

Aprobat:  
Serviciul de Informații și Securitate  
al Republicii Moldova  
ordinul nr. 13 din 3 aprilie 2006

Înregistrat:  
Ministerul Justiției  
al Republicii Moldova  
nr. de înregistrare 452 din 21 iunie 2006

\_\_\_\_\_ Ion URSU

\_\_\_\_\_ Victoria IFTODI

Anexa nr. 2  
la Ordinul directorului Serviciului  
de Informații și Securitate  
al Republicii Moldova  
nr. 13 din 3 aprilie 2006

## **Condițiile speciale de activitate a centrelor de certificare a cheilor publice**

### **I. Noțiuni generale**

1. Condițiile speciale de activitate a centrelor de certificare a cheilor publice (în continuare – condiții speciale) sînt elaborate în conformitate cu Legea nr. 264-XV din 15 iulie 2004 cu privire la documentul electronic și semnătura digitală și Hotărîrea Guvernului nr. 945 din 5 septembrie 2005 "Cu privire la centrele de certificare a cheilor publice".

2. Condițiile speciale stabilesc cerințele generale față de centrele de certificare și infrastructura acestora, organizarea procedurilor de bază ale centrelor de certificare, față de sistemul de gestionare a securității informaționale, precum și măsuri specifice în procedura de înregistrare, organizare și control al activității centrelor de certificare.

3. Condițiile speciale reprezintă un document de reglementare în domeniul semnăturii digitale și este obligatoriu pentru toate persoanele juridice care prestează servicii de certificare a cheilor publice și alte servicii ce țin de semnătura digitală.

4. În sensul prezentului document se definesc următoarele noțiuni:

*utilizatorul semnăturii digitale* – persoana fizică sau juridică, precum și dispozitivul sau aplicația care utilizează serviciile centrului de certificare;

*identificarea* – atribuirea unui identificator subiecților și obiectelor de acces și/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

*autentificarea* – verificarea apartenenței identificatorului atribuit subiectului de acces, confirmarea autenticității;

*integritatea* – certitudinea, necontradictorialitatea și actualitatea informației, protecția ei de distrugere și modificare neautorizată;

*accesibilitatea* – posibilitatea de a obține informația solicitată sau a accesa serviciul de informare într-o perioadă satisfăcătoare de timp;

*confidențialitatea* – protejarea informației contra divulgării neautorizate;

*mijloacele de protecție criptografică a informației (MPCI)* – mijloace tehnice, de program și tehnico-aplicative, sisteme și complexe de sisteme ce realizează algoritmi de conversie criptografică a informației, destinate să asigure integritatea și confidențialitatea informației în procesul de prelucrare, depozitare și transmitere a acesteia prin canalele de comunicații;

*lista certificatelor revocate* – lista certificatelor cheilor publice a căror valabilitate a fost suspendată sau a încetat înainte de expirarea termenului de valabilitate, întocmită de centrul de certificare;

*protecția tehnică și criptografică a informației* – protecția informației cu aplicarea metodelor matematice (criptografice) speciale, a mijloacelor de program, tehnice, tehnico-aplicative sau de alt gen, precum și a procedurilor tehnico-organizatorice;

*protecția informației de scurgeri* – ansamblu de măsuri îndreptate spre prevenirea răspândirii neautorizate a informației protejate prin canalele tehnice sau prin canalele secundare cu ajutorul mijloacelor tehnice speciale;

*protecția informației contra accesului neautorizat* – ansamblu de măsuri orientate spre prevenirea obținerii informației protejate de către subiectul interesat, cu încălcarea drepturilor sau regulilor de acces la informația protejată stabilite de actele juridice sau de proprietarul (deținătorul) informației;

*protecția informației contra acțiunilor neintenționate* – ansamblu de măsuri orientate spre prevenirea acțiunilor neintenționate, provocate de erorile utilizatorului, defectele mijloacelor tehnico-aplicative, fenomenele naturii sau alte cauze ce nu au ca scop direct modificarea informației, dar care duc la distorsiunea, distrugerea, copierea, blocarea accesului la informație, precum și la pierderea, distrugerea acesteia sau la defectarea suportului material al informației;

*politica de securitate* – totalitatea deciziilor documentate de administrare, îndreptate spre protejarea informației, a mijloacelor tehnice și de program ale sistemelor informaționale.

## **II. Serviciile și procedurile centrului de certificare**

5. Centrul de certificare prestează servicii obligatorii și neobligatorii în domeniul semnăturii digitale.

6. Serviciul de certificare a cheilor publice ale persoanelor fizice este un serviciu obligatoriu.

7. Centrul de certificare poate presta următoarele servicii neobligatorii:

a) certificarea cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al treilea (numai pentru centrele de certificare de nivelul al doilea);

b) certificarea cheilor publice ale serviciilor prestate în sfera informațională [servicii informaționale e-mail, VPN (Virtual Private Network), web etc.];

c) fixarea timpului de inițiere a evenimentelor, inclusiv fixarea timpului de semnare a documentului electronic;

d) alte servicii în domeniul semnăturii digitale.

8. În procesul prestării serviciilor de certificare a cheilor publice ale persoanelor fizice, centrul de certificare trebuie să asigure realizarea următoarelor proceduri:

a) înregistrarea persoanei fizice;

b) crearea (emiterea) certificatului cheii publice a persoanei fizice;

c) suspendarea valabilității certificatului cheii publice a persoanei fizice;

- d) restabilirea valabilității certificatului cheii publice a persoanei fizice;
- e) revocarea certificatului cheii publice a persoanei fizice;
- f) publicarea certificatelor cheilor publice;
- g) distribuirea informației privind certificatele suspendate și revocate (listelor certificatelor revocate).

9. Centrul de certificare asigură procesul de administrare (gestionare) a certificatelor cheilor publice prin realizarea complexă a procedurilor specificate.

### **III. Cerințele generale referitoare la centrul de certificare**

10. Obiectele utilizate de către centrul de certificare trebuie să aparțină acestuia cu titlu de proprietate, arendă, administrare sau folosință.

11. Centrul de certificare trebuie să utilizeze mijloace de semnătură digitală care posedă certificat de conformitate, eliberat conform prevederilor legislației în vigoare.

12. Organizarea regimului intern de activitate al centrului de certificare trebuie să excludă posibilitatea accesului fizic neautorizat la mijloacele semnăturii digitale, utilizarea sau modificarea neautorizată a acestora.

13. Centrul de certificare trebuie să creeze condițiile necesare pentru asigurarea securității cheilor publice și private ale persoanelor împuternicite ale centrului de certificare și a registrului certificatelor cheilor publice.

14. Centrul de certificare trebuie să asigure utilizarea cheii private a persoanei împuternicite a centrului de certificare numai pentru semnarea certificatelor cheilor publice și a listelor certificatelor revocate emise de către centrul de certificare.

15. Centrul de certificare trebuie să excludă posibilitatea de utilizare a cheii private a persoanei împuternicite a centrului de certificare dacă are motive să presupună că a fost încălcată confidențialitatea respectivei chei private.

16. Centrul de certificare trebuie să elaboreze și să aprobe politica de certificare, care să includă un set de reguli ce stabilesc utilizarea certificatului emis de centrul de certificare conform cerințelor de securitate stabilite.

17. Centrul de certificare trebuie să elaboreze și aprobe Regulamentul centrului de certificare, care să stabilească condițiile organizatorice, tehnice și de alt nivel ale activității centrului de certificare în procesul de prestare a serviciilor de certificare a cheilor publice.

18. Regulamentul centrului de certificare trebuie să conțină:

- a) lista serviciilor prestate de centrul de certificare și modalitatea de prestare a acestora;
- b) funcțiile, obligațiile și drepturile centrului de certificare;
- c) drepturile și obligațiile utilizatorilor semnăturii digitale;
- d) obligațiile financiare ale centrului de certificare;
- e) responsabilitățile părților;
- f) activitățile tehnico-organizatorice de bază de asigurare a securității centrului de certificare, inclusiv politica de confidențialitate;
- g) procedurile centrului de certificare;
- h) ordinea de publicare și distribuire a informației;

- i) modalitatea de accesare a resurselor informaționale ale centrului de certificare;
- j) modul de arhivare a informației documentate;
- k) procedurile de gestionare a cheilor persoanelor împuternicite ale centrului de certificare;
- l) algoritmul acțiunilor în cazul compromiterii cheii private a persoanei împuternicite a centrului de certificare și a utilizatorului semnăturii digitale;
- m) descrierea formatelor de date aprobate de către centrul de certificare;
- n) structura certificatului cheii publice a persoanei împuternicite a centrului de certificare;
- o) structura certificatelor cheilor publice ale utilizatorilor semnăturii digitale;
- p) structura listei certificatelor revocate;
- q) ordinea de sincronizare a timpului;
- r) modalitatea de soluționare a situațiilor litigioase în domeniul aplicării semnăturii digitale;
- s) ordinea de înștiințare a utilizatorilor semnăturii digitale privind politica de certificare și despre conținutul Regulamentului centrului de certificare.

19. Politica de certificare și Regulamentul centrului de certificare trebuie să corespundă recomandărilor IETF (Internet Engineering Task Force) RFC 3647 (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework).

20. Centrul de certificare trebuie să excludă posibilitatea divulgării informației de înregistrare a utilizatorilor semnăturii digitale cu excepția informației ce se utilizează pentru identificarea certificatelor cheilor publice ale acestora și care este publicată prin includerea acesteia în certificatele utilizatorilor semnăturii digitale.

21. Regimul de confidențialitate în cazul operării cu informația încredințată sau care a devenit cunoscută centrului de certificare în activitatea sa trebuie să asigure:

- a) limitarea numărului persoanelor cu funcții de răspundere cu drept de acces la informația confidențială;
- b) ordinea de admitere controlată a persoanelor cu funcții de răspundere la realizarea activităților legate de informația confidențială;
- c) delimitarea funcțională a responsabilităților persoanelor cu funcții de răspundere;
- d) identificarea și autentificarea utilizatorilor semnăturii digitale cu utilizarea mijloacelor moderne de autentificare și a protocoalelor criptografice;
- e) delimitarea accesului subiecților la diferite obiecte și/sau la funcțiile speciale ale centrului de certificare pe baza identificării subiecților și a delimitării funcționale a acestora;
- f) securitatea păstrării, prelucrării și transmisiei informației confidențiale prin intermediul canalelor de comunicații.

22. Centrul de certificare trebuie să asigure administrarea accesului subiecților la diferite obiecte și/sau la funcțiile speciale ale centrului de certificare pe baza identificării subiecților și a delimitării funcționale a acestora.

23. Centrul de certificare trebuie să asigure copiarea de rezervă, păstrarea și restabilirea informației critice pentru activitatea sa, precum și instalarea în caz de necesitate a resurselor tehnice suplimentare sau de rezervă.

24. Centrul de certificare trebuie să dispună de personal calificat suficient pentru funcționarea și asigurarea securității centrului de certificare.

25. Centrul de certificare trebuie să-și realizeze funcțiile pe baza principiului delimitării privilegiilor (responsabilităților) persoanelor cu funcții de răspundere: administratorul înregistrării, administratorul certificare, administratorul securitate și administratorul sistem.

26. Administratorul înregistrării este responsabil de corectitudinea (autenticitatea) informației de completare a certificatului cheii publice și înregistrarea titularilor certificatelor cheilor publice în procesul creării, suspendării sau restabilirii valabilității și revocării certificatelor cheilor publice.

27. Administratorul certificare (persoana împuternicită a centrului de certificare) este responsabil pentru crearea, suspendarea sau restabilirea valabilității și revocarea certificatelor cheilor publice, ținerea registrului certificatelor cheilor publice, păstrarea și utilizarea în siguranță a cheii sale private.

28. Administratorul securitate este responsabil de funcționarea corespunzătoare a sistemului complex de protecție a informației, precum și de elaborarea și implementarea politicii de securitate a centrului de certificare.

29. Administratorul sistem este responsabil de administrarea, funcționarea corespunzătoare și asigurarea securității complexului tehnic de program al centrului de certificare.

30. În caz de necesitate în centrul de certificare pot fi înființate funcții suplimentare, în special de operatori.

31. Operatorii realizează activități de deservire zilnică a complexului tehnic de program al centrului de certificare (copierea și restabilirea sistemului, gestionarea arhivelor, introducerea informației etc.).

32. Centrul de certificare trebuie să excludă cumularea funcțiilor de administrator înregistrării, administrator certificare, administrator securitate, administrator sistem și operator.

33. Centrul de certificare trebuie să sincronizeze activitatea serviciilor sale, inclusiv a mijloacelor tehnice și de program conform destinației, cu Timpul Universal Coordonat (UTC). Se recomandă utilizarea a două surse independente UTC. Este permisă sincronizarea cu Greenwich Mean Time – GMT.

#### **IV. Cerințele referitoare la procedurile de bază ale centrului de certificare**

##### ***Secțiunea 1. Cerințele față de procedura de înregistrare a persoanei fizice***

34. Persoanele fizice sînt înregistrate de către administratorul înregistrării, care administrează datele titularului certificatului cheii publice.

35. Administratorul înregistrării efectuează identificarea persoanei fizice ce a înaintat cererea de certificare a cheii sale publice în conformitate cu procedurile aprobate de către centrul de certificare.

36. Administratorul înregistrării trebuie să stabilească:

a) corespunderea procesului de completare și înaintare a cererii cu prevederile Legii cu privire la documentul electronic și semnătura digitală, ale Regulamentului centrului de certificare și ale altor documente normative în domeniul semnăturii digitale;

b) autenticitatea și valabilitatea informației prezentate în cerere;

c) corespunderea informației prezentate în cererea sub formă de document electronic și a celei din cererea sub formă de document pe suport de hârtie;

d) respectarea drepturilor persoanelor terțe.

37. Administratorul înregistrării trebuie să se asigure că persoana fizică ce a prezentat cererea de certificare a cheii publice este posesorul cheii private corespunzătoare.

38. Documentele electronice ale administratorului înregistrării trebuie să fie semnate cu semnătură digitală, să includă amprenta timpului, care stabilește momentul creării documentului electronic, și să fie transmise utilizând sistemele ce asigură confidențialitatea mesajelor.

39. Centrul de certificare trebuie să asigure protecția informației confidențiale a titularilor certificatelor cheilor publice.

### ***Secțiunea a 2-a. Cerințele față de procedura de certificare a cheii publice***

40. Centrul de certificare creează și emite certificate ale cheilor publice în conformitate cu procedurile aprobate de centrul de certificare.

41. Centrul de certificare trebuie să elaboreze și să aprobe politica și procedurile de certificare a cheilor publice în conformitate cu normele tehnice stabilite în domeniul semnăturii digitale.

42. Certificatul cheii publice a persoanei fizice este creat de către administratorul certificare (persoana împuternicită a centrului de certificare).

43. Administratorul certificare trebuie să verifice integritatea și autenticitatea datelor transmise de către administratorul înregistrării, precum și corespunderea acestora cu standardul certificatelor cheilor publice stabilit.

44. Centrul trebuie să asigure autenticitatea informației care se conține în certificatul cheii publice, precum și integritatea certificatului.

45. Certificatul cheii publice trebuie să corespundă profilurilor aprobate în centrul de certificare, corespunzătoare politicii de certificare.

46. Centrul de certificare trebuie să înscrie certificatul cheii publice în registrul certificatelor nu mai târziu de data și ora începerii termenului de valabilitate a certificatului.

47. Cheia privată a administratorului certificare trebuie să fie utilizată numai pentru semnarea certificatelor cheilor publice și a listelor certificatelor revocate (CRL) emise de acesta.

***Secțiunea a 3-a. Cerințele față de procedurile de suspendare și restabilire a valabilității și de revocare a certificatului cheii publice***

48. Centrul de certificare suspendă, restabilește valabilitatea sau revocă certificatul cheii publice în cazurile stabilite de actele normative în domeniul semnăturii digitale.

49. Centrul de certificare trebuie să elaboreze și să aprobe procedurile de suspendare, restabilire a valabilității și revocare a certificatelor cheii publice în conformitate cu normele tehnice stabilite din domeniul semnăturii digitale.

50. Centrul de certificare trebuie să elaboreze și să aprobe proceduri sigure de autentificare a persoanei ce a declarat intenția de a suspenda, restabili valabilitatea sau de a revoca certificatul său al cheii publice, precum și proceduri de confirmare a valabilității cererii de suspendare, restabilire a valabilității sau revocare a certificatului cheii publice.

51. Centrul de certificare suspendă imediat valabilitatea certificatului cheii publice dacă are motive să presupună că a fost încălcată confidențialitatea cheii private a titularului certificatului sau informația înscrisă în certificatul cheii publice nu corespunde realității.

52. Centrul de certificare revocă certificatul cheii publice în cazul stabilirii încălcării confidențialității cheii private a titularului certificatului sau a neveridicității datelor incluse în certificatul cheii publice.

53. Suspendarea, restabilirea valabilității și revocarea certificatului cheii publice se efectuează de către administratorul certificare sub supravegherea obligatorie a administratorului securitate sau a altei persoane cu funcții de răspundere, numită de conducătorul centrului de certificare.

54. Centrul de certificare trebuie să înscrie datele despre certificatul suspendat sau revocat în lista certificatelor revocate în decursul a 3 ore de lucru, indicând data și timpul includerii, cauza suspendării sau revocării acestuia.

55. Centrul de certificare trebuie să excludă posibilitatea restabilirii valabilității certificatului cheii publice revocat.

56. Certificatul cheii publice a cărui valabilitate a fost restabilită se exclude din lista certificatelor revocate în maxim 3 ore de lucru.

57. Centrul de certificare trebuie să asigure o procedură de emiteră la timp a listei reînnoite a certificatelor revocate.

58. Centrul de certificare trebuie să elaboreze și să aprobe procedura de informare a titularului certificatului cheii publice despre suspendarea, restabilirea valabilității sau revocarea certificatului.

***Secțiunea a 4-a. Cerințele față de procedurile de publicare a certificatelor cheilor publice și distribuire a informației referitoare la certificatele cheilor publice suspendate sau revocate***

59. Distribuirea (publicarea) certificatelor cheilor publice se efectuează în conformitate cu procedurile stabilite de centrul de certificare, iar accesul persoanelor terțe poate fi limitat dacă acest fapt este solicitat de titularul certificatului.

60. Centrul de certificare trebuie să elaboreze și să aprobe politica de control al accesului la certificatele cheilor publice emise de centrul de certificare.

61. Accesul la certificatele cheilor publice trebuie să fie acordat numai persoanelor ce au acest drept, conform regulilor stabilite de politica de securitate a centrului de certificare sau de către titularii certificatelor.

62. Centrul de certificare trebuie să ofere oricărei persoane informația referitoare la statutul certificatelor cheilor publice.

63. Centrul de certificare trebuie să prezinte informația referitoare la statutul certificatelor cheilor publice în regim de timp real (on-line), precum și pe alte căi stabilite de centrul de certificare, inclusiv prin distribuirea listelor certificatelor revocate pentru abonați (off-line).

64. Centrul de certificare trebuie să asigure integritatea și autenticitatea mesajelor în procesul de verificare a statutului certificatelor cheilor publice. Toate răspunsurile referitoare la starea certificatelor trebuie semnate cu semnătura digitală a persoanei împuternicite a centrului de certificare.

65. Centrul de certificare poate cere ca persoanele terțe să semneze cu semnătura digitală solicitările referitoare la statutul certificatelor cheilor publice.

66. Centrul de certificare poate răspunde solicitărilor referitoare la statutul certificatului cheii publice utilizând datele reînnoite în timpul ultimei înștiințări a utilizatorilor.

67. Centrul de certificare trebuie să facă publice certificatele cheilor publice ale persoanelor împuternicite ale centrului.

68. Informația inclusă în registrul certificatelor cheilor publice trebuie să fie protejată contra accesului neautorizat, modificării sau distrugerii.

69. Centrul de certificare trebuie să stabilească modalitățile de acces cu drept de înregistrare sau modificare a registrului certificatelor cheilor publice pentru persoanele ce au acest drept conform obligațiilor sale de serviciu.

70. Centrul de certificare trebuie să utilizeze mecanisme de autentificare a subiecților, care au acces la informația corespunzătoare din registrul certificatelor cheilor publice.

## **V. Cerințele referitoare la infrastructura centrului de certificare**

### ***Secțiunea 1. Cerințele referitoare la încăperi***

71. Încăperile centrului de certificare trebuie să asigure funcționarea stabilă a complexului tehnic de program, a sistemelor de telecomunicații și a altor componente tehnice, a sistemelor de energie electrică, termică și de apeduct, de aer condiționat, antiincendiar, să asigure protecția personalului și să contribuie la prevenirea sustragerii, pierderii, modificării neautorizate a datelor, precum și a distrugerii acestora sau a mijloacelor tehnico-aplicative.

72. Încăperile centrului de certificare trebuie să corespundă cerințelor normelor de igienă, securitate a muncii și protecție a mediului înconjurător, stabilite de legislația în vigoare.

73. Încăperile centrului de certificare trebuie să fie amplasate în perimetrul de securitate (perimetru unde are drept de acces numai personalul organizației a cărei parte este centrul de certificare) și să fie echipate corespunzător cu cerințele de asigurare a securității.

74. Din categoria încăperilor cu regim special (în continuare – încăperi speciale) ale centrului de certificare fac parte încăperile unde se instalează mijloacele tehnice de bază ale complexului tehnic de program (încăperi pentru servere), unde se păstrează suporturile materiale ce conțin: copiile de rezervă ale registrului certificatelor cheilor publice, copiile de rezervă ale resurselor de sistem și de program, cheile private ale angajaților centrului de certificare sau cheile secrete ale altor sisteme criptografice ale centrului de certificare.

75. Încăperile speciale ale centrului de certificare trebuie:

a) să corespundă condițiilor de maximă securitate, stabilite de prezentele condiții speciale, pentru asigurarea securității fizice și protecției tehnice a informației;

b) să fie dotate cu mijloace autonome și sisteme automate de semnalizare antiincendiu, stingere a incendiului și înlăturare a fumului conform normativelor NCM.E.03.03-2003 "Dotarea clădirilor și instalațiilor cu sisteme autonome de semnalizare și stingere a incendiilor" și NCM.E.03.05-2004 "Instalații autonome de stingere și semnalizare a incendiilor. Normativ pentru proiectare";

c) să corespundă cerințelor în vigoare în Republica Moldova privind proiectarea și exploatarea rețelei electrice, conform normelor cuprinse în Regulile de instalare a dispozitivelor electrice, Regulile privind exploatarea tehnică a dispozitivelor electrice ale consumatorilor și Regulile privind tehnici de securitate la exploatarea dispozitivelor electrice ale consumatorilor;

d) să asigure funcționarea mijloacelor tehnice principale pentru o perioadă de cel puțin 30 minute din momentul stopării furnizării energiei electrice de la sursa de bază;

e) să fie echipate cu mijloace de ventilare și condiționare a aerului care posedă certificat de conformitate, eliberat conform prevederilor legislației în vigoare.

76. În încăperile destinate pentru păstrarea documentației și a copiilor de rezervă ale registrului certificatelor cheilor publice trebuie să fie instalate dulapuri metalice.

### ***Secțiunea a 2-a. Cerințele referitoare la complexul tehnic de program***

77. Complexul tehnic de program al centrului de certificare trebuie să asigure executarea de către centru a funcțiilor de certificare a cheilor publice și să corespundă normelor tehnice în domeniul semnăturii digitale.

78. Exploatarea complexului tehnic de program al centrului de certificare trebuie efectuată conform cerințelor stabilite de asigurare a securității.

79. Mijloacele tehnice ale complexului tehnic de program, utilizate de centrul de certificare, trebuie să fie proprietate a centrului, fie închiriate sau primite în folosință pe baza unui contract scris.

80. Fiecare mijloc tehnic trebuie să fie înregistrat și testat în privința posibilității de utilizare și fiecare mijloc tehnic sau de program trebuie să fie însoțit de documentația tehnică.

81. Capacitatea de funcționare a mijloacelor tehnice trebuie verificată periodic pe parcursul întregului ciclu de exploatare, iar rezultatele verificării vor fi consemnate.

82. Toate mijloacele tehnice trebuie să fie asigurate cu posibilități de reparare. Pentru dispozitivele ce necesită deservire tehnică periodică trebuie elaborate instrucțiuni și grafice de deservire tehnică. Toate echipamentele și dispozitivele de control-măsurare trebuie întreținute în condiții ce asigură integritatea acestora.

83. Complexul tehnic de program al centrului de certificare trebuie să asigure posibilitatea copierii de rezervă și păstrării informației critice pentru activitatea centrului de certificare, restabilirii operative și complete a informației în caz de refuz al deservirii, de incidente sau erori în sisteme, precum și instalării, în caz de necesitate, a resurselor tehnice suplimentare sau de rezervă.

84. În activitatea sa centrul de certificare trebuie să utilizeze numai soft licențiat sau liber distribuit.

85. Centrul de certificare este obligat să asigure administrarea complexului tehnic de program sau a subsistemelor acestuia numai de către persoane împuternicite să administreze, precum și să excludă modificările neautorizate ale configurațiilor echipamentului, ale setărilor de sistem, ale algoritmilor de funcționare a mijloacelor de program, modificarea fluxurilor informaționale sau proceselor susținute.

### ***Secțiunea a 3-a. Cerințele referitoare la personal***

86. Centrul de certificare trebuie să dispună de un număr de angajați, cu calificare, experiență și pregătire profesională care să permită realizarea întregului spectru de funcții privind prestarea serviciilor în domeniul semnăturii digitale.

87. Încadrarea personalului centrului de certificare trebuie să fie prezentată în structura organizatorică și nomenclatorul de funcții, aprobate de conducătorul persoanei juridice. Nivelul de calificare a fiecărui specialist trebuie dovedit documentar.

88. Pentru fiecare specialist al centrului de certificare trebuie definite condițiile concrete privind nivelul de studii, de cunoștințe tehnice și experiență de lucru. De asemenea vor fi stabilite obligațiile de serviciu, funcțiile, drepturile, responsabilitățile și cerințele față de regimul de confidențialitate.

89. Fiecare angajat al centrului de certificare este obligat să cunoască și să îndeplinească obligațiile sale de serviciu, periodic să-și sporească nivelul de calificare, să studieze profesiile complementare profilului activității de bază.

90. Centrul de certificare trebuie să verifice și să evalueze periodic nivelul de calificare a specialiștilor săi și să asigure sporirea acestuia.

91. În cazul lipsei specialiștilor proprii pentru realizarea activităților specifice, centrul de certificare poate implica angajați ai altor organizații, cu asigurarea cerințelor de securitate stabilite.

92. Angajații centrului de certificare trebuie să semneze clauze de confidențialitate, în condițiile articolului 53 al Codului muncii al Republicii Moldova, precum și, după caz, angajamente de nedivulgare a secretului comercial, valabile atât pentru perioada contractului individual de muncă încheiat, cât și pentru perioada stabilită în contract după expirarea acțiunii acestuia.

## **VI. Cerințele referitoare la gestionarea resurselor informaționale ale centrului de certificare**

### ***Secțiunea 1. Cerințele referitoare la resursele informaționale***

93. Resursele informaționale ale centrului de certificare sînt registrul certificatelor cheilor publice și documentele de serviciu ale centrului de certificare.

94. Resursele informaționale ale centrului de certificare sînt ținute sub formă de documente pe suport de hîrtie și sub formă de documente electronice, păstrate pe suporturi materiale.

95. Resursa informațională principală a centrului de certificare este registrul certificatelor cheilor publice, care reprezintă un ansamblu de documente electronice și documente pe suport de hîrtie incluzînd:

- a) cereri de certificare a cheilor publice ale utilizatorilor semnăturii digitale;
- b) certificatele cheilor publice ale utilizatorilor semnăturii digitale;
- c) decizii de suspendare, restabilire a valabilității sau revocare a certificatelor cheilor publice ale utilizatorilor semnăturii digitale;
- d) certificatele cheilor publice ale persoanelor împuternicite ale centrului de certificare de nivelul al treilea (numai pentru centrele de certificare de nivelul al doilea);
- e) cereri de suspendare, restabilire a valabilității sau revocare a certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare de nivelul al treilea (numai pentru centrele de certificare de nivelul al doilea);
- f) listele certificatelor revocate.

96. Documentația centrului de certificare trebuie să corespundă standardului internațional ISO 15489 "Informația și documentația – gestionarea documentației".

### ***Secțiunea a 2-a. Cerințele față de păstrarea, în formă arhivată, a resurselor informaționale***

97. În formă arhivată vor fi păstrate următoarele resurse informaționale ale centrului de certificare:

- a) registrul certificatelor cheilor publice;
- b) jurnale de audit al complexului tehnic de program;
- c) alte tipuri de documente stabilite de centrul de certificare.

98. Termenul de păstrare în formă arhivată a registrului certificatelor cheilor publice va fi de cel puțin 10 ani din momentul revocării ultimului certificat inclus în registru.

99. Pregătirea pentru distrugere și efectuarea distrugerii documentelor arhivate se realizează de o comisie, formată din angajații centrului de certificare, în conformitate cu legislația în vigoare.

100. Lucrările de pregătire pentru distrugere și de distrugere a documentelor ce nu sînt supuse arhivării se efectuează de către angajații centrului de certificare ce gestionează documentele, în modul stabilit de conducătorul centrului de certificare.

### ***Secțiunea a 3-a. Cerințele față de asigurarea accesului la resursele informaționale***

101. Centrul de certificare asigură accesul utilizatorilor semnăturii digitale la registrul certificatelor cheilor publice prin intermediul:

- a) resurselor electronice oficiale ale centrului de certificare (portalul web);
- b) poștei electronice;
- c) rezolvării solicitărilor utilizatorilor semnăturii digitale conform procedurilor aprobate de centrul de certificare.

102. Accesul la documentele din arhivă ale centrului de certificare se realizează în conformitate cu legislația în vigoare.

## **VII. Cerințele referitoare la asigurarea securității centrului de certificare**

### ***Secțiunea 1. Cerințele referitoare la sistemul de securitate***

103. Obiectivele de bază privind asigurarea securității centrului de securitate sînt:

a) protecția informației confidențiale la depozitarea, prelucrarea și transmiterea acesteia (chei criptografice, mijloace de protecție criptografică a informației, date personale protejate conform legislației în vigoare, informație despre parole etc.);

b) verificarea integrității informației confidențiale și publice (informația despre titulari inclusă în certificatele cheilor publice, informația despre certificatele cheilor publice suspendate sau revocate, componentele aplicative distribuite liber și documentele aferente etc.);

c) verificarea integrității componentelor de program și de aparataj ale complexului tehnic de program;

d) asigurarea continuității în activitate;

e) asigurarea securității fizice a centrului de certificare.

104. Sistemul de securitate a centrului de certificare trebuie:

a) să protejeze informația referitor la titularii certificatelor cheilor publice prin intermediul asigurării confidențialității, integrității și asigurării accesului securizat la registrul certificatelor cheilor publice;

b) să asigure securitatea infrastructurii și a resurselor informaționale ale centrului de certificare;

c) să stabilească responsabilități referitor la securitatea informațională în centrul de certificare;

d) să minimizeze riscurile referitoare la utilizarea tehnologiilor informaționale;  
e) să asigure capacitatea centrului de certificare de a continua activitatea în cazuri excepționale sau alte situații critice (asigurarea continuității activității centrului de certificare).

105. Ansamblul măsurilor și al mijloacelor de protecție a informației în centrul de certificare trebuie să includă următoarele subsisteme:

a) subsistemul de protecție criptografică a informației, care include mijloacele de protecție criptografică a informației;

b) subsistemul de protecție a informației contra accesului neautorizat;

c) subsistemul de audit activ al securității informaționale a centrului;

d) subsistemul de detectare a intruziunilor;

e) subsistemul de protecție a informației contra acțiunilor neintenționate, inclusiv subsistemul de copiere de rezervă și arhivare a datelor;

f) subsistemul de asigurare a integrității informației, componentelor de program și de aparataj ale complexului tehnic de program al centrului de certificare, inclusiv prin metode criptografice;

g) subsistemul de asigurare a accesibilității, inclusiv subsistemul de asigurare a continuității funcționării complexului tehnic de program al centrului de certificare;

h) subsistemul de protecție a echipamentului complexului tehnic de program al centrului de certificare contra scurgerii de informații prin canalele tehnice și cele auxiliare;

i) subsistemul securității fizice.

106. Centrul de certificare trebuie să elaboreze condițiile de asigurare a securității proprii, criteriile și indicatorii de evaluare a nivelului de securitate, în concordanță cu care realizează activități și implementează mijloace concrete de protecție a informației.

107. Orice funcție a centrului de certificare poate fi delegată persoanelor terțe numai în condițiile când se respectă activitatea securizată a centrului de certificare.

108. Centrul de certificare trebuie să elaboreze și să aprobe procedurile interne de activitate, care să asigure funcționarea securizată a centrului de certificare.

109. Orice situație de forță majoră care poate influența în mod negativ realizarea procedurilor obligatorii ale centrului de certificare trebuie adusă la cunoștința titularilor certificatelor cheilor publice.

110. Centrul de certificare trebuie să elaboreze și să aprobe politica de securitate a centrului de certificare, care va reflecta viziunea asupra problemei securității informaționale a centrului de certificare, ansamblul de măsuri pentru asigurarea acesteia, responsabilitățile angajaților și mecanismele de control al stării securității informaționale.

111. Politica de securitate trebuie să asigure respectarea regulilor, standardelor și normelor general acceptate în domeniul securității informaționale și trebuie să includă:

a) categoriile resurselor centrului de certificare cu indicarea nivelului necesar de securitate pentru fiecare categorie;

b) analiza riscurilor centrului de certificare, ce pot apărea la utilizarea tehnologiilor informaționale și de telecomunicații;

- c) modelul de securitate a centrului de certificare;
- d) alegerea unui sistem complex de asigurare a securității centrului de certificare;
- e) principalele măsuri tehnico-organizatorice necesare pentru asigurarea securității centrului de certificare;
- f) condiții impuse mijloacelor tehnice de protecție a informației;
- g) enumerarea mijloacelor tehnice de protecție a informației;
- h) planul de acțiuni privind menținerea regimului de securitate a centrului de certificare, inclusiv planurile de continuitate în activitate;
- i) responsabilitățile personalului centrului de certificare privind asigurarea securității;
- j) proceduri de control al centrului de certificare privind respectarea condițiilor de securitate;
- k) procedura de aducere la cunoștința utilizatorilor semnăturii digitale a Regulamentului centrului de certificare și a politicii de securitate, de acceptare și asumare a obligațiilor de respectare a prevederilor Regulamentului și a politicii de securitate de către utilizatori;
- l) înștiințarea utilizatorilor semnăturii digitale despre nivelul de securitate a centrului de certificare.

112. Centrul de certificare trebuie să elaboreze și să aprobe sistemul de acordare a drepturilor de acces la resursele centrului de certificare, conform procedurilor de acces stabilite.

113. Centrul de certificare trebuie să analizeze toate componentele infrastructurii proprii (resurse aplicative și tehnice, mijloace de protecție a informației etc.) din punctul de vedere al riscurilor, să planifice și să realizeze activități de minimizare și evitare a riscurilor depistate.

114. Centrul de certificare trebuie să implementeze instrumente automatizate de analiză a sistemelor informaționale și de telecomunicații, precum și a proceselor de afaceri ale centrului de certificare, pentru depistarea vulnerabilităților în sistemul de securitate.

115. Centrul de certificare trebuie să elaboreze și să aprobe planul de acțiuni pentru asigurarea continuității activității, plan care va fi analizat și revizuit periodic pe baza analizei activității curente și rezultatelor testării în diferite situații excepționale posibile.

### ***Secțiunea a 2-a. Cerințele de asigurare a securității fizice***

116. Centrul de certificare trebuie să creeze și să mențină sistemul de securitate fizică care să asigure protecția infrastructurii, a resurselor informaționale și a personalului centrului, să fie flexibil în cazul modificării cerințelor de securitate înaintate, să permită adăugarea de noi funcționalități și să fie simplu în utilizare.

117. Sistemul de securitate fizică a centrului de certificare trebuie să includă următoarele subsisteme:

- a) gestionarea accesului la diferite obiecte fizice;
- b) depistarea intruziunilor neautorizate la obiectele fizice;

- c) gestionarea, analiza și înregistrarea informației;
- d) protecția tehnică și de inginerie (protecția pasivă);
- e) înștiințarea și asigurarea conexiunii în caz de situații excepționale.

118. Centrul de certificare trebuie să stabilească și să precizeze responsabilitățile angajaților legate de asigurarea securității fizice.

119. Informația privind amplasarea subsistemelor complexului tehnic de program al centrului de certificare este confidențială.

120. Echipamentul special și tehnic de inginerie, protecția și regimul de acces în încăperile speciale ale centrului de certificare trebuie să asigure securitatea informației confidențiale și a cheilor criptografice, accesul controlat în aceste încăperi, precum și accesul la mijloacele tehnice și cheile criptografice.

121. Centrul de certificare trebuie să-și clasifice încăperile cu regim special de acces, să stabilească reguli de acces și să aprobe lista persoanelor cărora le este permis accesul în aceste încăperi.

122. Accesul angajaților centrului de certificare în încăperile speciale se efectuează conform instrucțiunilor și ordinelor în vigoare în centrul de certificare.

123. Accesul fizic în încăperile speciale ale centrului de certificare trebuie să fie posibil numai în urma controlului dublu și conform drepturilor de acces stabilite.

124. Angajații centrului de certificare care au acces în încăperile speciale poartă răspundere personală pentru permiterea accesului persoanelor terțe în aceste încăperi.

125. Încăperile speciale vor fi dotate în mod obligatoriu cu sisteme de control al accesului și monitorizare video, care trebuie să permită supravegherea accesului persoanelor în aceste încăperi.

126. Încăperile speciale se dotează în mod obligatoriu cu sisteme de pază pe mai multe linii și semnalizare de alarmă, în conformitate cu normele metodologice și tehnice de proiectare și montare a sistemelor de alarmare împotriva efracției, aprobate prin Hotărîrea Guvernului nr. 667 din 8 iulie 2005 "Cu privire la măsurile de realizare a Legii nr. 283-XV din 4 iulie 2003 privind activitatea particulară de detectiv și de pază".

127. La amplasarea mijloacelor tehnice, centrul de certificare trebuie să asigure protecția lor contra accesului neautorizat, furt, incendii, inundații, câmpuri electromagnetice puternice și alte riscuri posibile.

128. Încăperile destinate pentru amplasarea personalului centrului de certificare, precum și alte încăperi de serviciu trebuie să fie echipate cu:

- a) sisteme de pază, alarmă și semnalizare antiincendiară;
- b) sisteme de control al accesului, care să permită supravegherea accesului personalului centrului de certificare în anumite încăperi.

129. În cazul amplasării încăperilor de serviciu sau a altor încăperi la parter și la ultimul etaj, precum și în cazul existenței balcoanelor, scărilor antiincendiară etc., la ferestrele încăperilor respective trebuie să fie instalate gratii din interior.

***Secțiunea a 3-a. Cerințele referitoare la asigurarea securității sistemelor informaționale și de telecomunicații***

130. Pentru micșorarea riscurilor legate de utilizarea tehnologiilor informaționale și de telecomunicații, centrul de certificare elaborează și implementează un set de măsuri de asigurare a securității sistemelor sale informaționale și de telecomunicații (mijloace de program și tehnice, canale de telecomunicații, echipament de rețea, informații prelucrate, depozitate și transmise), prin funcționarea următoarelor subsisteme de securitate:

- a) subsistemul de gestiune a accesului;
- b) subsistemul de înregistrare și evidență (audit);
- c) subsistemul de asigurare a integrității;
- d) subsistemul de asigurare a accesibilității;
- e) subsistemul de protecție criptografică.

131. Subsistemul de gestiune a accesului:

a) asigură delimitarea accesului la obiectele informaționale și la funcțiile sistemelor informaționale corespunzător cu regulile de acces, bazate pe atributele de acces;

b) efectuează verificarea identității subiecților ce obțin acces la componentele sistemelor informaționale;

c) verifică accesul subiecților la resursele protejate corespunzător cu nivelurile de acces stabilite;

d) gestionează fluxurile informaționale și aplică sigla de confidențialitate;

e) fixează cazurile de acces cu succes sau cu eșec.

132. Subsistemul de înregistrare și evidență:

a) înregistrează evenimentele de accesare (părăsire) a sistemului de către subiect conform următorilor parametri:

data și timpul tentativei de accesare (părăsire);

identificatorul subiectului de acces;

rezultatul tentativei de accesare (părăsire) – succes sau eșec;

b) înregistrează tentativele de lansare (stopare) a aplicațiilor și a proceselor destinate să prelucreze resursele protejate conform următorilor parametri:

data și timpul tentativei de lansare;

denumirea (identificatorul) aplicației sau procesului;

identificatorul subiectului de acces;

rezultatul tentativei de lansare – succes sau eșec;

c) înregistrează tentativele de obținere a drepturilor de acces (de executare a operațiilor) pentru aplicații și procese la resursele protejate conform următorilor parametri:

data și timpul tentativei de obținere a accesului (executare a operației);

denumirea (identificatorul) aplicației sau procesului;

identificatorul subiectului de acces;

specificățiile resursei protejate (identificator, nume logic, nume fișier, număr etc.);

tipul operației solicitate (citire, înregistrare, ștergere, montare etc.);

rezultatul tentativei de obținere a accesului (executare a operației) – succes sau eșec;

d) înregistrează tentativele de acces neautorizat al subiecților în sistem, tentativele de lansare neautorizată a aplicațiilor (proceselor) sau de executare a operațiilor, asigurând blocarea tuturor operațiunilor neautorizate și înștiințând despre acest fapt administratorul securitate;

e) înregistrează modificările drepturilor de acces al subiecților și statutul obiectelor de acces conform următorilor parametri:

data și timpul modificării drepturilor;

identificatorul administratorului care a operat modificările;

identificatorul subiectului de acces și noile drepturi sau specificațiile obiectului de acces și noul său statut;

f) înregistrează toate ieșirile de informație din sistem (documente electronice, date etc.) conform următorilor parametri:

data și timpul ieșirilor de date;

denumirea informației și calea spre ea;

specificațiile dispozitivului ce a eliberat informația (numele logic);

identificatorul subiectului de acces care a solicitat informația;

volumul documentului eliberat (număr de pagini, foi, copii) și rezultatul eliberării de informație (succes, eșec);

g) ține evidența resurselor protejate ale centrului de certificare, înregistrează intrarea/ieșirea suporturilor materiale ce conțin informație confidențială;

h) protejează datele "protocate" (jurnalul de înregistrări, fișiere log etc.) contra modificărilor;

i) identifică și arată evenimentele curente.

133. Subsistemul de asigurare a integrității menține stabilitatea mediului aplicativ, integritatea informației prelucrate, a mijloacelor tehnico-aplicative și a mijloacelor de protecție a informației.

134. Subsistemul de asigurare a accesibilității:

a) asigură funcționarea continuă a sistemelor informaționale și de telecomunicații ale centrului de certificare;

b) asigură păstrarea garantată a resurselor informaționale ale centrului de certificare, precum și posibilitatea de restabilire a lor în caz de necesitate sau în cazul situațiilor de forță majoră;

c) asigură utilizatorilor sistemului acces permanent la resursele informaționale ale centrului de certificare, corespunzător cu normele stabilite de acces la informație.

135. Subsistemul de protecție criptografică:

a) realizează criptarea informației confidențiale în sistemul informațional și în canalele de telecomunicații;

b) asigură controlul accesului subiecților la operațiile de criptare și la cheile criptografice, corespunzător cu regulile de acces stabilite.

136. Arhitectura sistemelor informaționale și de telecomunicații ale centrului de certificare și a subsistemelor acestora trebuie să fie destul de flexibilă, să permită dezvoltarea simplă, fără modificări structurale, a configurațiilor mijloacelor utilizate și completarea de noi funcții și resurse.

137. Sistemele informaționale și de telecomunicații ale centrului de certificare trebuie să fie însoțite de documentație care să asigure exploatarea lor calificată.

138. Componentele critice ale sistemelor informaționale și de telecomunicații ale centrului de certificare trebuie să includă sisteme de rezervă și de repornire în cazul încălcării regimului de securitate sau refuzului (deficienței) de deservire.

139. Sistemele informaționale și de telecomunicații, componentele lor, mijloacele tehnice și de program ale centrului de certificare trebuie să corespundă normelor stabilite de politica de securitate informațională, iar prestatorii de servicii (producătorii, furnizorii etc.) trebuie să asigure suportul tehnic necesar.

140. Centrul de certificare trebuie să asigure protecția sistemelor informaționale și de telecomunicații proprii contra acțiunilor aplicațiilor malefice (sistemul de protecție antivirus).

141. Centrul de certificare trebuie să-și clasifice resursele sistemului informațional, să stabilească procedurile de acces și să aprobe lista persoanelor cu drept de acces la resursele specifice ale sistemului informațional și de telecomunicații.

142. Centrul de certificare trebuie să elaboreze, să aprobe și să implementeze mecanismele și procedurile necesare de delimitare și control al accesului logic și fizic la echipamentele sistemelor informaționale și de telecomunicații.

143. Accesul angajaților centrului de certificare la resursele sistemelor informaționale și de telecomunicații trebuie să fie acordat pe baza instrucțiunilor și ordinelor aprobate în centrul de certificare corespunzător drepturilor de acces.

144. Centrul de certificare trebuie să stabilească și să documenteze procedurile privind administrarea și utilizarea resurselor de program și de sistem.

145. Sistemele informaționale și de telecomunicații noi sau modernizate, componentele acestora, mijloacele tehnice și de program trebuie să fie implementate numai în conformitate cu procedurile stabilite, cu respectarea cerințelor privind asigurarea securității informaționale.

146. Centrul de certificare trebuie să elaboreze și să aprobe instrucțiuni de implementare a sistemelor informaționale și de telecomunicații noi sau de modificare a celor existente, a componentelor acestora, a mijloacelor tehnice și de program.

147. Personalul responsabil al centrului de certificare trebuie să fie instruit privind funcționalitatea și regulile de administrare (exploatare) a sistemelor informaționale și de telecomunicații, a componentelor, a mijloacelor tehnice și de program noi sau modernizate.

148. Toate modificările de configurare a sistemelor informaționale și de telecomunicații în ansamblu, a componentelor acestora, a mijloacelor tehnice și de program trebuie să fie testate pînă la implementarea acestora în mediul operațional. Decizia despre modificare trebuie luată numai după realizarea unei evaluări a riscurilor referitoare la implementarea modificărilor respective.

149. Centrul de certificare trebuie să elaboreze și să aprobe proceduri formale de control al modificărilor în sistemul informațional și de telecomunicații, al modificărilor componentelor acestuia, al mijloacelor tehnice și de program.

150. Centrul de certificare trebuie să utilizeze conexiuni și mecanisme securizate și controlabile, care să asigure integritatea și confidențialitatea informației la transmiterea prin intermediul rețelelor publice.

151. Centrul de certificare trebuie să implementeze mecanisme de ecranare a rețelelor, pentru a proteja sistemele informaționale și de telecomunicații interne, precum și resursele centrului de certificare în general.

152. Personalul responsabil al centrului de certificare (administratorii sistem) este obligat să efectueze controlul zilnic al stării sistemelor informaționale și de telecomunicații, al componentelor acestora, sistemelor operaționale și aplicative, precum și al instrumentelor de securitate.

#### ***Secțiunea a 4-a. Condițiile de utilizare a mijloacelor de protecție criptografică a informației***

153. Centrul de certificare asigură securitatea informației confidențiale la depozitare, prelucrare și transmitere prin canalele de comunicații, aplicând tehnologiile de criptare a informației cu utilizarea mijloacelor de protecție criptografică a informației (MPCI).

154. În scopul elaborării și realizării măsurilor de asigurare a securității informației și utilizării MPCI, centrul de certificare trebuie să creeze o subdiviziune pentru protecția criptografică a informației (să numească un angajat), să elaboreze și să aprobe instrucțiuni care să reglementeze procesele de pregătire, introducere, prelucrare, păstrare și transmitere a informației confidențiale protejate cu MPCI.

155. Subdiviziunea de protecție criptografică:

a) elaborează și implementează sistemul de protecție criptografică a informației confidențiale a centrului de certificare;

b) elaborează instrucțiunile și măsurile de asigurare a funcționării și securității MPCI utilizate;

c) asigură păstrarea și evidența purtătorilor materiali de informație confidențială, MPCI și documentației aferente, purtătorilor materiali de informație-cheie, precum și evidența utilizatorilor ce folosesc nemijlocit MPCI;

d) instruește utilizatorii MPCI privind regulile de lucru cu MPCI;

e) controlează modalitatea de respectare de către utilizatori a normelor de utilizare a MPCI stabilite, precum și a documentației de exploatare și tehnice aferente MPCI;

f) verifică integritatea resurselor de program și de sistem ale mijloacelor tehnice unde au fost instalate MPCI, precum și integritatea MPCI;

g) depistează faptele de încălcare a normelor de utilizare a MPCI și întreprinde măsurile necesare de evitare a urmărilor acestor încălcări.

156. Angajații subdiviziunii de protecție criptografică sînt obligați:

a) să respecte regimul de confidențialitate în procesul de îndeplinire a obligațiilor de serviciu;

b) să depisteze la timp tentativele persoanelor terțe de a obține date privind informația confidențială, MPCI utilizate și suporturile-cheie;

c) să ia măsuri urgente de prevenire a cazurilor de divulgare a informației confidențiale și de scurgere a informației la utilizarea MPCCI.

157. Angajații subdiviziunii de protecție criptografică trebuie să posede un nivel de calificare corespunzător și să activeze conform fișei de post.

158. Centrul de certificare implementează și exploatează MPCCI conform documentației tehnice și de exploatare aferentă acestor mijloace, pe baza instrucțiunilor aprobate, precum și în conformitate cu prezentele condiții speciale.

159. Instrucțiunile ce reglementează modul de exploatare în siguranță a MPCCI trebuie să prevadă:

a) drepturile și obligațiile angajaților centrului de certificare ce exploatează MPCCI;

b) ordinea de amplasare, instalare, păstrare și utilizare a MPCCI și a documentației privind exploatarea acestora;

c) ordinea de creare, evidență, distribuire, păstrare și distrugere a cheilor criptografice;

d) ordinea de cercetare a faptelor de încălcare a regulilor stabilite la utilizarea MPCCI, a cheilor criptografice, precum și măsurile de înlăturare a consecințelor;

e) ordinea de control al respectării cerințelor de asigurare a protecției informației cu ajutorul MPCCI.

160. Condițiile de implementare și exploatare a MPCCI trebuie să excludă posibilitatea accesului neautorizat la ele, modificarea, furtul și difuzarea necontrolată a acestora.

161. MPCCI utilizate de centrul de certificare trebuie să fie verificate periodic pe parcursul întregului ciclu de funcționare.

162. MPCCI trebuie să fie inventariate. MPCCI de tip aplicativ sînt supuse evidenței împreună cu mijloacele tehnice pe care le rulează.

163. În caz de necesitate, pentru asigurarea integrității cheilor criptografice pot fi create copii de rezervă, care se păstrează conform normelor stabilite de asigurare a protecției contra accesului neautorizat și acțiunilor neintenționate.

164. Angajații centrului de certificare poartă răspundere personală pentru integritatea și securitatea cheilor criptografice.

165. Subdiviziunea de protecție criptografică ține evidența suporturilor materiale de chei criptografice.

166. Suporturile materiale de chei criptografice neutilizate sau scoase din uz sînt distruse de subdiviziunea de protecție criptografică.

167. Distrugerea cheilor criptografice se efectuează prin distrugerea fizică a suportului material sau prin distrugerea garantată a informației-cheie fără deteriorarea suportului (pentru utilizarea repetată a acestuia).

168. Cheile criptografice ale MPCCI trebuie schimbate periodic. Procedura de schimbare a cheilor criptografice se stabilește de către centrul de certificare.

169. Dacă există suspiciuni privitoare la compromiterea cheilor criptografice sau MPCCI, acestea sînt scoase imediat din uz, iar subdiviziunea de protecție criptografică efectuează toate acțiunile de verificare a acestui fapt și înlăturare a urmărilor.

### ***Secțiunea a 5-a. Condițiile de protecție tehnică a informației***

170. Centrul de certificare asigură protecția informației confidențiale prin utilizarea tehnologiilor și a mijloacelor speciale de prevenire a scurgerii informației prin canalele tehnice.

171. Centrul de certificare trebuie să excludă prezența necontrolată a persoanelor sau a mijloacelor de transport, precum și instalarea întâmplătoare a antenelor, într-o zonă de 15 metri de la locul amplasării mijloacelor tehnice principale ale complexului tehnic de program (în continuare – perimetru controlat).

172. Încăperile pentru servere ale centrului de certificare trebuie să fie protejate contra scurgerii informației din cauza emisiilor electromagnetice prin ecranarea încăperilor sau instalarea sistemelor de bruijă electromagnetică.

173. În cazul ecranării încăperilor trebuie asigurată continuitatea conexiunii electrice a materialului tuturor părților ecranului: pereți, tavan, podea, ferestre și uși. Materialul pentru uși trebuie să posede un contact electric sigur cu ecranul încăperii pe toată suprafața, construcțiile de ecranare trebuie să posede prize de pământ care să fie amplasate în regiunea controlată.

174. Centrul de certificare trebuie să asigure protecția informației contra scurgerii prin intermediul rețelei electrice [încrucișarea rețelelor electrice ale obiectului cu instalarea filtrelor de protecție care să blocheze (bruijeze) semnalul].

175. În încăperile centrului de certificare unde sînt amplasate mijloacele tehnice ce prelucrează informație confidențială trebuie exclusă sau limitată instalarea altor dispozitive electrice, radio sau de alt gen.

176. Utilajul pe liniile care au ieșire în afara regiunii controlate trebuie instalate la o distanță de cel puțin de 3 metri de la mijloacele tehnice principale ale complexului tehnic de program al centrului de certificare.

177. Suficiența măsurilor de protecție tehnică realizate, precum și necesitatea instalării mijloacelor tehnice speciale suplimentare se stabilesc conform rezultatului cercetărilor speciale și de evaluare a nivelului de protejare al obiectului.

### ***Secțiunea a 6-a. Condițiile referitoare la asigurarea securității resurselor informaționale***

178. Resursele informaționale ale centrului de certificare trebuie să fie clasificate și definite pe categorii în funcție de nivelul de securitate al acestora.

179. Toată informația, datele și documentele trebuie să fie prelucrate și păstrate conform nivelului de clasificare și categoriei acestei informații.

180. Toată informația, datele și documentele, clasificate ca fiind confidențiale, trebuie păstrate într-un mediu sigur separat.

181. Centrul de certificare trebuie să ia măsuri de protecție a datelor personale conform legislației Republicii Moldova.

182. Registrul certificatelor cheilor publice trebuie păstrat și gestionat în condiții care îi vor asigura integritatea, accesibilitatea și confidențialitatea.

183. Centrul de certificare trebuie să creeze copii de rezervă ale registrului certificatelor cheilor publice, precum și pentru altă informație critică.

184. Copiile de rezervă se păstrează în încăperi speciale ale centrului de certificare.

185. Documentele centrului de certificare trebuie să fie protejate contra pierderii, distrugerii și falsificării.

186. Centrul de certificare trebuie să fixeze termenele de utilizare și păstrare a documentelor și a informației, să elaboreze nomenclatorul dosarelor, în care vor fi specificate tipurile documentelor principale și perioada de păstrare a acestora.

187. Utilizarea resurselor informaționale ale centrului de certificare în scopuri personale de către angajații centrului este interzisă.

188. Angajații centrului de certificare sînt obligați să cunoască riscurile legate de încălcarea securității informației cu care lucrează.

#### ***Secțiunea a 7-a. Condițiile referitoare la sistemul de administrare a securității informaționale***

189. Centrul de certificare trebuie să creeze sistemul de administrare a securității informaționale, să realizeze monitorizarea permanentă a sistemului de securitate informațională și să gestioneze riscurile.

190. Pentru administrarea securității informaționale se recomandă standardul internațional ISO/IEC 17799-2005 "Tehnologii informaționale. Cod de practici privind administrarea securității informaționale".

### **VIII. Controlul activității centrului de certificare**

191. Centrul de certificare este obligat să efectueze o dată în doi ani un control complex al activității sale.

192. Controlul complex al activității centrului de certificare se efectuează de către organului abilitat cu elaborarea și promovarea politicii de stat și cu exercitarea controlului în domeniul aplicării semnăturii digitale – Serviciului de Informații și Securitate al Republicii Moldova (în continuare – organ competent), cu atragerea, după caz, a specialiștilor în domeniu.

193. La inițiativa centrului de certificare, controlul complex al activității acestuia poate fi realizat de către organizații specializate de audit și de consultare în domeniul tehnologiilor informaționale, cu atragerea reprezentantului organului competent, din contul centrului de certificare.

194. Se recomandă ca organizația ce realizează controlul complex al activității centrului de certificare să corespundă următoarelor cerințe:

a) să posede personal cu calificare atestată prin certificate de auditori în domeniul sistemelor informaționale (standarde internaționale CISA sau CISM);

b) să posede experiență de audit în domeniul tehnologiilor informaționale de minim 2 ani.

195. Organizația ce realizează controlul complex al activității centrului de certificare trebuie:

a) să asigure independența controlului efectuat;

b) să efectueze controlul în conformitate cu normele și standardele de audit în domeniul tehnologiilor informaționale și de securitate a sistemelor informaționale;

c) să utilizeze o metodologie de audit bazată pe evaluarea riscurilor și pe procedurile corespunzătoare de evaluare a măsurilor de gestionare a riscurilor;

d) să asigure confidențialitatea informației obținute în urma controlului.

196. Organizația ce realizează controlul complex al activității centrului de certificare trebuie să întocmească un act de verificare și o încheiere.

197. Actul de verificare se semnează de către persoana responsabilă care a efectuat controlul activității centrului de certificare, reprezentantul organului competent și conducătorul persoanei juridice în cadrul căreia își desfășoară activitatea centrul de certificare.

198. Încheierea se întocmește pe baza actului de verificare și reprezintă documentul care atestă (infirmă) concordanța activității centrului de certificare cu normele stabilite în domeniul semnăturii digitale.

199. Încheierea trebuie să cuprindă:

a) evaluarea calității și continuității serviciilor în domeniul semnăturii digitale prestate de către centrul de certificare;

b) corespunderea activității centrului de certificare cu standardele, normele tehnice și alte documente normative din domeniul semnăturii digitale;

c) corespunderea activității centrului de certificare cu prevederile Regulamentului centrului de certificare, politicii de certificare și politicii de securitate;

d) corespunderea activității centrului de certificare cu funcțiile și obligațiile stabilite;

e) concordanța procedurilor principale ale centrului de certificare cu cerințele înaintate;

f) concordanța activității centrului de certificare cu cerințele de asigurare a securității centrului de certificare;

g) concluzii privind suficiența măsurilor de asigurare a confidențialității, a integrității și accesibilității informației și a serviciilor informaționale;

h) evaluarea calității și complexității procedurilor interne ale centrului de certificare;

i) analiza funcțiilor de gestionare a riscurilor centrului de certificare;

j) respectarea procedurilor de asigurare a continuității în activitate a centrului de certificare;

k) corespunderea complexului tehnic de program al centrului de certificare cu cerințele înaintate;

l) evaluarea măsurilor întreprinse pentru remedierea celor constatate în urma auditului precedent.

200. Rezultatele controlului complex al activității centrului de certificare (copia actului și încheierii), efectuat de către o organizație specializată de audit și de consultare în domeniul tehnologiilor informaționale, se prezintă organului competent.

201. Centrul de certificare trebuie să efectueze periodic auditul intern al activității sale, în conformitate cu Regulamentul privind efectuarea auditului intern aprobat de către acest centru.

## IX. Crearea, reorganizarea și lichidarea centrului de certificare

### *Secțiunea 1. Condițiile la crearea centrului de certificare*

202. Pentru prestarea serviciilor de certificare a cheilor publice, centrul de certificare trebuie să îndeplinească procedura de înregistrare conform normelor stabilite și să certifice cheia publică a persoanei împuternicite a centrului de certificare la centrul de certificare ierarhic superior.

203. Pentru înregistrarea centrului de certificare, persoana juridică care creează centrul de certificare este obligată să asigure îndeplinirea următoarelor condiții:

a) să creeze (numească) o subdiviziune pentru realizarea funcțiilor centrului de certificare;

b) să formeze un stat de personal, cu calificarea necesară pentru prestarea serviciilor de certificare a cheilor publice și a altor servicii în domeniul semnăturii digitale;

c) să amenajeze încăperi speciale, precum și alte încăperi de lucru ale centrului de certificare conform condițiilor referitoare la încăperile centrului de certificare stabilite în prezentele condiții speciale;

d) să creeze complexul tehnic de program al centrului de certificare în conformitate cu normele tehnice din domeniul semnăturii digitale și conform prezentelor condiții speciale;

e) să numească persoana împuternicită a centrului de certificare (administratorul certificare), administratorul înregistrării, administratorul securitate și administratorul sistem;

f) să creeze sistemul de securitate al centrului de certificare în conformitate cu prezentele condițiile speciale;

g) să creeze o subdiviziune (să numească un angajat) responsabilă de protecția criptografică a informației în centrul de certificare;

h) să elaboreze și să aprobe baza normativă a centrului de certificare necesară pentru prestarea serviciilor de certificare a cheilor publice, care include următoarele documente obligatorii:

politica de certificare a centrului de certificare;

Regulamentul centrului de certificare;

politica de securitate a centrului de certificare;

politica de acordare și control al accesului la resursele centrului de certificare;

planul de gestionare a riscurilor;

planul de asigurare a continuității activității centrului de certificare;

procedurile de restabilire a activității centrului de certificare;

instrucțiuni ce reglementează securitatea și exploatarea MPCİ;

regulamentul privind efectuarea auditului intern al centrului de certificare.

i) să obțină o garanție bancară la o bancă înregistrată pe teritoriul Republicii Moldova sau o poliță de asigurare la o companie de asigurări înregistrată în Republica Moldova în favoarea organului competent pentru o sumă în lei echivalentă a 20.000 euro.

204. În procesul înregistrării, centrul de certificare trebuie să treacă procedura unui control complex în conformitate cu cerințele de control al activității centrului de certificare, stabilite în prezentele condiții speciale.

### ***Secțiunea a 2-a. Condițiile referitoare la reorganizarea centrului de certificare***

205. Reorganizarea centrului de certificare se efectuează prin formele prevăzute de legislație, funcțiile acestuia fiind transmise unei alte persoane juridice.

206. Transmiterea centrului de certificare se efectuează:

- a) pe baza contractului de transmitere a centrului de certificare;
- b) pe baza deciziei de reorganizare a persoanei juridice.

207. Persoana juridică trebuie să anunțe organul competent și centrul de certificare ierarhic superior despre decizia privind transmiterea centrului de certificare în termen de cel puțin de 30 de zile până la momentul transmiterii.

208. Persoana juridică trebuie să anunțe toate centrele de certificare ierarhic inferioare și utilizatorii semnăturii digitale despre decizia privind transmiterea centrului de certificare și despre necesitatea reîncheierii contractelor de deservire cu noul centru de certificare în termen de cel puțin de 30 zile până la momentul transmiterii.

209. Prin decizia persoanelor juridice interesate se creează comisia de transmitere a centrului de certificare.

210. În componența comisiei de transmitere a centrului de certificare trebuie să intre:

- a) reprezentanții persoanelor juridice;
- b) reprezentantul organului competent;
- c) alte persoane, stabilite de părți.

211. În procesul de transmitere, centrul de certificare trebuie:

a) să distrugă cheile private ale persoanelor împuternicite ale centrului de certificare fără a le atinge confidențialitatea, în conformitate cu cerințele stabilite de organul competent;

b) să transmită registrul certificatelor cheilor publice.

212. Registrul certificatelor cheilor publice sub formă de documente electronice se transmite pe suporturi materiale, iar registrul certificatelor cheilor publice sub formă de documente pe suport de hârtie se transmite sub formă de arhivă a documentelor pe suporturi de hârtie.

213. Certificatele cheilor publice eliberate de către centrul de certificare continuă să fie valabile până la expirarea termenul de valabilitate.

214. La încheierea lucrărilor comisiei se întocmește actul de primire-predare, conform căruia persoana juridică căreia i-a fost transmis centrul de certificare devine succesorul de drepturi al centrului. Actul se semnează de membrii comisiei și se aprobă de către conducătorii persoanelor juridice interesate.

### ***Secțiunea a 3-a. Condițiile referitoare la lichidarea centrului de certificare***

215. Centrul de certificare poate fi lichidat:

- a) la inițiativa persoanei juridice care a creat centrul de certificare;
- b) la inițiativa organului competent în cazul încălcării normelor în domeniul semnăturii digitale;
- c) în cazul lichidării persoanei juridice care a creat centrul de certificare.

216. Persoana juridică trebuie să anunțe organul competent și centrul de certificare ierarhic superior despre decizia de lichidare a centrului de certificare în termen de cel puțin de 30 de zile până la momentul lichidării.

217. Utilizatorii semnăturii digitale vor fi înștiințați despre decizia de lichidare a centrului de certificare într-o perioadă de cel puțin 30 de zile până la momentul lichidării.

218. Procedura de lichidare a centrului de certificare la inițiativa persoanei juridice care a creat centrul de certificare se inițiază prin ordinul conducătorului persoanei juridice.

219. Prin ordinul conducătorului persoanei juridice care lichidează centrul de certificare se creează comisia de lichidare, în sarcina căreia intră desfășurarea procedurii de lichidare.

220. Lichidarea centrului de certificare la inițiativa organului competent este efectuată pe cale judiciară în baza încheierii organului competent privind încălcarea legislației în domeniul semnăturii digitale. După pronunțarea hotărârii instanței de judecată, prin ordinul conducătorului organului competent, se creează comisia de lichidare.

221. În componența comisiei de lichidare trebuie să intre:

- a) conducătorul persoanei juridice ce a creat centrul de certificare;
- b) reprezentantul organului competent;
- c) alte persoane, numite prin ordin.

222. În procesul de lichidare, centrul de certificare trebuie:

- a) să distrugă cheile private ale persoanelor împuternicite ale centrului de certificare fără a le atinge confidențialitatea în conformitate cu cerințele stabilite de către organul competent;
- b) să revoce certificatele cheilor publice ale utilizatorilor semnăturii digitale eliberate de centrul de certificare aflat în curs de lichidare;
- c) să publice statutul certificatelor cheilor publice;
- d) să transmită spre păstrare organului competent registrul certificatelor cheilor publice.

223. Registrul certificatelor cheilor publice sub formă de documente electronice se transmite pe suporturi materiale, iar registrul certificatelor cheilor publice sub formă de documente pe suport de hârtie se transmite sub formă de arhivă a documentelor pe suporturi de hârtie, fapt ce se consemnează în actul de primire-predare, semnat de către conducătorul persoanei juridice și reprezentantul organului competent, responsabil pentru păstrare. Registrul certificatelor cheilor publice se păstrează în formă arhivată în conformitate cu legislația în vigoare.

224. Comisia de lichidare întocmește un act, în urma căruia centrul de certificare își încetează existența.