**Republica Moldova**

**GUVERNUL**

**HOTĂRÎRE** Nr. 201
din 28.03.2017

**privind aprobarea Cerinţelor minime obligatorii de securitate cibernetică**

Publicat : 07.04.2017 în Monitorul Oficial Nr. 109-118 art Nr : 277

În scopul executării prevederilor art. 10 alin. (1) şi art. 18 alin. (1) din Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, art. 11 alin. (2) lit. e) şi f) şi art. 24 din Legea nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr. 70-73, art. 314), cu modificările ulterioare, şi ale Programului naţional de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărîrea Guvernului nr. 811 din 29 octombrie 2015 (Monitorul Oficial al Republicii Moldova, 2015, nr. 306-310, art. 905), Guvernul HOTĂRĂŞTE:

1. Se aprobă Cerinţele minime obligatorii de securitate cibernetică (se anexează).

2. Ministerul Tehnologiei Informaţiei şi Comunicaţiilor, în termen de 6 luni de la data intrării în vigoare a prezentei hotărîri, va asigura definitivarea cadrului instituţional pentru implementarea Cerinţelor minime obligatorii de securitate cibernetică, va elabora modelul de politică internă privind securitatea cibernetică a instituţiei şi va definitiva lista sistemelor informaţionale automatizate de stat de importanţă majoră, pentru aplicarea cerinţelor de securitate avansată.

3. Cancelaria de Stat, ministerele şi alte autorităţi administrative centrale subordonate Guvernului şi structurile organizaţionale din sfera lor de competenţă (autorităţile administrative din subordine, serviciile publice desconcentrate şi cele aflate în subordine, instituţiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), autorităţile administrative autonome şi unităţile cu autonomie financiară, în termen de pînă la 31 decembre 2017, vor asigura implementarea Cerinţelor minime obligatorii de securitate cibernetică.

4. Controlul asupra executării prezentei hotărîri se pune în sarcina Ministerului Tehnologiei Informaţiei şi Comunicaţiilor.

**PRIM-MINISTRU** **Pavel FILIP**

**Nr. 201. Chişinău, 28 martie 2017.**

Anexă
la Hotărîrea Guvernului nr.201
din 28 martie 2017

# CERINȚELE MINIME OBLIGATORII DE SECURITATE CIBERNETICĂ

## I. DISPOZIȚII GENERALE

1. Cerințele minime obligatorii de securitate cibernetică (în continuare – *Cerințe minime*) se aplică în cadrul Cancelariei de Stat, ministerelor, altor autorităţi administrative centrale subordonate Guvernului, inclusiv al structurilor organizaţionale din sfera lor de competenţă (autorităţile administrative din subordine, serviciile publice desconcentrate şi cele aflate în subordine, instituţiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), al autorităților administrative autonome și unităţilor cu autonomie financiară (în continuare – *instituții*) faţă de:

1) echipamentele (hardware) și produsele de program (software) existente în cadrul fiecărei instituţii;

2) sistemele informatice, resursele și sistemele informaționale existente în instituție (în continuare – sisteme), precum și cele aflate la etapa de elaborare, testare și implementare.

2. Cerințele minime, după domeniul de aplicare, sînt de două categorii:

1) nivelul 1 – de securitate cibernetică de bază (utilizare TIC în activitatea instituției);

2) nivelul 2 – de securitate cibernetică avansată (utilizare TIC în activitatea instituției și prestare servicii bazate pe TIC).

3. Aceste cerinţe nu se aplică în cazul sistemelor informaţionale şi reţelelor de comunicaţii speciale, atribuite la secretul de stat.

4. În alte cazuri, prevăzute de legislația în vigoare, se aplică cerințele speciale de securitate cibernetică.

5. În sensul prezentelor Cerințe, următoarele noţiuni principale semnifică:

*autentificare multifactorială* – autentificare cu cel puțin doi factori de autentificare independenți;

*cerințe minime obligatorii de securitate cibernetică* – sistemul de management al securității cibernetice – toate politicile, procedurile, planurile, procesele, practicile, rolurile, responsabilitățile, resursele și structurile care sînt folosite pentru a proteja și păstra intactă informația;

*paravan de protecție (firewall)* – un dispozitiv sau o serie de dispozitive configurate în așa fel încît să filtreze, să cripteze sau să intermedieze traficul dintre diferite domenii de securitate pe baza unor reguli predefinite;

*actualizare* – procedeu de modificare a unor fișiere și aplicații ale calculatorului sau crearea unor noi;

*protecție malware* – măsură tehnică de securitate, efectuată prin folosirea de programe antivirus, în scopul protecției cibernetice;

*antispyware* – măsură tehnică de securitate, efectuată prin folosire de programe, în scop de prevenire a intruziunii cibernetice;

*test de penetrare* – evaluare a securității cibernetice a unui sistem împotriva diferitor tipuri de atacuri.

Alţi termeni sînt utilizaţi în sensul definit de Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat, Legea nr.1069-XIV din 22 iunie 2000 cu privire la informatică şi Hotărîrea Guvernului nr. 811 din 29 octombrie 2015 „Cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020”.

## II. ORGANIZAREA SISTEMULUI INTERN DE SECURITATE CIBERNETICĂ

6. Conducătorul autorității poartă răspundere pentru asigurarea securității cibernetice în instituție.

7. Conducătorul autorității desemnează, prin act administrativ, persoana (subdiviziunea) responsabilă de punerea în aplicare a sistemului de management al securității cibernetice în instituție și prezintă Ministerului Tehnologiei Informației și Comunicațiilor informația respectivă în termen de cinci zile lucrătoare de la desemnarea acesteia.

8. Persoana responsabilă are următoarele atribuții:

1) organizează sistemul de management al securității cibernetice în instituție conform sistemului de management al securității cibernetice;

2) participă, cel puțin o dată pe an, la cursurile de formare organizate de Ministerul Tehnologiei Informației și Comunicațiilor privind securitatea cibernetică și, respectiv, organizează cursuri pentru angajații instituției;

3) asigură elaborarea, implementarea și respectarea prevederilor următoarelor documente: planul de acțiuni pentru asigurarea securității cibernetice al instituției, politica de securitate cibernetică a instituției, planul de instruire și responsabilizare în securitatea cibernetică a personalului, regulamentele interne de securitate cibernetică, procedurile de recuperare.

9. Setul de documente se aprobă de conducătorul instituției și trebuie să fie revizuit cel puțin o dată pe an, dacă:

1) a fost modificat sistemul și poate fi afectată securitatea acestuia;

2) au fost descoperite noi amenințări la securitatea sistemului;

3) s-a constatat o creștere bruscă a incidentelor de securitate asupra sistemului sau s-a depistat cel puțin un incident semnificativ de securitate a sistemului;

4) a fost restructurată persoana/subdiviziunea organizatorică responsabilă de sistemul de securitate cibernetică;

5) au fost modificate și/sau completate legi și/sau acte normative care reglementează funcționarea sistemului.

10. Sistemul de securitate cibernetică asigură:

1) disponibilitatea informației (accesul la informație pentru o anumită perioadă de timp specificată, conform specificațiilor tehnice);

2) integritatea informației (păstrarea informației cu toate atributele sale inițiale și modificarea ei doar de către persoanele autorizate);

3) confidențialitatea informației (acces la informație doar al persoanelor autorizate și doar la datele prestabilite pentru acces);

4) protecția echipamentelor și produselor program (calculatoare, software, sisteme de stocare a datelor, echipamente de rețea și alte echipamente tehnice);

5) identificarea și remedierea vulnerabilităților;

6) efectuarea copiilor de rezervă și stabilirea procedurilor de recuperare.

11. Politica de securitate cibernetică, în calitate de document instituțional, include:

1) scopul și obiectivele;

2) principiile de organizare internă a managementului de securitate cibernetică;

3) analiza situației și vulnerabilităților (disponibilitate, integritate și confidențialitate a datelor, precum și analiza riscurilor și căilor de remediere);

4) declarația managementului instituției de susținere a scopului și principiilor securității cibernetice în instituție.

12. Planul de instruire și responsabilizare în securitatea cibernetică a personalului instituției include:

1) instruirea în igiena și etica cibernetică (programe/cursuri de formare în domeniul securității

cibernetice);

2) măsurile de securitate internă privind activitatea personalului (autorizație de acces, stabilirea drepturilor, obligațiilor, restricțiilor, responsabilizarea angajaților, monitorizarea, proceduri de asistență ale utilizatorilor în cazuri de urgență);

3) măsurile de securitate privind activitatea personalului/companiilor externe cooptate (coordonarea responsabilităților, acorduri de nedivulgare, autorizație de acces, monitorizare, planul de contingență (intervenție) pentru suspendarea operațiunilor de externalizare).

13. Regulamentele interne de securitate cibernetică prevăd:

1) dezvoltarea, actualizarea, modificarea, mentenanța sistemelor informaționale;

2) gestionarea activelor și facilităților de comunicații electronice și tehnologia informației;

3) stocarea copiilor de rezervă ale datelor, precum şi ale procedurilor de control;

4) păstrarea datelor de acces, de jurnalizare a activităților;

5) monitorizarea securităţii sistemului;

6) regulile de gestionare a evenimentelor de securitate;

7) procedurile de utilizare a datelor în cazuri excepționale (de urgență)

8) procedurile de evaluare a securității cibernetice.

14. Procedurile de recuperare includ:

1) stabilirea procedurilor privind copierea de rezervă și de recuperare în cazul unui incident de securitate cibernetică;

2) descrierea acțiunilor măsurabile de recuperare;

3) atribuirea responsabilităților pentru restabilirea funcționalităților;

4) stabilirea procedurilor de notificare.

## III. CERINȚELE MINIME OBLIGATORII DE SECURITATE CIBERNETICĂ DE NIVELUL 1 (UTILIZAREA TIC ÎN ACTIVITATEA INSTITUȚIEI)

15. Controlul accesului se realizează după cum urmează:

1) drepturile, obligațiile, restricțiile și responsabilitățile utilizatorilor urmează a fi stabilite de către persoana responsabilă de proces și comunicat într-o formă stabilită responsabilului/subdiviziunii de securitate cibernetică;

2) persoana care desfășoară activități de administrare a sistemului utilizează conturi diferite pentru funcții de administrare și funcții de utilizator;

3) fiecare cont de utilizator este asociat cu o persoană anumită. În cazul în care sistemul prevede neadmiterea utilizării acestor conturi de către alte persoane, atunci sistemul trebuie să includă mijloace tehnice speciale, care să nu admită utilizarea acestor conturi de către persoane terțe;

4) în cazul în care sistemul nu este utilizat pentru autentificarea multifactorială, adică nu este un atribut de o natură statică (de exemplu, simbolic, un mesaj de cod-text de unică folosință), dar este un atribut de altă natură, utilizatorii sistemului trebuie să utilizeze o parolă;

5) utilizatorul sistemului trebuie să folosească în calitate de parolă o combinaţie din numere (0-9), caractere latine (minuscule şi majuscule) şi simboluri speciale (!#%), constituită din numărul minim de caractere, stabilit prin regulamentul intern de securitate, dar nu mai puțin de 7 caractere;

6) se interzice stocarea electronică și transportarea în formă necriptată a parolelor utilizatorilor sistemului, inclusiv a procesului de autentificare a utilizatorilor. Se admite transportarea acestora prin rețea publică necriptată doar în cazul utilizării unei parole de o singură folosință, cu o valabilitate de 48 de ore de la momentul transmiterii acestora;

7) sistemul trebuie să dispună de mecanisme de gestiune a parolelor, precum şi să asigure autentificarea şi identificarea utilizatorului pentru o perioadă limitată de timp;

8) nu se admite utilizarea în echipamentele și produsele program a parolelor implicite (de la

producător);

9) datele despre activitățile în sistem (jurnalizarea) se stochează în timp real şi se păstrează pe perioada stabilită prin regulamentul intern de securitate, dar nu mai puțin de 6 luni;

10) orice activitate în sistem trebuie să poată fi identificată într-un anumit cont de utilizator sau adresă IP;

11) managementul drepturilor de utilizator trebuie să asigure ca fiecare utilizator să poată face uz doar de drepturile sale. Verificarea activităților în sistem se realizează periodic, la etape de timp stabilite conform regulamentului intern de securitate, dar nu mai rar de o dată la 6 luni;

12) managementul controlului accesului trebuie să fie setat ca să permită acces autorizat din rețea externă prin Internet doar cu o parolă de o singură folosință, inclusiv prin semnătura electronică din cadrul serviciului electronic guvernamental de autentificare şi control al accesului (MPass).

16. Securitatea fizică presupune:

1) delimitarea clară a perimetrului rezervat diferitor grupuri de echipamente IT, alcătuirea planurilor camerelor de servere și a rețelelor;

2) asigurarea condițiilor de încălzire, ventilare și aer condiționat a încăperilor specializate;

3) asigurarea accesului în spațiile specializate strict conform competențelor;

4) asigurarea securității energetice prin utilizarea unor dispozitive conforme normativelor în vigoare și cu protecție la suprasarcină;

5) asigurarea mentenanței adecvate, conform cerințelor tehnice;

6) evidența echipamentelor și produselor program, utilizare în cadrul instituției.

17. Securitatea operațională stabilește că:

1) echipamentele și produsele program trebuie să fie protejate ca să asigure operaționalitatea sistemelor;

2) pe calculatoarele conectate la rețeaua Internet trebuie să fie instalat cel puțin:

a) un sistem de operare cu actualizările curente aplicate;

b) program antivirus activat și actualizat;

c) paravan de protecție (firewall) activat;

d) instalare caracteristici de blocare automată a sistemului în caz de neutilizare a acestuia (screen saver, log-off);

3) controlul tehnic se efectuează periodic, conform regulamentului intern de securitate, şi vizează:

a) securitatea rețelelor, nodurilor și liniilor majore de interconectare cu rețele externe;

b) evaluarea necesităților de instalare și utilizare a echipamentelor fără fir, conform regulamentului intern de securitate, securizarea conexiunilor fără fir (autorizarea echipamentelor și criptarea datelor);

c) securitatea serverelor web, DNS și DHCP;

d) securitatea serverelor cu baze de date (instalarea în zona intranet, configurarea rețelei pentru a elimina camera pentru acces direct din rețeaua externă);

e) securitatea echipamentelor de rețea (router, comutator, caracteristici de control al accesului);

f) starea caracteristicilor de securitate cibernetică;

g) administrarea pachetelor de actualizare a produselor program privind securitatea cibernetică;

h) verificarea vulnerabilităților sistemelor și remedierea deficiențelor;

i) cerințele privind securitatea la utilizarea rețelei Internet;

4) aplicarea cerințelor de securitatea cibernetică la utilizarea rețelelor:

a) caracteristicile echipamentelor şi produselor program pentru gestionarea fluxului de la/către utilizatori, conform regulamentului intern de securitate;

b) serviciile de rețea care nu sînt utilizate trebuie să fie dezactivate;

c) echipamentele active de rețea trebuie configurate și testate astfel încît să asigure izolarea rețelei private de rețelele adiacente;

5) elaborarea planului de continuitate, care va asigura restaurarea caracteristicilor sistemului și a

datelor în caz de incident de securitate, care să includă:

a) procedura de efectuare a copiilor de rezervă (back-up) ale datelor, aplicaţiilor şi sistemelor (automată/manuală, periodicitatea și durata disponibilității);

b) conţinutul copiei de rezervă (date, aplicaţii, sisteme);

c) amplasarea copiei/copiilor de rezervă;

d) testarea periodică a copiilor de rezervă;

e) procedura de recuperare/restaurare a datelor, aplicaţiilor şi sistemelor;

f) procedura de constatare a necesității efectuării altor copii de rezervă.

6) stabilirea mecanismului de scoaterea din uz a echipamentelor, distrugerea datelor ce le conțin și reutilizarea lor;

7) stabilirea cerințelor de securitate și restricții pentru echipamentele personale utilizate în cadrul instituției.

18. Schimbul securizat de date şi de comunicări include următoarele:

1) aplicarea ghidului de utilizare a serviciilor sistemului de poştă electronică, aprobat ca document tehnic pentru toate autoritățile sus-menționate, și obligarea personalului privind:

a) verificarea chenarului cu adrese înainte de expediere a corespondenței și a destinatarului, pentru a evita erorile;

b) precauția față de conținutul mesajelor recepționate, verificarea datelor expeditorului/companiei, în mod special a celor de la expeditori necunoscuți, privind eventuala falsificare a identității pentru a ascunde adevărata sa origine;

c) verificarea și scanarea antivirus a anexelor la mesaje recepționate și a extensiilor acestora;

2) interzicerea:

a) redirecționării automate a mesajelor din poșta de serviciu spre alte conturi personale/private;

b) utilizării poştei electronice de serviciu pentru a expedia sau redirecționa mesaje considerate obscene, amenințătoare, ofensatoare, calomnioase, defăimătoare, rasiste, pornografice, de hărțuire, de ură, remarci discriminatorii și alte mesaje antisociale;

c) transmiterii/retransmiterii în lanț a mesajelor cu divers conținut irelevant pentru activitatea de serviciu;

d) utilizării poştei electronice de serviciu pentru obţinerea unui cîştig material, în scopuri personale, politice sau de alt gen;

e) distribuirii materialelor protejate de drepturi de autor;

f) transmiterea informațiilor confidențiale prin mesaje electronice nesecurizate;

g) utilizarea poștei electronice de serviciu pentru răspîndirea virușilor de calculator, de infiltrare în sisteme, deteriorare sau distrugere a datelor, produselor program și echipamentelor ori care duc la degradarea sau perturbarea performanței rețelei;

h) ascunderea și încercarea de a ascunde identitatea atunci cînd este trimis un mesaj prin poșta electronică de serviciu;

3) limitarea accesului personalului la conținut obscen și antisocial, a descărcării conținutului protejat de drepturi de autor, utilizarea neconformă a informațiilor de serviciu și distribuirea lor, descărcarea materialelor din surse necunoscute, precum și alte activități ce contravin obiectivelor instituției.

## IV. CERINȚELE MINIME OBLIGATORII DE SECURITATE CIBERNETICĂ DE NIVELUL 2 (UTILIZAREA TIC ÎN ACTIVITATEA INSTITUȚIEI ȘI PRESTAREA SERVICIILOR BAZATE PE TIC)

Suplimentar cerințelor din capitolul III, în cazul instituțiilor ce prestează servicii bazate pe TIC, doar pentru infrastructura respectivă, se aplică următoarele cerințe avansate.

19. Controlul accesului se realizează în felul următor:

1) parolele utilizatorilor de sistem se modifică nu mai tîrziu de 90 de zile calendaristice, cu limitarea posibilității de modificare manuală a acesteia nu mai des de două ori în decursul a 24 de ore;

2) parolele se stabilesc astfel încît să nu coincidă cu nici una dintre cele cinci parole utilizate anterior;

3) contul utilizatorului se blochează imediat în cazul în care utilizatorul a folosit parola incorect de trei ori consecutiv, cu excepția contului administratorului de sistem. Pentru aceste cazuri se stabilește procedura de reactivare a contului utilizatorului;

4) contul de acces al administratorului, în cazul accesării de la distanță a sistemului, inclusiv a echipamentelor care nu se află în posesia instituției, este asigurat doar cu autentificarea multifactorială și utilizarea unui canal securizat de comunicații;

5) accesul fizic la echipamentele care asigură funcționarea sistemului este permis de către instituție doar persoanelor autorizate;

6) instituția asigură păstrarea pe o perioadă de cel puțin 6 luni a înregistrărilor accesului în sistem, începînd cu prima accesare a utilizatorului.

20. Securitatea fizică include următoarele:

1) accesul în spațiul rezervat pentru echipamentele IT se realizează conform atribuțiilor stabilite în fișa postului, prin utilizarea unor mecanisme de securizare avansată. Accesările se monitorizează și se înregistrează inclusiv pe perioada de valabilitate a accesului și suspendarea acestuia în cazul eliberării din funcție;

2) securitatea energetică prevede implementarea măsurilor de protecție și control al surselor de alimentare: utilizarea unor dispozitive de protecție la suprasarcină, surse de tensiune neîntrerupte, generatoare electrice de rezervă și cablare alternativă. Cablurile de alimentare cu energie electrică trebuie să fie protejate. Sursele de alimentare UPS se vor instala obligatoriu la centrele de date, pentru a menține funcționarea pe timpul deconectărilor de rețea, pînă la conectarea la surse alternative de energie;

3) echipamentele utilizate în sistemul informatic trebuie amplasate și protejate astfel încît să fie redus riscul deteriorării lor în cazul calamităților naturale și al altor accidente;

4) prevenirea, detectarea și stingerea incendiilor; interzicerea fumatului în aria rezervată echipamentelor IT, înlăturarea materialelor inflamabile, utilizarea detectoarelor de căldură și fum, dotarea cu stingătoare de incendii, utilizarea dispozitivelor de alarmă, instruirea personalului pentru cazuri de urgență;

5) protecția împotriva inundațiilor și a excesului de umiditate, care implică dotarea perimetrului IT cu detectoare de umiditate, conectate la dispozitive de alarmă;

6) asigurarea condițiilor de încălzire, ventilare și aer condiționat; asigurarea unui mediu ambiental controlat, conform cerințelor tehnice.

21. Securitatea operațională presupune:

1) instalarea/operarea în nodurile ce interacționează cu rețele externe a sistemului de securitate cibernetică pentru prevenirea intruziunilor (IPS) și/sau a sistemului de depistare a intruziunilor (IDS);

2) instalarea/utilizarea registrului evenimentelor cu următoarele caracteristici:

a) păstrarea datelor pentru o perioadă de cel puțin 12 luni;

b) înregistrarea activităților utilizatorilor în sistem, cu indicarea corectă a timpului, care trebuie să coincidă efectiv cu timpul universal coordonat (UTC) al organului competent;

c) sistemul înregistrează conținutul monitorizării planificate și analiza acesteia, în scopul de a detecta incidentele. Datele minime înregistrate sînt: numele utilizatorului, timpul și IP adresa;

d) sistemul va fi dotat cu un mecanism de filtrare/gestionare a mesajelor de eroare generate;

3) aplicarea regulilor de utilizare de către instituție a dispozitivelor mobile, aprobate ca document tehnic pentru toate autoritățile sus-menționate, care vor include:

a) cerințele pentru protecția fizică și responsabilizarea utilizatorilor;

b) aplicarea politicii de gestionare a componentelor produselor de program, inclusiv a pachetelor de actualizări;

c) aplicarea politicii de gestionare a resurselor informaționale pentru echipamentele de rețea;

d) prevederile privind controlul accesului;

e) tehnicile criptografice;

f) protecția antivirus;

g) dezactivarea accesului la dispozitivul mobil de la distanță, în scopul prevenirii ștergerii informației sau blocării acestuia;

h) aplicarea politicilor de gestiune a copiilor de rezervă;

4) implementarea mecanismelor de prevenire și depistare promptă a instalării și utilizării neautorizate a punctelor de acces la rețelele fără fir în cadrul instituției;

5) managementul evoluțiilor IT prevede implementarea unor proceduri care să ofere siguranța că sînt îndeplinite următoarele condiţii:

a) descrierea procesului de modificări/aprobări ale persoanelor autorizate, testărilor și rapoartelor planificate;

b) actualizările la timp și complete;

c) gestiunea fişelor de schimbări/intervenţii;

d) actualizarea manualelor de instalare/utilizare, în concordanţă cu ultima versiune de sistem;

e) gestiunea/evidenţa versiunilor produselor program utilizate şi ale documentaţiei tehnice;

6) managementul mijloacelor de stocare externă prevede că:

a) datele confidențiale sau importante, stocate pe suport amovibil sînt criptate;

b) multiplicarea copiilor se realizează la necesitate și pe dispozitive separate;

c) personalul ce utilizează mijloacele de stocare externă urmează a fi instruite corespunzător;

d) la scoaterea din uz a mijloacelor de stocare care conţin informaţii cu grad de clasificare, datele de pe mijlocul de stocare se extrag, iar echipamentul se distruge;

7) analiza riscurilor se efectuează periodic, dar nu mai rar de o dată la doi ani, și servește pentru ajustarea politicii de securitate cibernetică și a regulamentelor interne;

8) efectuarea separării sarcinilor pentru următoarele categorii de activităţi în domeniul TI:

a) proiectarea și programarea sistemelor;

b) administrarea și întreținerea sistemelor;

c) introducerea datelor;

d) securitatea cibernetică;

e) administrarea bazelor de date;

f) managementul modificărilor şi dezvoltării sistemului informatic;

9) efectuarea auditului intern de securitate anual, pînă la finele lunii ianuarie a anului următor, de către subdiviziunile responsabile de tehnologia informației, pentru a verifica:

a) eliminarea de pe calculatoarele instituției conectate la Internet a datelor și programelor care nu sînt necesare;

b) prezența paravanului de protecție. Dacă necesităţile cer conectarea directă la Internet cu riscuri minime, se utilizează includerea în configuraţie a unei protecţii de tip „firewall”, pentru a facilita controlul traficului dintre reţeaua entităţii şi Internet, dar şi pentru a stopa intruziunea pachetelor de date externe, neautorizate;

c) protecția împotriva virușilor informatici prin implementarea unei proceduri privind utilizarea unei soluţii antivirus care să ofere: aplicarea acesteia în toate serverele şi stațiile de lucru; actualizarea fişierului de definiţii antivirus; interdicția dezactivării antivirusului de către utilizatori la staţia proprie de lucru; antivirusul scanează toate fişierele (pe server şi pe stațiile de lucru) automat, în mod periodic;

d) detectarea şi corectarea altor modificări neautorizate ale configurărilor realizate de către utilizatori, care sporesc riscurile de securitate cibernetică;

10) efectuarea periodică a testului de penetrare a sistemelor informaționale automatizate de importanță majoră se efectuează în conformitate cu politica de securitate cibernetică a instituției. Rezultatele testului sînt prezentate Ministerului Tehnologiei Informației şi Comunicațiilor, în termen de o lună, împreună cu planul de remediere a deficiențelor depistate.

## V. CERINȚELE MINIME OBLIGATORII DE ASIGURARE A SECURITĂȚII CIBERNETICE LA ACHIZIȚIA SISTEMELOR INFORMAȚIONALE NOI SAU ACTUALIZAREA CELOR EXISTENTE

22. La inițierea achizițiilor de sisteme informaționale automatizate noi sau actualizarea celor existente, instituția trebuie să asigure includerea în documentația de achiziții, ca parte a cerințelor nonfuncționale, a următoarelor cerințe:

1) suportul anumitor sisteme de securitate şi de mentenanţă (inclusiv înlăturarea lacunelor de securitate ale sistemului, într-o perioadă prestabilită);

2) transmiterea către instituție a dreptului de autor asupra codului-sursă a produselor program;

3) stabilirea perioadei de timp în care se efectuează actualizările propriu- zise;

4) sistemul de securitate cibernetică poate prevedea caracteristici mai stricte decît cele prevăzute în prezentele Cerințe, dar în măsura în care nu intră în conflict cu legislația în vigoare;

5) înainte de achiziționarea unui nou sistem sau dezvoltarea celui existent, instituția elaborează şi aprobă politica de securitate şi se asigură că sistemele noi, pe parcursul dezvoltării lor, vor fi conforme prezentelor Cerințe;

6) înainte de a pune în funcțiune un nou sistem, instituția trebuie să se asigure de funcționalitatea caracteristicilor de securitate ale acestuia conform cerințelor prestabilite, prin efectuarea de o terţă parte a testelelor respective;

7) instituția asigură efectuarea periodică a auditului de securitate a sistemului, în conformitate cu documentaţia tehnică aprobată;

8) dezvoltarea şi testarea sistemului nu trebuie să fie sau să prezinte un pericol pentru integritatea datelor stocate în sistem.

## VI. CERINȚE DE SECURITATE LA EXTERNALIZAREA ADMINISTRĂRII/MENTENANŢEI SISTEMELOR

23. În cazul în care instituția externalizează serviciile de administrare şi mentenanţă a sistemelor informaţionale şi încheie un contract cu furnizorul extern de servicii, contractul trebuie să includă şi cerințe de securitate. Contractul va stabili, cel puțin:

1) reglementările interne de securitate cibernetică ale instituției pe care trebuie să le urmeze prestatorul de servicii în realizarea prevederilor contractuale;

2) serviciile externalizate;

3) cerințele precise pentru volumul şi calitatea serviciilor externalizate documentate ca Service Level Agreement (SLA);

4) drepturile şi obligațiile instituției şi prestatorului de servicii externalizate:

a) dreptul instituției de a monitoriza continuu calitatea serviciilor furnizate;

b) dreptul instituției de a înainta prestatorului extern de servicii un titlu executoriu cu privire la aspectele legate de externalizarea de bună-credință, de înaltă calitate, executarea la timp şi corectă a legilor şi a regulamentelor;

c) dreptul instituției de a înainta prestatorului extern de servicii o cerere scrisă motivată pentru încetarea imediată a contractului de externalizare, în cazul în care instituția a constatat că prestatorul

extern de servicii nu respectă cerințele contractului de externalizare privind valoarea sau calitatea serviciului;

d) obligația prestatorului extern de servicii de a furniza instituției informația privind monitorizarea continuă a calității serviciilor de externalizare prestate;

e) dreptul de audit al prestatorului de serviciu, dacă au fost notificate nonconformități critice.

## VII. RĂSPUNSUL LA INCIDENTE, CONTINUITATEA PROCESELOR ȘI RECUPERAREA

24. Planul de răspuns la incidente stabilește că:

1) instituția trebuie să elaboreze și să pună în aplicare planul de răspuns de incidente cibernetice;

2) în cazul unor încălcări ale securității cibernetice, persoana responsabilă/subdiviziunea asigură imediata notificare, înregistrare și verificare a incidentelor de securitate cibernetică și punerea în aplicare a măsurilor de contracarare a acestora, conform procedurilor stabilite.

25. Continuitatea activității și procedurile de recuperare în caz de dezastru trebuie să prevadă:

1) implementarea procedurilor de efectuare a copiilor de rezervă și a celor de recuperare;

2) elaborarea și implementarea obiectivelor de recuperare, conform obiectivelor momentului de recuperare (OMR) și perioadei de recuperare (OPR).

26. Conformitatea cu cerințele interne și externe de securitate cibernetică stipulează că:

1) instituția actualizează planul său de acțiuni pentru asigurarea securității cibernetice, care precizează măsurile puse în aplicare și cele planificate;

2) instituția asigură conformitatea sa cu cerințele externe de securitate cibernetică, prevăzute de legislație.