



GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr. _____

din _____
Chișinău

Privind aprobarea Cerințelor minime obligatorii de securitate cibernetică

În scopul executării prevederilor art. 10 alin. (1) și art. 18 alin. (1) din Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare, art. 11 alin. (2) lit. e) și f) și 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, și ale Programului național 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 HOTĂRĂȘTE:

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

2. Ministerul Tehnologiei Informației și Comunicațiilor, în termen de 6 luni de la data intrării în vigoare a prezentei hotărîri, va asigura definitivarea cadrului instituțional pentru implementarea Cerințelor minime obligatorii de securitate cibernetică, va elabora modelul de politică internă privind securitatea cibernetică a instituției și va definitiva lista sistemelor informaționale automatizate de stat de importanță majoră, pentru aplicarea cerințelor de securitate avansată.

3. Cancelaria de Stat, ministerele și alte autorități administrative centrale subordonate Guvernului și structurile organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice desconcentrate și cele aflate în subordine, instituțiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator), autoritățile administrative autonome și unitățile cu autonomie financiară, în termen de pînă la 31 decembrie 2017, vor asigura implementarea Cerințelor minime obligatorii de securitate cibernetică.

4. Controlul asupra executării prezentei hotărîri se pune în sarcina Ministerului Tehnologiei Informației și Comunicațiilor.

Prim-ministru

PAVEL FILIP

CERINȚELE MINIME DE SECURITATE CIBERNETICĂ

I. Dispoziții generale

1. Cerințele minime de securitate cibernetică a sistemelor și resurselor informaționale, a echipamentelor și produselor program (în continuare – Cerințe) se aplică:

a) în cadrul Cancelariei de Stat, ministerelor, altor autorități administrative centrale subordonate Guvernului, inclusiv structurilor organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice desconcentrate și cele aflate în subordine, instituțiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator) (în continuare - instituții);

b) echipamentelor (hardware) și produselor program (software) existente în cadrul fiecărei instituții;

c) sistemelor informatice, resurselor și sistemelor informaționale existente în instituție (denumite în continuare - sisteme), precum și celor aflate la etapa de elaborare, testare și implementare.

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

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

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

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

4. În sensul prezentelor Cerințe, următoarele noțiuni principale semnifică:

cerințele minime de securitate cibernetică (CMSC) - include toate politicile, procedurile, planurile, procesele, practicile, rolurile, responsabilitățile, resursele și structurile care sunt folosite pentru a proteja și păstra intactă informația;

paravan de protecție (firewall) – un dispozitiv sau o serie de dispozitive configurate în așa fel încât să filtreze, să cripteze sau să intermedieze traficul între 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 folosire de programe de antivirus, în scop de protecție cibernetică;

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

- d) protecția echipamentelor și produselor program (calculatoare, software, sisteme de stocare a datelor, echipamente de rețea și alte echipamente tehnice;
- e) identificarea și remedierea vulnerabilităților;
- f) efectuarea copiilor de rezervă și stabilirea procedurilor de recuperare.

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

- a) Scopul și obiectivele;
- b) principiile de organizare internă a managementului de securitate cibernetică;
- c) analiza situației și vulnerabilităților (disponibilitate, integritate și confidențialitate a datelor, precum și analiza riscurilor și căilor de remediere;
- d) declarația managementului instituției susținere a scopului și principiilor securității cibernetice în instituție.

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

- a) Instruire în igiena și etica cibernetică (programe/cursuri de formare în domeniul securității cibernetice);
- b) 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);
- c) Măsurile de securitate privind activitatea personalului/companiilor externe cooptate (coordonarea responsabilităților, acorduri de nedivulgare, autorizație de acces, monitorizare, planul de contingență (intervență) pentru suspendarea operațiunilor de externalizare).

12. Regulamentele interne de securitate cibernetică prevăd:

- a) dezvoltarea, actualizarea, modificarea, mentenanța sistemelor informaționale;
- b) gestionarea activelor și facilităților de comunicații electronice și tehnologia informației;
- c) stocarea copiilor de rezervă a datelor, precum și procedurile de control;
- d) păstrarea datelor de acces, de jurnalizare a activităților;
- e) monitorizarea securității sistemului;
- f) reguli de gestionare a evenimentelor de securitate;
- g) proceduri de utilizare a datelor în cazuri excepționale (de urgență)
- h) proceduri de evaluare a securității cibernetice.

13. Procedurile de recuperare includ:

- a) stabilirea procedurilor privind copierea de rezervă și de recuperare în cazul unui incident de securitate cibernetică;
- b) descrierea acțiunilor măsurabile de recuperare;
- c) atribuirea responsabilităților pentru restabilirea funcționalităților;
- d) stabilirea procedurilor de notificare.

III. Cerințele minime de securitate cibernetică de nivelul 1

(utilizare TIC în activitatea instituției)

14. Controlul accesului

a) 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;

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

c) 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;

d) 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;

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

f) 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 parolei de o singură folosință, cu o valabilitate de 48 de ore din momentul transmiterii acestora;

g) sistemul trebuie să dispună de funcționalitatea ce nu permite utilizatorului salvarea parolelor, astfel încât la conectare ulterioară să nu poată intra în sistem fără introducerea parolei;

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

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

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

k) 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 odată la 6 luni;

l) 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.

15. Securitatea fizică

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

- b) Asigurarea condițiilor de încălzire, ventilare și aer condiționat a încăperilor specializate;
- c) Asigurarea accesului în spațiile specializate, strict conform competențelor;
- d) Asigurarea securității energetice, prin utilizarea unor dispozitive conforme normativelor în vigoare și cu protecție la suprasarcină;
- e) Asigurarea mentenanței adecvate, conform cerințelor tehnice;
- f) Evidența echipamentelor și produselor program, utilizare în cadrul instituției.

16. Securitatea operațională

- a) Echipamentele și produsele program trebuie să fie protejate ca să asigure operaționalitatea sistemelor;
- b) Pe calculatoarele conectate la rețeaua Internet, trebuie să fie instalat, cel puțin:
 - un sistem de operare cu actualizările curente aplicate;
 - program antivirus activat și actualizat;
 - paravan de protecție (firewall) activat;
 - instalare caracteristici de blocare automată a sistemului în caz de neutilizare a acestuia (screen saver, log-off).
- c) Controlul tehnic se efectuează periodic, conform regulamentului intern de securitate, și vizează:
 - Securitatea rețelelor, nodurilor și liniilor majore de interconectare cu rețele externe;
 - Evaluarea necesităților de instalare și utilizare a echipamentelor fără fir, conform regulamentului intern de securitate, securizarea conexiunilor fără fir (autorizarea echipamentelor și criptarea datelor);
 - Securitatea serverelor web, DNS și DHCP;
 - Securitatea serverelor cu baze de date (instalarea în zona Intranet, configurarea rețelei pentru a elimina camera pentru acces direct din rețeaua externă);
 - Securitatea echipamentelor de rețea (router, comutator, caracteristici de control al accesului);
 - Starea caracteristicilor de securitate cibernetică;
 - Administrarea pachetelor de actualizare a produselor program privind securitatea cibernetică;
 - Verificarea vulnerabilităților sistemelor și remedierea deficiențelor;
 - Cerințe privind securitatea la utilizarea rețelei Internet.
- d) Aplicarea cerințelor de securitatea cibernetică la utilizarea rețelelor:
 - Caracteristici ale echipamentelor și produselor program pentru gestionarea fluxului de la/către utilizatori, conform regulamentului intern de securitate;
 - Serviciile de rețea care nu sunt utilizate trebuie să fie dezactivate;
 - Echipamentele active de rețea trebuie configurate și testate astfel, încât să asigure izolarea rețelei private de rețelele adiacente.

e) Elaborarea planului de continuitate, care va asigura restaurarea caracteristicilor sistemului și a datelor, în caz de incident de securitate, care să includă:

- Procedura de efectuare a copiilor de rezervă (back-up) a datelor, aplicațiilor și sistemelor (automata/manuală, periodicitatea și durata disponibilității);

- Conținutul copiei de rezervă (date, aplicații, sisteme);

- Amplasarea copiei/copiilor de rezervă;

- Testarea periodică a copiilor de rezervă;

- Procedura de recuperare/restaurare a datelor, aplicațiilor și sistemelor;

- Procedura de constatare a necesității efectuării altor copii de rezervă.

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

g) Stabilirea cerințelor de securitate și restricții pentru echipamentele personale utilizate în cadrul instituției.

17. Schimb securizat de date și de comunicări

a) Elaborarea ghidului de utilizare a serviciilor sistemului de poștă electronică și obligarea personalului privind:

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

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

- verificarea și scanarea antivirus a anexelor la mesaje recepționate și a extensiilor acestora.

b) Interzicerea:

- redirectionării automate a mesajelor din poșta de serviciu spre alte conturi personale/private;

- utilizării poștei electronice de serviciu pentru a expedia sau redirectiona mesaje considerate obscene, amenințătoare, ofensatoare, calomnioase, defăimătoare, rasiste, pornografice, de hărțuire, mesaje de ură, remarci discriminatorii și alte mesaje anti-sociale;

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

- utilizării poștei electronice de serviciu pentru obținerea unui câștig material, în scopuri personale, politice sau de alt gen;

- distribuirea materialelor protejate de drepturi de autor;

- transmiterea informațiilor confidențiale prin mesaje electronice nesecurizate;

- utilizarea poștei electronice de serviciu pentru răspândirea virusilor de calculator, de infiltrare în sisteme, deteriorare sau distrugere a datelor, produse program și echipamente, sau ce duc la degradarea sau perturbarea performanței rețelei;

- ascunderea și încercarea de a ascunde identitatea atunci când este trimis un mesaj prin poșta electronică de serviciu.

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

Suplimentar cerințelor din Capitolul III „Cerințe minime de securitate cibernetică de nivelul 1”, în cazul instituțiilor ce prestează servicii bazate pe TIC, doar pentru infrastructura respectivă, se aplică următoarele cerințe avansate.

18. Controlul accesului

a) Parolele utilizatorilor de sistem trebuie să fie modificate nu mai târziu de 90 de zile calendaristice, cu limitarea posibilității de modificare manuală a acestora nu mai des de două ori în decursul a 24 de ore;

b) parolele trebuie să fie stabilite astfel, încât să nu coincidă cu oricare dintre cele cinci parole, utilizate anterior;

c) contul utilizatorului trebuie să fie blocat imediat, dacă 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;

d) 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 autentificare multifactorială și utilizarea unui canal securizat de comunicații;

e) accesul fizic la echipamentele care asigură funcționarea sistemului trebuie să fie permis de către instituție doar persoanelor autorizate;

f) instituția trebuie să asigure păstrarea pe o perioadă de cel puțin 6 luni, a înregistrărilor accesului în sistem, începând cu prima accesare a utilizatorului. Aceste date sînt păstrate într-un sistem aparte.

19. Securitatea fizică

a) 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 perioada de valabilitate a accesului și suspendarea acestuia în cazul eliberării din funcție.

b) Securitatea energetică, prevede implementarea măsurilor de protecție și control a 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.

c) Echipamentele utilizate în sistemul informatic trebuie amplasate și protejate astfel, încît să fie redus riscul deteriorării lor în cazul calamităților naturale și altor accidente;

d) 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;

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

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

20. Securitatea operațională

a) 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);

b) Instalarea/utilizarea registrului evenimentelor cu următoarele caracteristici:

- păstrarea datelor cel puțin pentru 12 luni;
- înregistrările activităților utilizatorilor în sistem sunt create cu indicarea corectă a timpului care trebuie să coincidă efectiv cu timpul universal coordonat (UTC);

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

- mesajul de eroare pentru utilizatorul de sistem conține doar informațiile minime necesare pentru acesta sau este repartizat manual către personalul de suport al sistemului pentru a-i ajuta să rezolve eroarea;

c) Reguli de utilizare de către instituție a dispozitivelor mobile, ce vor include:

- cerințe pentru protecția fizică și responsabilizarea utilizatorilor;
- aplicarea politicii de gestionare a componentelor produselor de program, inclusiv a pachetelor de actualizări;

- aplicarea politicii de gestionare a resurselor informaționale pentru echipamentele de rețea;

- prevederi privind controlul accesului;

- tehnici criptografice;

- protecția antivirus;

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

- aplicarea politicilor de gestiune a copiilor de rezervă.

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

e) Managementul evoluțiilor IT prevede implementarea unor proceduri care să ofere siguranța că sunt îndeplinite următoarele condiții:

- Descrierea procesului de modificări/aprobări a persoanelor autorizate, testărilor și rapoartelor planificate;

- Actualizările se efectuează la timp și sunt complete;
- Gestiunea fișelor de schimbări/intervenții;
- Actualizarea manualelor de instalare/utilizare, în concordanță cu ultima versiune de sistem;
- Gestiunea/evidența versiunilor produselor program utilizate și documentației tehnice.

f) Managementul mijloacelor de stocare externă prevede:

- Datele confidențiale sau importante, stocate pe suport amovibil sunt criptate;
- Multiplicarea copiilor se realizează la necesitate și pe dispozitive separate;
- Personalul ce utilizează mijloacele de stocare externă urmează a fi instruite corespunzător;
- La scoaterea din uz, datele de pe mijlocul de stocare se extrag, iar echipamentul se distruge.

g) 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;

h) Efectuarea separării sarcinilor pentru următoarele categorii de activități în domeniul TI:

- proiectarea și programarea sistemelor;
- administrarea și întreținerea sistemelor;
- introducerea datelor;
- securitatea cibernetică;
- administrarea bazelor de date;
- managementul modificărilor și dezvoltării sistemului informatic.

i) Efectuarea auditului intern de securitate, efectuat anual pînă la finele lunii ianuarie a anului următor de către subdiviziunile responsabile de tehnologia informației, verifică:

- Eliminarea de pe calculatoarele instituției conectate la Internet, a datelor și programelor care nu sînt necesare;

- Prezența paravanului de protecție. Dacă necesitățile cer conectarea directă la Internet cu riscuri minime, se utilizează includerea în configurație a unei protecții de tip "firewall" pentru a facilita controlul traficului între rețeaua entității și Internet, dar și pentru a stopa intruziunea pachetelor de date externe, neautorizate;

- Protecție împotriva virusilor informatici prin implementarea unei proceduri privind utilizarea unei soluții antivirus care să ofere: aplicarea acestora în toate serverele și stațiile de lucru; actualizarea fișierului de definiții antivirus; interdicția dezactivării antivirusului de către utilizatori la stația proprie de lucru; antivirusul scanează toate fișierele (pe server și pe stațiile de lucru) automat, în mod periodic;

- Detectare și corectare a altor modificări neautorizate a configurărilor, realizate de către utilizatori și ce sporesc riscurile de securitate cibernetică.

j) 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 sunt prezentate MTIC, în termen de o lună, împreună cu planul de remediere a deficiențelor depistate.

V. Cerințele minime de asigurare a securității cibernetice la achiziția sistemelor informaționale noi sau actualizarea celor existente

21. 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 non-funcționale, următoarele cerințe:

a) Suportul anumitor sisteme de securitate și de mentenanță (inclusiv înlăturarea lacunelor de securitate ale sistemului, într-o perioadă prestabilită);

b) Transmiterea către instituție a dreptului de autor asupra codul sursă a produselor program;

c) Stabilirea perioadei de timp în care se efectuează actualizările propriu zise;

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

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

f) Înainte de a pune în funcțiune un nou sistem, instituția trebuie să se asigure că caracteristicile de securitate ale acestuia funcționează conform cerințelor prestabilite, prin efectuarea de o terță parte a testelor respective;

g) Instituția asigură efectuarea periodică a auditului de securitate a sistemului, în conformitate cu documentația tehnică aprobată;

h) Dezvoltarea și testarea sistemului nu trebuie să fie sau să prezinte un pericol pentru integritatea datelor stocate în sistem.

VI. Cerințe de securitate la externalizarea administrării/mentenanței sistemelor

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

a) Prestatorul de servicii, în realizarea prevederilor contractuale, trebuie să urmeze reglementările interne de securitate cibernetică ale instituției;

b) descrierea serviciilor externalizate;

c) cerințe precise pentru volumul și calitatea serviciilor externalizate documentate ca Service Level Agreement (SLA);

d) drepturile și obligațiile instituției și prestatorului de servicii externalizate;

- dreptul instituției de a monitoriza continuu calitatea serviciilor furnizate;
- dreptul instituției pentru 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 și corectă a legilor și a regulamentelor;
- 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;
- obligația prestatorului extern de servicii de a furniza instituției informația privind monitorizarea continuă a calității serviciilor de externalizare prestate;
- dreptul de audit a prestatorului de serviciu, dacă au fost notificate non-conformități critice.

VII. Răspunsul la incidente, continuitatea proceselor și recuperarea

23. Planul de răspuns la incidente

a) Instituția trebuie să elaboreze și să pună în aplicare planul de răspuns de incidente cibernetice;

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

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

a) Implementarea procedurilor de efectuare a copiilor de rezervă și celor de recuperare;

b) Elaborarea și implementarea obiectivelor de recuperare, conform obiectivelor momentului de recuperare (OMR) și perioadei de recuperare (OPR).

25. Conformitatea cu cerințele interne și externe de securitate cibernetică:

a) Instituția actualizează planul său de acțiuni pentru asigurarea securității cibernetice, care precizează măsurile puse în aplicare și cele planificate.

b) Instituția asigură conformitatea sa cu cerințele externe de securitate cibernetică, prevăzute de legislație.

NOTĂ INFORMATIVĂ
la proiectul Hotărîrii de Guvern
privind aprobarea cerințelor minime de securitate cibernetică

În conformitate cu prevederile Hotărîrii Guvernului nr.857 din 31.10.2013 cu privire la Strategia națională de dezvoltare a societății informaționale "Moldova Digitală 2020", un obiectiv al cărui este și "Crearea condițiilor pentru sporirea gradului de securitate și încredere în spațiul digital", a fost elaborat și adoptat Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, aprobat prin Hotărîrea Guvernului nr. 811 din 29.10.2015.

Conform Planului de acțiuni, anexă la Program, obiectivul specific „Procesarea, stocarea și accesarea în siguranță a datelor, inclusiv a datelor de interes public” va fi realizat prin promovarea unei serii de acțiuni, printre care un rol aparte revine Cerințelor minime de securitate cibernetică.

Prezentele Cerințe minime de securitate cibernetică care urmează a fi aplicate în cadrul Cancelariei de Stat, ministerelor, altor autorități administrative centrale subordonate Guvernului, inclusiv structurilor organizaționale din sfera lor de competență (autoritățile administrative din subordine, serviciile publice descentralizate și cele aflate în subordine, instituțiile publice în care Cancelaria de Stat, ministerul sau altă autoritate administrativă centrală are calitatea de fondator). Aceste cerințe se aplică sistemelor și resurselor informaționale la etapa de testare, precum și sistemelor create pentru a fi implementate sau utilizate, la alte etape (de planificare, proiectare, dezvoltare) de elaborare a sistemului pentru a asigura un sistem adecvat de protecție cibernetică. Aceste cerințe nu se aplică în cazul sistemelor informaționale și rețelelor de comunicații speciale, atribuite la secretul de stat și celor ce conțin date cu caracter personal, care sunt reglementate prin acte speciale.

Cerințele minime de securitate cibernetică, după domeniul de aplicare, sînt de două categorii: nivelul 1 - de securitate cibernetică de bază (utilizare TIC în activitatea instituției) și nivelul 2 - de securitate cibernetică avansată (utilizare TIC în activitatea instituției și prestare servicii bazate pe TIC). Prezentul proiect conține prevederi de securitate pentru ambele nivele - prevederi privind controlul accesului, securitatea fizică și cea operațională, etc.

Un aspect important al Cerințelor vizează procedurile, responsabilitățile și reglementările interne: politica de securitate cibernetică, reglementările interne de securitate cibernetică, ghidul de utilizare a poștei electronice, planul de recuperare, etc.

Astfel, adoptarea prezentei Hotărîri de Guvern privind Cerințele minime de securitate cibernetică va contribui la colectarea, procesarea, stocarea și accesarea în siguranță a datelor, inclusiv a datelor de interes public, va delimita responsabilitățile și va reglementa procedurile interne în instituțiile publice pentru asigurarea gradului necesar de securitate cibernetică.

Ministru

S. Botnari

Vasile BOTNARI