

**GUVERNUL REPUBLICII MOLDOVA**

**HOTĂRÂRE** nr. \_\_\_\_\_  
din \_\_\_\_\_ 2024

**cu privire la aprobarea Regulamentului de organizare și funcționare a Sistemului  
informațional în domeniul protecției copilului**

În temeiul art. 22 din Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr. 6-12, art. 44), cu modificările ulterioare,

Guvernul **HOTĂRĂȘTE**:

1. Se aprobă Regulamentul de organizare și funcționare a Sistemului informațional în domeniul protecției copilului (se anexează).
2. Asigurarea condițiilor juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional în domeniul protecției copilului se realizează de către Ministerul Muncii și Protecției Sociale, în calitate de posesor al acestuia.
3. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Muncii și Protecției Sociale.

**Prim-ministru**

**Dorin RECEAN**

**Contrasemnează:**

vicepremier, ministrul dezvoltării  
economice și digitalizării

**Dumitru ALAIBA**

ministrul muncii  
și protecției sociale

**Alexei BUZU**

## **REGULAMENTUL**

### **de organizare și funcționare a Sistemului informațional în domeniul protecției copilului**

#### **I. DISPOZIȚII GENERALE**

1. Regulamentul de organizare și funcționare a Sistemului Informațional în domeniul protecției copilului (*în continuare – SIPC*) are drept scop implementarea Conceptului Sistemului informațional în domeniul protecției copilului și stabilirea structurii, funcțiilor, subiecților, atribuțiilor, interoperabilității și modului de menținere a sistemului.

2. SIPC stabilește modul de organizare și funcționare a resursei informaționale de stat destinată păstrării, prelucrării și furnizării informației privind copiii (aflați în situație de risc, separați de părinți) și familia lor, precum și a informației referitoare la acțiunile întreprinse în privința acestora. Regulamentul reglementează cerințele față de protecția datelor în procesul de colectare, actualizare, păstrare, procesare și furnizare a informațiilor, precum și schimbul autorizat de date cu alte sisteme informaționale.

3. În sensul prezentului Regulament se definesc următoarele noțiuni:

*identificare* - atribuirea unui identificator subiectelor și obiectelor de acces și/sau compararea identificatorului prezentat cu lista identificatoarelor atribuite;

*integritate* - certitudinea, coerența și actualitatea informației, protecția acesteia împotriva distrugerii și modificării neautorizate;

*întreținerea sistemului* - totalitatea măsurilor cu caracter tehnic îndreptate spre asigurarea funcționării complexului tehnic de program și administrarea resursei informaționale a SIPC;

*administrator global* – rol atribuit în cadrul SIPC, persoanelor autorizate, care au drept de acces complet în sistem, permițându-le să gestioneze adăugarea de noi utilizatori, modificarea setărilor, vizualizarea și editarea întregului conținut din sistemul informațional;

*administrator local* – rol atribuit în cadrul SIPC, persoanelor autorizate la nivel local/raional, care permite utilizatorilor gestionarea conturilor altor utilizatori și monitorizarea conținutului creat în cadrul sistemului, în limitele competențelor acordate;

*generator de statistici* – rol atribuit în cadrul SIPC, persoanelor autorizate, care permite utilizatorilor vizualizarea rapoartelor statistice generate în cadrul sistemului.

#### **II. STRUCTURA ȘI CARACTERISTICILE SIPC**

4. SIPC are o structură modulară cu următoarele contururi funcționale – (1) contur „Administrare”, (2) contur „Profil copil” (3) Contur „Management de caz”, (4) Contur „Adopții”, (5) Contur „Rapoarte și analitică”.

5. SIPC are următoarele caracteristici:

1) managementul cazului:

- a) realizează înregistrarea cazului în sistem utilizând formularul de înregistrare a cazului copilului aflat în situație de risc sau separat de părinți;
  - b) realizează documentarea evaluării inițiale și evaluării complexe a copiilor aflați în situație de risc și a copiilor separați de părinți, a evaluărilor legate de cazurile de adopție;
  - c) realizează implementarea, monitorizarea și revizuirea planului individual de asistență a copilului și a familiei copilului;
- 2) managementul sarcinilor – realizează un set de funcționalități pentru documentarea și urmărirea acțiunilor întreprinse conform managementului de caz în cazul copiilor aflați în situație de risc, copiilor separați de părinți, copiilor adoptabili și copiilor adoptați. Acestea includ: planificarea sarcinilor pentru managerul de caz, editarea, examinarea și aprobarea cazurilor, schimbările de stare a cazului, gestionarea incidentelor, alerte și notificări, ținerea evidenței;
  - 3) managementul documentelor – atașarea documentelor și a fișierelor scanate necesare pentru managementul de caz;
  - 4) managementul referirilor – realizează referirea cazului la diverse servicii;
  - 5) managementul transferurilor – realizează transferul cazului între autoritățile tutelare din alte Unități Administrativ Teritoriale la schimbarea locului de trai a copilului;
  - 6) generarea de rapoarte și tablouri de bord, precum sunt:
    - a) rapoarte statistice și rapoarte zilnice de lucru;
    - b) tablouri de bord a indicatorilor de performanță în domeniul managementului de caz, serviciilor alternative de plasament a copiilor, adopției, violenței împotriva copiilor;
  - 7) exportul datelor – realizează exportul datelor depersonalizate din sistem în format CSV, Excel și PDF;
  - 8) managementul nomenclatoarelor – gestionarea (crearea, vizualizarea, modificarea și ștergerea) datelor nomenclatoarelor utilizate în cadrul sistemului;
  - 9) managementul utilizatorilor, rolurilor și permisiunilor – gestionarea utilizatorilor, atribuirea de roluri și setarea permisiunilor de acces și gestionarea profilului utilizatorilor.

### **III. CATEGORIILE DATELOR PRELUCRATE**

6. SIPC este integrat cu alte sisteme informaționale, reprezentând un mediu informațional securizat, exhaustiv și transparent.

7. Prin intermediul SIPC sunt prelucrate următoarele categorii de date cu caracter personal despre copil:

- 1) numărul de identificare (IDNP);
- 2) numărul certificatului de naștere a copilului;
- 3) numele și prenumele copilului;
- 4) data, luna și anul nașterii a copilului;
- 5) sexul copilului;
- 6) naționalitatea copilului;
- 7) gradul de dizabilitate al copilului;
- 8) raionul/municipiul și localitatea/sectorul din viza de domiciliu a copilului;
- 9) datele de contact ale copilului;
- 10) riscul la care este expus copilul, conform prevederilor Legii nr. 140/2013

privind protecția specială a copiilor aflați în situație de risc și a copiilor separați de părinți.

8. Prin intermediul SIPC sunt prelucrate următoarele categorii de date cu caracter personal despre familia copilului:

- 1) numărul de identificare a persoanei (IDNP);
- 2) numele și prenumele persoanei;
- 3) data, luna și anul nașterii a persoanei;
- 4) sexul;
- 5) relația de rudenie cu copilul;
- 6) condiții locative și bunăstarea familiei;
- 7) datele de contact ale reprezentanților legali/responsabililor legali ai copilului.

9. Prin intermediul SIPC sunt prelucrate date privind contactul copilului cu următoarele servicii:

- 1) Educație
    - a) denumirea instituției;
    - b) data înmatriculării;
    - c) clasa/anul de studii;
    - d) numele, prenumele reprezentantului instituției;
    - e) datele de contact ale reprezentantului instituției;
    - f) cerințe educaționale speciale (CES) ale copilului.
  - 2) Sănătate
    - a) instituția medicală unde este luat la evidență copilul;
    - b) numele, prenumele medicului de familie/asistentului medical;
    - c) datele de contact ale medicului de familie/asistentului medical;
    - d) tipul de asistență medicală de care a beneficiat copilul;
    - e) perioada de asistență medicală de care a beneficiat copilul.
  - 3) Asistență socială
    - a) tipul serviciilor de care a beneficiat și/sau beneficiază copilul sau familia copilului;
    - b) tipul prestațiilor sociale de care a beneficiat și/sau beneficiază copilul sau familia copilului;
    - c) separarea de familia biologică și tipul de plasament: tutelă/curatelă, custodie, serviciu de plasament de tip familial, serviciu de plasament de tip rezidențial.
  - 4) Ordine publică
    - a) aflarea în evidență la organele de drept;
    - b) motivul aflării în evidență la organele de drept;
    - c) măsurile aplicate în raport cu copilul;
    - d) sancțiuni aplicate în raport cu copilul.
10. Prin intermediul SIPC sunt prelucrate date despre serviciile sociale:
- a) codul serviciului social;
  - b) denumirea serviciului social;
  - c) tipul serviciului social;
  - d) locul de acordare a serviciului social.

11. În SIPC, datele cu caracter personal sunt utilizate doar în scopul în care este notificat, fără a se urmări obținerea unor informații în interes personal.

#### **IV. SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII,**

## ADMINISTRĂRII, MENTENANȚEI, DEZVOLTĂRII ȘI UTILIZĂRII SIPC ȘI ATRIBUȚIILE ACESTORA

12. Proprietarul SIPC este Statul.

13. Posesorul și Deținătorul SIPC este Ministerul Muncii și Protecției Sociale, care este responsabil de administrarea și dezvoltarea sistemului.

14. Posesorul/Deținătorul este responsabil de elaborarea și promovarea politicilor în domeniul dezvoltării și administrării SIPC și asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea și dezvoltarea sistemului informațional de stat.

15. Administratorul tehnic al SIPC este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică” (STISC), care își exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale de stat.

16. Destinatari ai datelor din SIPC sunt autoritățile/instituțiile publice centrale și locale, în limitele competențelor ce le sunt atribuite.

17. Registratorii de date în SIPC sunt următorii:

1) persoanele responsabile din cadrul autorităților tutelare locale și teritoriale ce vor fi autorizate să opereze în sistem;

2) persoanele responsabile din cadrul Agențiilor teritoriale de asistență socială din subordinea Ministerului Muncii și Protecției Sociale;

3) personalul responsabil pentru dezvoltarea politicilor de protecție a drepturilor copilului și familiilor cu copii din cadrul Ministerului Muncii și Protecției Sociale;

4) alte persoane cu atribuții în domeniul protecției drepturilor copilului.

18. Registratorii de date în SIPC au următoarele drepturi în limita competențelor atribuite:

1) înregistrarea datelor copiilor aflați în situație de risc și a copiilor separați de părinți;

2) înregistrarea dosarelor copiilor aflați în situație de risc și a copiilor separați de părinți;

3) completarea formularelor de evaluare inițială și evaluare complexă a situației copilului și familiei copilului;

4) dezvoltarea planului individual de asistență a copilului și a planului individual de asistență a familiei copilului;

5) revizuirea planului individual de asistență a copilului și a planului individual de asistență a familiei copilului;

6) realizarea și altor acțiuni, conform managementului de caz, aprobat de Ministerul Muncii și Protecției Sociale;

7) înregistrarea informației privind copiii adoptabili și evidența copiilor adoptabili;

8) înregistrarea cererilor de adopție și evidența adoptatorilor;

9) înregistrarea informației privind potrivirea copiilor adoptabili și a adoptatorilor ținând cont de interesul superior al copilului și de cererea adoptatorului;

10) înregistrarea informației privind copiii adoptați și evidența copiilor adoptați, inclusiv încărcarea rapoartelor de evaluare postadopție.

19. Furnizorii de date ai SIPC prin intermediul platformei de interoperabilitate

(MConnect) sunt:

- 1) Agenția Servicii Publice (ASP), care va asigura furnizarea datelor cu caracter personal ale persoanelor fizice;
  - 2) Casa Națională de Asigurări Sociale (CNAS), care va asigura furnizarea datelor privind prestațiile sociale acordate copilului și familiei acestuia;
  - 3) Ministerul Sănătății (MS), care va asigura furnizarea datelor despre starea de sănătate și bunăstare a copilului;
  - 4) Ministerul Educației și Cercetării (MEC), care va asigura furnizarea datelor despre copil din sistemul educației;
  - 5) Ministerul Muncii și Protecției Sociale (MMPS), care va asigura furnizarea datelor privind prestațiile sociale și serviciile sociale, precum și solicitanții și beneficiarii de asistență socială;
  - 6) Compania Națională de Asigurări în Medicină (CNAM), care va asigura furnizarea datelor despre medicul de familie și instituția medico-sanitară la care este înregistrat copilul;
  - 7) Consiliul Național pentru Determinarea Dizabilității și Capacității de Muncă (CNDDCM), care va asigura furnizarea datelor privind determinarea dizabilității copilului;
  - 8) Ministerul Afacerilor Interne (MAI) care va asigura furnizarea datelor despre persoanele care nu au atins vârsta de 18 ani, aflate la evidență centralizată, în conformitate cu prevederile Legii nr. 216/2003 cu privire la Sistemul informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni;
  - 9) Agenția de Administrare a Instanțelor Judecătorești (AAIJ) care va asigura furnizarea datelor privind cazurile de infracțiuni asupra copiilor în cazul cărora au fost pornite dosare penale și se află pe rolul instanțelor de judecată;
20. Alți furnizori de date pentru SIPC sunt: Inspectoratul General al Poliției, Inspectoratul de Stat al Muncii, Procuratura Generală, etc.

## **V. REGIMUL JURIDIC DE UTILIZARE A DATELOR SIPC**

21. Accesul la SIPC este segmentat pentru utilizatorii interni (care includ posesorul/deținătorul, registratorul și alți utilizatori ale căror drepturi de acces sunt definite în acte normative) și utilizatorii externi (utilizatorii care accesează datele prin platforma de interoperabilitate).

22. Utilizatorii beneficiază de drepturi de acces la informația din SIPC conform atribuțiilor și funcțiilor deținute și regimului juridic al informației accesate. Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu și profilului de acces. Informația conținută în SIPC se accesează în conformitate cu Legea nr. 148/2023 privind accesul la informațiile de interes public și în limitele stabilite de aceasta, precum și în conformitate cu alte acte normative.

23. Administratorul tehnic are acces la datele din SIPC, în scopul prestării serviciilor de administrare, inclusiv mentenanță adaptivă și perfectivă a SIPC.

24. Drepturile și obligațiile posesorului SIPC:

- 1) să asigure crearea, dezvoltarea, funcționarea și administrarea SIPC;
- 2) să propună soluții pentru perfecționarea și eficientizarea procesului de

funcționare a SIPC;

3) să asigure accesul utilizatorilor în conformitate cu drepturile de acces stabilite și atribuțiile delegate;

4) să inițieze procedura de suspendare a drepturilor de acces la SIPC pentru subiecții care nu respectă prevederile Regulamentului, inclusiv măsurile tehnice și organizatorice de protecție și securitate;

5) să aprobe instrucțiuni și ghiduri privind introducerea, examinarea, păstrarea și completarea datelor, precum și funcționarea SIPC;

6) să monitorizeze procesul de înregistrare și prelucrare a datelor în SIPC;

7) să stabilească măsurile tehnice și organizatorice de protecție și securitate a SIPC;

8) să asigure întreținerea (mentenanța) SIPC în conformitate cu prevederile legislației;

9) să exercite alte atribuții necesare asigurării bunei funcționări și guvernante a SIPC.

25. Drepturile și obligațiile registratorului:

1) să vizualizeze și să editeze informațiile din SIPC conform rolului atribuit;

2) să acceseze spațiul informațional al SIPC în limitele rolului atribuit;

3) să acceseze informațiile care se conțin în SIPC și care au fost prezentate de către acesta;

4) să înainteze Posesorului propuneri privind modificarea actelor normative care reglementează funcționarea SIPC;

5) să solicite și să primească de la Posesor asistență metodologică și practică privind funcționarea SIPC;

6) să asigure corectitudinea, autenticitatea și veridicitatea datelor introduse în SIPC;

7) să asigure actualizarea datelor introduse în SIPC;

8) să întreprindă măsuri pentru evitarea accesului neautorizat al persoanelor terțe;

9) să utilizeze funcționalitățile SIPC în exclusivitate conform destinației acestora și în strictă conformitate cu legislația;

10) să utilizeze informația obținută din SIPC doar în scopurile stabilite în legislație.

26. Drepturile și obligațiile altor categorii de subiecți:

1) să participe la implementarea și dezvoltarea SIPC;

2) să înainteze posesorului SIPC propuneri privind modificarea actelor normative care reglementează funcționarea SIPC;

3) să solicite și să primească de la Posesorul SIPC ajutor metodologic și practic privind funcționarea acestuia;

4) să solicite și să primească de la Posesor informații referitoare la nivelul agreat al serviciilor conform indicatorilor stabiliți în anexele tehnice;

5) să solicite și să primească de la posesor accesul la datele/informațiile din SIPC în conformitate cu scopul prelucrării și rolul atribuit;

6) să asigure accesul securizat la informația conținută în SIPC, respectarea condițiilor de securitate și a regulilor de exploatare a acestuia;

7) să ia măsurile organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu

instrucțiunile posesorului SIPC;

8) să aducă la cunoștința posesorului SIPC, în termen de o zi, orice situație (incidente aflate în afara ariei de competență a participantului) care ar putea influența în mod negativ exercitarea funcțiilor participantului.

27. Modificarea și/sau completarea datelor din SIPC se pot realiza de către utilizatori în baza rolurilor și permisiunilor atribuite, după cum urmează:

1) Administrator global – gestionează alte roluri de utilizator; gestionează clasificatoarele, arhiva și jurnalele din sistem, accesul la tablouri de bord;

2) Administrator local – gestionează conturile de utilizatori locali/raionali și monitorizează activitățile acestor utilizatori;

3) Generator de statistici – generează rapoarte statistice la nivel local, raional și național, calculează indicatori de performanță și are acces la tablouri de bord;

4) Manager de caz – asigură înregistrarea și coordonarea tuturor acțiunilor aferente acordării asistenței beneficiarului, în conformitate cu procedurile reglementate de managementul de caz și legislația în domeniul protecției copilului.

28. Toate modificările operate în SIPC sunt jurnalizate și se păstrează în ordine cronologică prin utilizarea serviciului electronic guvernamental de jurnalizare (MLog).

29. Modalitatea de autentificare în SIPC se realizează prin utilizarea serviciului electronic guvernamental de autentificare și control al accesului (MPass). Exploatarea SIPC fără autorizare nominală este strict interzisă și este considerată ca acces neautorizat la un sistem informațional public.

30. Dreptul de acces la SIPC nu este unul permanent, acesta putând fi suspendat sau revocat. Introducerea și/sau modificarea datelor în SIPC de pe un nume sau profil de utilizator străin este strict interzisă, fiind considerată ca acces neautorizat.

31. Revocarea/suspendarea dreptului de acces la SIPC se efectuează de către Posesor/Deținător, în una dintre următoarele situații:

1) la încetarea/suspendarea raporturilor de serviciu/de muncă ale utilizatorului;

2) la intervenirea modificărilor raporturilor de serviciu/de muncă, când noile atribuții nu impun accesul la datele din SIPC;

3) la constatarea încălcării securității informaționale;

4) în alte cazuri, în limitele legislației.

## **VI. INTEROPERABILITATEA CU ALTE SISTEME INFORMAȚIONALE**

32. Pentru asigurarea actualizării operative și automate a conținutului informațional al SIPC cu informație veridică, poate fi efectuată interacțiunea și sincronizarea datelor cu alte sisteme informaționale, importându-se automat sau exportându-se date spre verificare și/sau completare a conținutului informațional al SIPC.

33. SIPC interacționează, prin intermediul platformei de interoperabilitate Mconnect, cu următoarele sisteme și resurse informaționale de stat:

1) Sistemul informațional automatizat „Registrul de stat al populației”;

2) Sistemul informațional automatizat „Asistență socială”;

3) Sistemul informațional automatizat „Asistența medicală primară”;

4) Sistemul informațional automatizat al Companiei Naționale de Asigurări în Medicină;

5) Sistemul informațional automatizat al Casei Naționale de Asigurări Sociale;



6) Sistemul informațional automatizat „Determinarea dizabilității și capacității de muncă”;

7) Sistemul informațional de management în educație al Ministerului Educației și Cercetării;

8) Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”;

9) Sistemul informatic „Programul integrat de gestionare a dosarelor”;

10) Sistemul informațional automatizat al Biroului Național de Statistică.

34. SIPC utilizează următoarele servicii electronice guvernamentale de platformă:

1) serviciul electronic guvernamental integrat de semnătură electronică (MSign) – serviciu reutilizabil, furnizat la nivelul platformei tehnologice comune a Guvernului, care are scopul de a oferi un mecanism integrator, securizat și flexibil pentru diferite soluții de aplicare și verificare a autenticității semnăturii electronice de către utilizatori (inclusiv în contextul utilizării sistemelor informaționale și a serviciilor electronice), oferite de către furnizorii de semnătură electronică în conformitate cu legislația;

2) serviciul electronic guvernamental de jurnalizare (MLog) – serviciu centralizat, reutilizabil, componentă a platformei tehnologice guvernamentale comune (MCloud), care are scopul de a oferi un mecanism securizat și flexibil de jurnalizare și audit, asigurând evidența evenimentelor, în contextul utilizării sistemelor informaționale;

3) serviciul guvernamental de notificare electronică (MNotify) – serviciu centralizat, reutilizabil, componentă a platformei tehnologice guvernamentale comune (MCloud), care are scopul de a oferi un mecanism de transmitere a notificărilor în cadrul sistemelor informaționale deținute de ministere, autorități administrative și structuri organizaționale din sfera lor de competență, precum și alte instituții publice, prestatoare de servicii publice;

4) serviciul electronic guvernamental de autentificare și control al accesului (MPass) – serviciu reutilizabil, furnizat la nivelul platformei tehnologice guvernamentale comune, care are scopul de a oferi un mecanism integrator, securizat și flexibil de autentificare și control al accesului utilizatorilor în sistemele informaționale, inclusiv serviciile electronice.

## **VII. ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI SIPC**

35. Datele din SIPC fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și a integrității datelor înregistrate și prelucrate în cadrul SIPC se efectuează de către subiecții cu drepturi de acces la sistem și cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora.

36. Prelucrarea datelor cu caracter personal se efectuează în conformitate cu prevederile actelor normative în domeniul protecției datelor cu caracter personal. Prelucrarea, stocarea și utilizarea datelor cu caracter personal se efectuează doar în scopul asistenței copiilor aflați în situație de risc și nu va depăși durata necesară atingerii scopurilor declarat. Stocarea datelor cu caracter personal pe o perioadă mai mare, în scopuri statistice, de cercetare istorică sau științifică, se va face cu respectarea garanțiilor privind prelucrarea datelor cu caracter personal, prevăzute de normele ce reglementează aceste domenii, și numai pentru perioada necesară realizării acestor scopuri.

37. Persoanele împuternicite sunt obligate să nu divulge datele și informațiile cu caracter personal la care au primit acces în legătură cu exercitarea atribuțiilor funcționale, inclusiv după încetarea activității lor.

38. Măsurile de protecție și securitate a datelor din SIPC reprezintă totalitatea acțiunilor juridice, organizatorice, economice și tehnologice orientate spre prevenirea pericolelor asociate resurselor și infrastructurii informaționale.

39. Obiectul asigurării protecției și securității datelor din SIPC este complexul de mijloace software și hardware care asigură realizarea proceselor informaționale, și anume:

1) baza de date, sistemele informaționale, sistemele operaționale, sistemele de gestiune a bazelor de date, sistemele de evidență și alte aplicații care asigură funcționarea SIPC;

2) sistemele de comunicații electronice, rețelele, serverele, calculatoarele și alte mijloace tehnice de prelucrare a datelor.

40. Protecția datelor din SIPC se efectuează prin următoarele metode:

1) prevenirea acțiunilor intenționate și/sau neintenționate ale utilizatorilor care pot duce la distrugerea sau denaturarea datelor;

2) utilizarea obligatorie a produselor de program licențiate și aprobate. Orice solicitare de instalare a unui produs de program trebuie coordonată cu Administratorul tehnic;

3) monitorizarea procesului de exploatare al SIPC prin intermediul mecanismului de jurnalizare efectuat de deținătorul tehnic al acestuia.

41. La utilizarea și exploatarea SIPC, utilizatorii asigură implementarea normelor de securitate, acestea urmând să conțină acte ce confirmă:

1) identitatea persoanei responsabile de implementarea normelor de securitate și împuternicirile acesteia;

2) implementarea principalelor măsuri tehnico-organizatorice necesare asigurării funcționării SIPC;

3) implementarea procedurilor interne ce exclud cazurile de modificare nesancționată a mijloacelor software și/sau a informației din SIPC;

4) informarea utilizatorilor interni și instruirea acestora cu privire la modalitățile și mecanismele de asigurare a securității informaționale;

5) procedurile de control intern ale utilizatorilor SIPC privind respectarea condițiilor de securitate informațională.

42. Schimbul informațional se efectuează cu utilizarea mijloacelor software și hardware, doar prin canale securizate, asigurând integritatea și securitatea datelor.

43. Utilizatorii interni desemnează o persoană subordonată nemijlocit conducătorului instituției, responsabilă de implementarea și monitorizarea respectării normelor de securitate informațională.

44. Normele de securitate informațională se aduc la cunoștința fiecărui utilizator intern și se semnează de acesta. Fiecare utilizator intern este obligat să cunoască normele securității informaționale și procedurile pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

45. Utilizatorii interni asigură instruirea angajaților privind metodele și procedeele de contracarare a pericolelor informaționale.

## VI. ASIGURAREA CONTROLULUI INTERN ȘI EXTERN AL SIPC

46. Întreținerea SIPC este supusă controlului intern și extern. Controlul intern privind organizarea și funcționarea SIPC se efectuează de către Posesor/Deținător. Controlul extern asupra respectării cerințelor privind crearea, întreținerea, exploatarea și reorganizarea SIPC se efectuează de către instituții abilitate și certificate în domeniul auditului.

47. Responsabilitatea pentru organizarea funcționării SIPC aparține Posesorului/Deținătorului acestuia.

48. Utilizatorii, în atribuțiile cărora intră întreținerea SIPC, introducerea datelor, furnizarea informațiilor și asigurarea funcționării SIPC, poartă răspundere personală, în conformitate cu legislația, pentru completitudinea, autenticitatea, veridicitatea, integritatea informației, precum și pentru păstrarea și utilizarea ei.

49. Toți subiecții SIPC poartă răspundere disciplinară, civilă, contravențională sau penală, conform legislației, pentru prelucrarea, divulgarea, transmiterea informației din sistem persoanelor terțe, contrar legislației.

50. Pentru asigurarea funcționalității eficiente și neîntrerupte a SIPC, schimbul informațional de date SIPC este asigurat în regim non-stop.

51. Funcționarea SIPC se suspendă de către Administratorul tehnic, la inițiativa proprie sau la demersul persoanei responsabile din cadrul Ministerului Muncii și Protecției Sociale, care asigură funcționalitatea sistemului informațional și a resurselor informaționale la nivel central și/sau local, în caz de apariție a uneia dintre următoarele situații:

1) în timpul efectuării lucrărilor profilactice ale complexului de mijloace software și hardware al SIPC;

2) la apariția circumstanțelor de forță majoră;

3) la încălcarea cerințelor sistemului, securității informației, dacă aceasta prezintă pericol pentru funcționarea SIPC;

4) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SIPC;

5) la cererea scrisă a posesorului.

52. În cazul apariției circumstanțelor de forță majoră și a dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SIPC din vina terțelor persoane, poate fi sistată funcționarea SIPC, cu informarea utilizatorilor SIPC prin mijloacele tehnice disponibile.