r) promovarea transparenței financiare în activitatea autorităților publice, a asociațiilor obștești și a societăților comerciale, în contextul asigurării securității informaționale;
- s) dezvoltarea culturii de securitate informațională;
- t) consolidarea cooperării cu societatea civilă în domeniul asigurării securității informaționale.

Secțiunea a 4-a

Amenințările la adresa securității informaționale

13. Principalele amenințări la adresa securității informaționale sînt:

- a) acțiunile subversive în scopul influențării politicii interne și externe a statului;
- b) amenințările hibride de securitate în scopul subminării securității naționale;
- c) dominația informațională externă pe teritoriul necontrolat de către autoritățile constituționale ale Republicii Moldova;
- d) elaborarea și aplicarea, de către alte state și entități, a concepției de război informațional;
- e) subminarea informațională a campaniilor electorale;
- f) alterarea conținutului informațiilor vehiculate în spațiul public (prin manipulare, dezinformare, prin tănuirea sau falsificarea informației) cu scopul de a genera panică, tensiuni ori conflicte sociale;
- g) îngrădirea accesului la informațiile publice;
- h) difuzarea materialelor cu caracter extremist, a pornografiei infantile și a mesajelor psihologic distructive;
- i) activitatea organizațiilor extremiste și teroriste, interesul acestora privind posesia și utilizarea armei informaționale;
- j) monopolul asupra formării, recepționării și/sau răspîndirii informației, inclusiv prin intermediul rețelelor de comunicații electronice;
- k) criminalitatea informatică transnațională, activitatea organizațiilor criminale internaționale, a grupurilor sau persoanelor, orientată spre obținerea accesului neautorizat la resursele de rețea și informație;
- l) acțiunile de distrugere, deteriorare sau suprimare radioelectronică a resurselor și sistemelor informaționale, a rețelelor de comunicații electronice și a sistemelor de protecție a informației;
- m) activitatea ilegală a structurilor politice, economice, militare, activitatea de spionaj a serviciilor speciale străine, a unor grupuri sau persoane, orientate spre obținerea accesului neautorizat la resursele informaționale sau obținerea controlului asupra funcționării resurselor, tehnologiei informației, sistemelor informaționale și rețelelor de comunicații electronice;
- n) nivelul redus de utilizare a tehnologiilor informaționale de către autoritățile administrației publice, de către instituțiile financiare de creditare, precum și în domeniul industriei, al agriculturii, al educației, al sănătății, al deservirii populației; nivelul redus de instruire a populației privind utilizarea sistemelor informaționale;
- o) diversiunile informaționale;
- p) lipsa culturii de securitate informațională;
- q) alocarea insuficientă a mijloacelor financiare pentru măsurile de asigurare a securității informaționale;

r) delimitarea neclară a atribuțiilor autorităților administrației publice responsabile de elaborarea și realizarea politicii de asigurare a securității informaționale a Republicii Moldova.

Capitolul II

INSTRUMENTELE ȘI CĂILE DE SOLUȚIONARE A PROBLEMEI

Secțiunea 1

Asigurarea securității informaționale la nivel național

14. Direcțiile strategice și tactice în domeniul asigurării securității informaționale se formează în baza intereselor naționale și ținându-se cont de amenințările la adresa securității informaționale a Republicii Moldova.

15. Asigurarea securității informaționale se bazează pe următoarele principii:

- a) legalității;
- b) caracterului sistemic, complex și științific;
- c) delimitării atribuțiilor autorităților care asigură securitatea informațională;
- d) realizării, pe etape, a programelor tematice privind asigurarea securității informaționale;
- e) controlului asupra adoptării și executării deciziilor;
- f) asigurării securității informaționale fără a prejudicia interesele persoanei, ale societății și ale statului;
- g) transparenței;
- h) continuității asigurării securității naționale;
- i) protecției datelor cu caracter personal.

16. În exercitarea atribuțiilor de asigurare a securității informaționale, statul, în persoana autorităților publice competente:

- a) efectuează analiza și prognoza obiectivă și multilaterală a amenințărilor la adresa securității informaționale a Republicii Moldova, elaborează măsuri, metode și mecanisme de asigurare a securității informaționale;
- b) elaborează și realizează, în comun cu instituțiile publice și private, programe tematice de stat în domeniul asigurării securității informaționale;
- c) organizează activitatea autorităților administrației publice, a asociațiilor obștești, a societăților comerciale în vederea realizării unui set de măsuri orientate spre prevenirea sau neutralizarea amenințărilor la adresa securității informaționale a Republicii Moldova;
- d) promovează, pe teritoriul Republicii Moldova, politica de susținere a producătorilor naționali de mijloace de informatizare și protecție a informației, întreprinde măsuri de protecție a pieței interne împotriva pătrunderii unor mijloace de informatizare, produse informaționale și mijloace de protecție a informației care nu corespund standardelor naționale și/sau internaționale;
- e) facilitează și promovează accesul persoanelor fizice și juridice la resursele și sistemele informaționale globale.

Secțiunea a 2-a

Metodele de asigurare a securității informaționale

17. În scopul prevenirii și contracarării amenințărilor la adresa securității informaționale a Republicii Moldova se elaborează și se aplică metode juridice, tehnico-organizatorice, economice, contrainformative și de securitate.

18. Metodele juridice prevăd:

- a) ajustarea standardelor naționale în domeniul securității informaționale la standardele internaționale;

b) elaborarea și perfecționarea legislației privind securitatea informațională a Republicii Moldova în scopul prevenirii, depistării și contracarării acțiunilor de alterare a informațiilor, de propagandă, a acțiunilor teroriste și extremiste în spațiul informațional, inclusiv: obținerea accesului neautorizat la informație; copierea, utilizarea sau distrugerea ilegală a informației ori falsificarea acesteia; distribuirea premeditată a informației neveridice; dezvăluirea ilegală a informației cu accesibilitate limitată, folosirea în scopuri criminale sau de profit a informației respective.

19. Metodele tehnico-organizatorice prevăd:

a) dezvoltarea și perfecționarea unui sistem informațional modern pentru asigurarea eficientă a securității naționale;

b) dezvoltarea capacităților de reacție urgentă, la nivel național, ale organelor de drept și de securitate pentru prevenirea, depistarea și contracararea acțiunilor/inacțiunilor ilegale în domeniul comunicațiilor electronice și al criminalității informatice, precum și tragerea la răspundere a persoanelor vinovate;

c) crearea unui sistem unic de stat de monitorizare și control al spațiului informațional național, inclusiv al traficului web protejat;

d) elaborarea, utilizarea și perfecționarea mijloacelor de protecție a informației, a metodelor de control al eficacității mijloacelor respective; crearea și aplicarea resurselor, tehnologiilor, sistemelor informaționale și a rețelilor de comunicații electronice protejate; sporirea fiabilității mijloacelor tehnice speciale și a asigurării de program;

e) crearea sistemelor și a mijloacelor de prevenire a acțiunilor speciale exercitate asupra sistemelor informaționale și de comunicații electronice, care provoacă distrugerea, lichidarea, distorsionarea informației sau modificarea regimului de funcționare a sistemelor și mijloacelor de informatizare și comunicație;

f) depistarea dispozitivelor tehnice speciale de obținere ascunsă a informației și a programelor dăunătoare (malware); prevenirea captării informației pe canalele tehnice; utilizarea mijloacelor criptografice de protecție la păstrarea, prelucrarea și transmiterea informației prin rețele de comunicații electronice; controlul asupra executării cerințelor speciale de protecție a informației;

g) certificarea mijloacelor de protecție tehnică și criptografică a informației; licențierea activității în domeniul asigurării securității informaționale; standardizarea metodelor și mijloacelor de protecție a informației;

h) elaborarea unui mecanism de conlucrare între autoritățile publice competente și persoanele fizice și juridice care desfășoară activitate în domeniul cibernetic al Republicii Moldova în vederea acordării de către acestea a accesului la codul sursă al aplicațiilor elaborate, comercializate și distribuite;

i) exercitarea controlului în domeniul aplicării tuturor tipurilor de semnături electronice;

j) perfecționarea sistemului de certificare a utilajului de comunicații electronice și a programelor sistemelor automatizate de prelucrare a informației, în scopul asigurării corespunderii acestora cerințelor securității informaționale;

k) elaborarea sistemului de atestare a obiectelor de informatizare privind îndeplinirea cerințelor de asigurare a protecției informației în timpul efectuării lucrărilor ce țin de prelucrarea și păstrarea informației cu accesibilitate limitată, în special a celei atribuite la secret de stat;

l) perfecționarea sistemului de control al acțiunilor personalului și utilizatorilor resurselor, sistemelor informaționale și rețelilor de comunicații electronice protejate; pregătirea specialiștilor în domeniul asigurării securității informaționale.

20. Metodele economice prevăd:

a) stabilirea volumului și modului de finanțare a programelor speciale de asigurare a securității informaționale, a altor lucrări legate de aplicarea metodelor juridice și tehnico-organizatorice de protecție a informației;

b) crearea unui sistem de asigurare a riscurilor informaționale ale persoanelor fizice și juridice.

21. Metodele contrainformative și de securitate prevăd:

a) identificarea imixtiunilor de natură subversivă în spațiul informațional, capabile să afecteze securitatea informațională a Republicii Moldova;

b) prevenirea, depistarea și contracararea amenințărilor hibride de securitate în spațiul informațional care subminează suveranitatea, independența și integritatea teritorială ale Republicii Moldova;

c) prevenirea, depistarea și contracararea riscurilor și amenințărilor generate de acțiunile ostile în spațiul informațional, capabile să provoace război informațional împotriva Republicii Moldova;

d) asigurarea protecției informative și contrainformative a intereselor naționale în spațiul informațional;

e) elaborarea și punerea în aplicare a unor măsuri de profilaxie menite să prevină, să identifice și să înlăture cauzele și condițiile ce conduc la subminarea securității informaționale;

f) prevenirea, depistarea și contracararea activităților subversive în spațiul informațional ale organizațiilor extremiste și teroriste, centrelor subversive și serviciilor străine de spionaj;

g) prevenirea, depistarea și contracararea activităților informativ-subversive generate de servicii speciale străine cu scopul defăimării Republicii Moldova pe plan extern.

Secțiunea a 3-a

Cooperarea internațională în domeniul securității informaționale

22. În cadrul cooperării internaționale în domeniul securității informaționale, Republica Moldova pornește de la interesele sale naționale, acționând în conformitate cu normele unanim recunoscute ale dreptului internațional și cu prevederile tratatelor internaționale la care este parte.

23. Direcțiile principale ale cooperării internaționale a Republicii Moldova pe problemele asigurării securității informaționale sînt:

a) asigurarea securității în cadrul schimbului de informații, inclusiv în cazul transmiterii acestora prin rețele de comunicații electronice naționale și internaționale;

b) prevenirea, depistarea și contracararea accesului neautorizat la informațiile cu accesibilitate limitată din rețelele de comunicații electronice bancare internaționale și din sistemele de comerț electronic, la informațiile organelor internaționale de drept;

c) interzicerea elaborării, răspîndirii și aplicării armei informaționale;

d) schimbul de informații, experiențe și analize, în condiții de parteneriat, cu autoritățile altor state cu atribuții informative, contrainformative și de aplicare a legii, în scopul prevenirii, depistării și contracarării amenințărilor hibride de securitate în spațiul informațional.

24. Realizarea direcțiilor specificate necesită o intensificare a cooperării Republicii Moldova cu organizațiile internaționale ce își desfășoară activitatea în domeniul asigurării securității informaționale.

25. Cooperarea internațională în domeniul securității informaționale are drept scop devenirea Republicii Moldova stat-furnizor de securitate pe plan regional și mondial.

Secțiunea a 4-a

Organizarea sistemului de asigurare a securității informaționale

26. Asigurarea securității informaționale se efectuează în baza delimitării atribuțiilor autorităților legislative, executive și judecătorești în domeniul respectiv.

27. Competența și atribuțiile instituțiilor ce asigură securitatea informațională sînt prevăzute de actele normative ce reglementează domeniile de activitate ale instituțiilor respective.

28. Securitatea informațională reprezintă o componentă inseparabilă a securității naționale, fiind asigurată, în limita competențelor stabilite de lege, de către Parlamentul, Guvernul, Președintele Republicii Moldova, Consiliul Suprem de Securitate, Serviciul de Informații și Securitate, Ministerul Economiei și Infrastructurii, Ministerul Afacerilor Interne, Ministerul Apărării, Ministerul Afacerilor Externe și Integrării Europene, Ministerul Educației, Culturii și Cercetării, Procuratura, instanțele judecătorești, Consiliul Coordonator al Audiovizualului, Consiliul de Observatori al Instituției Publice Naționale a Audiovizualului Compania „Teleradio-Moldova”, Comisia Electorală Centrală, Centrul Național pentru Protecția Datelor cu Caracter Personal.

29. Autoritățile administrației publice locale, inclusiv ale UTA Găgăuzia, întreprinderile, instituțiile și organizațiile, indiferent de tipul de proprietate și forma juridică de organizare, persoanele fizice implicate în asigurarea securității informaționale realizează sarcini în domeniul securității informaționale în modul stabilit de legislația Republicii Moldova.

30. Serviciul de Informații și Securitate, în limita competențelor, exercită atribuțiile autorității naționale de coordonare a activității autorităților publice desfășurate în domeniul securității informaționale.

31. Pentru realizarea intereselor statului în spațiul informațional și în domeniul asigurării securității informaționale pot fi create comisii de stat sau interdepartamentale care să soluționeze problemele privind asigurarea securității informaționale a Republicii Moldova, în conformitate cu împuternicirile acordate.

32. Realizarea consecventă și deplină a prevederilor prezentei Concepții va garanta dezvoltarea continuă a sistemului de securitate informațională a Republicii Moldova.