Proiect

GUVERNUL REPUBLICII MOLDOVA
HOTĂRÂRE nr. _____
din _____ _____ 2024

cu privire la aprobarea Conceptului Sistemului informațional de evidență a agresorilor în cazurile de violență în familie și a Regulamentului resursei informaționale formate de Sistemul informațional de evidență a agresorilor în cazurile de violență în familie

În temeiul art. 8 alin. (6) lit. b) din Legea nr. 45/2007 cu privire la prevenirea și combaterea violenței împotriva femeilor și a violenței în familie (Monitorul Oficial al Republicii Moldova, 2008, nr. 55-56, art. 178), cu modificările ulterioare și art. 22, lit. c) și d) 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 instituie Sistemul informațional de evidență a agresorilor în cazurile de violență în familie.

2. Se aprobă:

(1) Conceptul Sistemului informațional de evidență a agresorilor în cazurile de violență în familie, conform anexei nr. 1;

(2) Regulamentul resursei informaționale formate de Sistemul informațional de evidență a agresorilor familiali în cazurile de violență în familie, conform anexei nr. 2.

3. Asigurarea condițiilor juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea Sistemului informațional de evidență a agresorilor în cazurile de violență în familie se realizează de către Ministerul Afacerilor Interne, în calitate de posesor al acestuia.

4. Realizarea prevederilor prezentei hotărâri se va efectua din contul și în limitele alocațiilor aprobate prin legea bugetară anuală, precum și din alte surse neinterzise de legislație.

5. Controlul asupra executării prezentei hotărâri se pune în sarcina Ministerului Afacerilor Interne.

Prim-ministru **Dorin RECEAN**

Contrasemnează:

Viceprim-ministru, ministrul dezvoltării
economice și digitalizării **Dumitru ALAIBA**

Ministrul afacerilor interne **Adrian EFROS**

Anexa nr. 1 la Hotărârea
Guvernului nr._____/2024

CONCEPTUL
Sistemului informațional de evidență a agresorilor în cazurile de violență în familie

INTRODUCERE

Conceptul Sistemului informațional de evidență agresorilor în cazurile de violență în familie (în continuare – *Concept*) este elaborat în conformitate cu Reglementarea tehnică „Procesele ciclului de viață al software-ului" RT 38370656-002:2006, aprobată prin Ordinul ministrului dezvoltării informaționale nr. 78/2006, actualmente Ministerul Dezvoltării Economice și Digitalizării.

Prezentul Concept oferă o viziune conceptuală pentru instituirea și operarea unui Sistem informațional destinat evidenței a agresorilor familiali, incluzând scopul, obiectivele, principiile, caracteristicile de bază și funcționalitatea, ținând cont de sarcinile principale ale Ministerului Afacerilor Interne în calitate de organ central de specialitate al administrației publice centrale, care realizează prerogativele constituționale ale Guvernului privind elaborarea, promovarea și implementarea politicii statului în vederea asigurării ordinii și securității publice, respectării drepturilor și libertăților fundamentale ale cetățenilor, inclusiv, prioritizarea acțiunilor în domeniul prevenirii și combaterii violenței față de femei și violenței în familie, protecției victimelor acestui viciu social, reducerii comportamentului agresiv al făptuitorilor, precum și oferirea unui răspuns prompt exigențelor *Convenției Consiliului Europei privind prevenirea și combaterea violenței împotriva femeilor și a violenței domestice (Convenției de la Istanbul)*, ratificată de Republica Moldova prin Legea nr. 144/2021.

Din perspectiva performanței instituționale, Sistemul informațional de evidență a agresorilor în cazurile de violență în familie permite optimizarea activităților organelor de drept, în procesul de colectare și înregistrare a informațiilor despre persoanele care au săvârșit infracțiuni și contravenții de violență în familie, care creează sistematic situații de conflict în familie, aplică violență (fizică, psihologică, sexuală, economică) sau manifestă comportament violent față de membrii de familie, amenință membrii familiei cu moartea sau cu cauzarea vătămărilor corporale, persoanele liberate condiționat de răspundere penală sau condamnate cu suspendarea condiționată a executării pedepsei, persoanele în privința cărora sunt aplicate măsuri de constrângere cu caracter medical, restricții aplicate prin ordinul de restricție de urgență sau ordonanță de protecție, agresorii familiali în privința cărora este aplicată monitorizarea electronică sau cei obligați să participe la programe speciale de tratament sau de consiliere în vederea reducerii comportamentului violent, precum și alte decizii judiciare relevante etc.

Conceptul este aliniat la *Programul de consolidare a încrederii și siguranței societății prin formare profesională, integritate și digitalizare a sistemului afacerilor interne pentru anii 2022-2025,* aprobat prin Hotărârea Guvernului nr. 947/2022, și urmărește asigurarea unui nivel avansat de interconexiune cu comunitatea, drept condiție de eficientizare a funcționalității sistemului afacerilor interne, prin intermediul creșterii continue și adaptării nivelului de profesionalism al angajaților, al integrității instituționale și individuale, precum și aplicarea tehnologiilor informaționale contemporane drept instrumente avansate de muncă, în favoarea siguranței cetățeanului și a comunității.

CAPITOLUL I
DISPOZIŢII GENERALE

1. Conceptul are menirea de a contribui la implementarea unui sistem informațional în domeniul prevenirii și combaterii violenței în familie, proiectat ca parte integrată a componentei informaționale și de comunicații electronice a infrastructurii guvernării electronice din Republica Moldova.

2. Definirea SI Agresor

1) Denumirea completă: **Sistemul informațional de evidență agresorilor în cazurile de violență în familie**.

Abreviere: **SI Agresor**.

2) Resursa informațională formată de SI Agresor, reprezintă un ansamblu sistematizat de resurse și tehnologii informaționale, informații documentate, mijloace tehnice de program și metodologii, aflate în interconexiune și destinate evidenței persoanelor catalogate în categoria agresorilor, subiecți ai violenței în familie prevăzuți la art. 3 alin. (2) din Legea nr. 45/2007 cu privire la prevenirea și combaterea violenței împotriva femeilor și a violenței în familie; păstrării, prelucrării și utilizării informațiilor despre agresorii familiali în contextul situațiilor prevăzute la pct. 10 alin. (1), precum și automatizării proceselor și fluxurilor de lucru specifice domeniului prevenirii și combaterii violenței în familie.

3. SI Agresor servește drept instrument de susținere a activității organelor de drept, prin oferirea mijloacelor tehnice de colectare, administrare, prelucrare și interpretare a datelor, emiterea de liste, rapoarte, grafice, date statistice și comparative, despre agresorii familiali, informării autorităților publice centrale și autorităților administrației publice locale, persoanelor fizice și juridice despre serviciile și programele de reabilitare a agresorilor.

4. În sensul prezentului Concept se utilizează noțiunile definite în Legea nr. 45/2007 cu privire la prevenirea și combaterea violenței împotriva femeilor și a violenței în familie, Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat.

5. Scopurile SI Agresor

1) Scopul principal al SI Agresor constă în îmbunătățirea comunicării în cadrul sistemului afacerilor interne printr-o mai bună organizare a fluxului de informații dintre autoritățile administrative ale MAI și subdiviziunile polițienești teritoriale, dar și alte autorități publice centrale, organizații necomerciale și instituții abilitate cu competențe în domeniu, în vederea optimizării proceselor operaționale, sporirii eficienței instituționale și consolidării capacității de a asigura siguranța victimelor violenței în familie. Acest sistem propune să îmbunătățească colaborarea și coordonarea dintre autoritățile administrative și instituțiile din subordinea MAI, precum și să faciliteze comunicarea cu alte entități de drept public sau privat.

2) Scopurile specifice ale SI Agresor sunt:

a) sprijinirea autorităților publice și organizațiilor necomerciale în coordonarea acțiunilor privind implementarea mecanismului de soluționare a actelor de violență în familie;

b) asigurarea informațională a autorităților publice, în cazul prestării serviciilor de protecție a victimelor violenței în familie și serviciilor de reabilitare a agresorilor;

c) sporirea eficienței intervenției în soluționarea cazurilor de violență în familie și reducerea timpului necesar destinat soluționării cazului de violență în familie.

6. Principiile de bază ale SI Agresor sunt:

1) *principiul legitimității*, presupune că, funcțiile și operațiile realizate în SI Agresor de utilizatorii acestuia sunt de natură legală, în conformitate cu drepturile omului și legislația națională;

2) *principiul autenticității datelor,* conform căruia toate datele din sistemele informaționale ale participanților la schimbul de date, furnizate prin intermediul platformei de interoperabilitate (MConnect), se prezumă a fi autentice, se consideră integre și veridice și stau la baza actelor juridice, iar furnizorii de date sunt obligați să asigure integritatea și veridicitatea acestora;

3) *principiul confidențialității informației*, presupune răspunderea personală, în conformitate cu legislația, a persoanelor responsabile de prelucrarea informației în SI Agresor pentru utilizarea și difuzarea neautorizată a acesteia;

4) *principiul securității informaționale,* care presupune asigurarea nivelului dorit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, denaturării, distrugerii și utilizării neautorizate, rezistența la atacuri și protecția caracterului confidențial, a integrității, protecției datelor cu caracter personal;

5) *principiul identificării*, conform căruia pachetelor informaționale li se atribuie un cod unic la nivel de sistem, prin care este posibilă identificarea univocă și preferențierea la acestea;

6) *principiul destinației strategice,* presupune că destinatarii pot beneficia de date și informații exacte despre subiectul evidenței al SI Agresor, necesare pentru a elabora și implementa eficient politicile de prevenire și combatere a violenței în familie;

7) *principiul temeiniciei datelor*, presupune introducerea datelor în SI Agresor se efectuează doar în baza înscrierilor din documentele acceptate drept surse de informații;

8) *principiul stabilității,* constă în capacitatea sistemului de a funcționa eficient în condițiile oricăror modificări ale cadrului normativ;

9) *principiul extensibilității*, conform căruia, componentele SI Agresor oferă facilități de ajustare și de extindere a funcționalităților existente pentru conformare cu viitoarele necesități;

10) *principiul interoperabilității sistemelor informaționale*, ce presupune capacitatea tehnică a sistemelor informaționale și capacitatea organizatorică a participanților de a reutiliza date printr-un proces eficient de schimb de date;

11) *principiul integrității și auditului,* presupune unu sistem de audit și monitorizare regulată pentru a asigura conformitatea cu legislația și pentru a detecta eventuale abateri. Incidentele de neconformitate vor fi gestionate conform procedurilor stabilite;

12) *principiul accesibilității*, care va sigura că, SI Agresor este accesibil pentru toți utilizatorii autorizați, inclusiv pentru persoane cu dizabilități, prin implementarea unor soluții de accesibilitate digitală.

7. Obiectivele Sistemului sunt:

1) dezvoltarea unei soluții tehnice flexibile și moderne care permite formarea bazei naționale de date care cuprinde totalitatea informațiilor privind agresorii familiali, infracțiunile și contravențiile din domeniul prevenirii și combaterii violenței în familie, restricțiile aplicate față de aceștia și alte decizii relevante;

2) automatizarea procesului de sistematizare, ordonare, diseminare a informației cu privire la infracțiunile și contravențiile prevăzute la pct. 10 alin. (1) lit. b) și c);

3) oferirea unui mediu de lucru securizat;

4) posibilitatea de a genera date statistice și rapoarte personalizate în baza informațiilor stocate cu privire la agresorii familiali, cauzele penale și cele contravenționale pornite în privința acestora, deciziile instanțelor, aplicarea măsurilor de protecție, etc.;

5) oferirea suportului informațional organelor de constatare, de urmărire penală și celor ce efectuează activitatea specială de investigații;

6) instituirea unui mecanism de feedback care permite utilizatorilor să ofere sugestii și recomandări pentru îmbunătățirea funcționalității și eficienței SI Agresor;

7) implementarea unor algoritmi de inteligență artificială pentru analiza și identificarea pattern-urilor în datele colectate, pentru a sugera riscuri și nevoi suplimentare de intervenție;

8) implementarea unor module de analiză avansată pentru identificarea și raportarea tendințelor de violența în familie, pentru a sprijini prevenirea și intervenția pro-activă;

9) asigurarea accesului facilitat la resursele informaționale de stat prin intermediul platformei de interoperabilitate (MConnect);

10) implementarea procedurilor de control al accesului la date și asigurarea securității și confidențialității maxime a masivelor de date și a utilizatorilor.

8. Sarcinile de bază ale SI Agresor sunt:

1) oferirea unui instrument de lucru specialiștilor cu atribuții în domeniul prevenirii și combaterii violenței în familie, pentru evidența informațiilor cu privire la cazurile de violență în familie;

2) colectarea, stocarea și gestionarea datelor şi informațiilor privind cazurile de violență în familie, datelor despre agresorii familiali și victimele violenței în familie;

3) evidența datelor spațiale în format electronic cu privire la agresori, în cazurile de violență în familie;

4) publicarea datelor spațiale în diferite formate (raster, vector) pentru vizualizare;

5) asigurarea interoperabilității datelor spațiale din SI Agresor cu datele spațiale din alte sisteme informaționale (Registrul informației criminalistice și criminologice, Registrului de stat al contravențiilor, Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”, Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112, Registrul de stat al armelor, Sistemul informațional judiciar (Programul integrat de gestionare a dosarelor), Registrul procedurilor de executare, Registrul persoanelor reținute, arestate și condamnate, Registrul de Stat al Populației, Registrul dactiloscopic, Sistemul informațional geografic național, Registrul de stat al unităților administrativ-teritoriale și al străzilor din localitățile de pe teritoriul Republicii Moldova și alte sisteme informaționale relevante), în conformitate cu Regulamentul cu privire la normele de aplicare care stabilesc modalitățile tehnice de interoperabilitate și armonizare a seturilor și serviciilor de date spațiale, precum și termenul de implementare, aprobat prin Hotărârea Guvernului nr. 683/2018;

6) asigurarea descrierii datelor spațiale, a serviciilor de rețea și a condițiilor de utilizare a acestora pe Geoportalul infrastructurii naționale de date spațiale, conform prevederilor Regulamentului cu privire la normele de creare și actualizare a metadatelor pentru seturile și serviciile de date spațiale, aprobat prin Hotărârea Guvernului nr.738/2017.

7) acordarea de sprijin autorităților publice centrale în monitorizarea și pronosticarea fenomenului, la elaborarea și promovarea politicilor de prevenire și combatere a violenței în familie și de asistență socială a victimelor și agresorului;

8) oferirea unui mecanism pentru acces rapid la informațiile critice în situații de urgență, asigurând că datele necesare sunt disponibile imediat pentru intervenții rapide;

9) asigurarea unui mecanism de actualizare regulată și precisă a datelor despre agresori și cazuri de violență în familie, pentru a menține relevanța și acuratețea informațiilor din sistem;

10) asigurarea interacțiunii și colaborării informaționale pe parcursul schimbului informațional interministerial sau interdepartamental;

11) asigurarea vizualizării informației stocate (cu diverse niveluri de acces) și generarea de rapoarte predefinite și specifice.

CAPITOLUL II
SPAȚIUL JURIDICO-NORMATIV AL FUNCȚIONĂRII SISTEMULUI

9. Cadrul normativ al SI Agresor este constituit din legislația internațională în domeniu la care Republica Moldova este parte și legislația națională.

1) Printre actele internaționale cu relevanță în domeniu se menționează:

a) Convenția Consiliului Europei privind prevenirea și combaterea violenței împotriva femeilor și a violenței domestice (Convenției de la Istanbul), ratificată de Republica Moldova prin Legea nr. 144/2021;

b) Convenția asupra eliminării tuturor formelor de discriminare față de femei, ratificat prin Hotărârea Parlamentului nr. 87/1994.

2) Cadrul normativ-juridic al SI Agresor este întemeiat pe legislația națională, incluzând:

a) Constituția Republicii Moldova;

b) Codul penal al Republicii Moldova nr. 985/2002;

c) Codul de procedură penală al Republicii Moldova nr. 122/2003;

d) Codul contravențional al Republicii Moldova nr. 218/2008;

e) Codul de procedură civilă al Republicii Moldova nr. 225/2003;

f) Codul de executare al Republicii Moldova nr. 443/2004;

g) Legea nr. 45/2007 cu privire la prevenirea și combaterea violenței împotriva femeilor și a violenței în familie;

h) Legea nr. 148/2023 privind accesul la informațiile de interes public;

i) Legea nr. 1069/2000 cu privire la informatică;

j) Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat;

k) Legea nr. 71/2007 cu privire la registre;

l) Legea nr. 133/2011 privind protecția datelor cu caracter personal;

m) Legea nr. 124/2022 privind identificarea electronică și serviciile de încredere;

n) Legea nr. 142/2018 cu privire la schimbul de date și interoperabilitate;

o) Legea nr. 185/2020 cu privire la Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții;

p) Legea nr. 216/2003 cu privire la Sistemul informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni;

q) Hotărârea Guvernului nr. 947/2022 cu privire la aprobarea Programului de consolidare a încrederii și siguranței societății prin formare profesională, integritate și digitalizare a sistemului afacerilor interne pentru anii 2022-2025;

r) Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat;

s) Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal;

t) Hotărârea Guvernului nr. 650/2023 cu privire la aprobarea Strategiei de transformare digitală a Republicii Moldova pentru anii 2023-2030;

u) Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);

v) Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);

w) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);

x) Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);

y) Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017;

z) Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);

aa) Hotărârea Guvernului nr. 376/2020 pentru aprobarea Conceptului serviciului guvernamental de notificare electronică (MNotify) și a Regulamentului privind modul de funcționare și utilizare a serviciului guvernamental de notificare electronică (MNotify);

bb) Hotărârea Guvernului nr. 712/2020 cu privire la serviciul guvernamental de plăți electronice (MPay);

cc) Hotărârea Guvernului nr. 375/2020 pentru aprobarea Conceptului Sistemului informațional automatizat ,,Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) și a Regulamentului privind modul de ținere a Registrului împuternicirilor de reprezentare în baza semnăturii electronice;

dd) Decretul Președintelui Republicii Moldova nr. 1743/2004 privind edificarea societății informaționale în Republica Moldova;

ee) Reglementarea tehnică „Procesele ciclului de viață al software-ului” RT 38370656-002:2006, aprobată prin Ordin al ministrului dezvoltării informaționale nr. 78/2006;

ff) Ordinul viceministrului dezvoltării informaționale nr. 94/2009 cu privire la aprobarea unor reglementări tehnice.

gg) Ordinul comun al Ministerului Muncii și Protecției Sociale, Ministerului Afacerilor Interne, Ministerului Sănătății, Ministerului Justiției și Consiliului Național pentru Asistență Juridică Garantată de Stat nr. 48/298/610/162/5 din 22 iunie 2022 cu privire la aprobarea Instrucțiunii privind mecanismul de cooperare intersectorială în cazurile de violență în familie.

CAPITOLUL III.
SPAŢIUL FUNCŢIONAL AL SISTEMULUI

10. Funcțiile de bază ale SI Agresor sunt:

1) formarea resursei informaționale (Registrul agresorilor familiali).

Funcțiile de bază în procesul de formare a bazei de date a Sistemului sunt stocarea, actualizarea, păstrarea și arhivarea informației cu privire la agresorii familiali:

a) care au fost denunțați că creează sistematic situații de conflict în familie, manifestă comportament violent față de membrii de familie sau amenință membrii familiei cu moartea sau cu cauzarea vătămărilor corporale și există riscul eminent de realizare a acestor amenințări, privind violența:

- fizică;
- psihologică;
- sexuală;
- economică.

b) care au săvârșit infracțiunile prevăzute la: art. 145 alin. (2) lit. e^1), art. 171 alin. (2) lit. c) și alin. (3) lit. a) (în situația în care făptuitorul este membru de familie), art. 172 alin. (2) lit. c) alin. (3) lit. b) (în situația în care făptuitorul este membru de familie), art. 175 alin. (2) lit. c), art. 175^1 alin. (2) lit. b), art. 174 alin. (1^1) lit. a) (în situația în care făptuitorul este membru de familie), art. 201, art. 201^1 și art. 320^1 din Codul penal;

c) care au săvârșit contravențiile prevăzute de art. 78^1 și 318^1;

d) liberați condiționat de răspundere penală pentru actele de violență în familie;

e) condamnați cu suspendarea condiționată a executării pedepsei, pentru acte de violență în familie;

f) reținuți, arestați și condamnați pentru actele de violență în familie;

g) în privința cărora sunt aplicate măsuri de constrângere cu caracter medical;

h) în privința cărora au fost emise decizii privind obligarea de a participa la programe speciale de tratament sau de consiliere în vederea reducerii comportamentului violent;

i) în privința cărora au fost aplicate restricții prin ordinul de restricție de urgență;

j) în privința cărora au fost aplicate restricții prin ordonanță de protecție;

k) în privința cărora este aplicată monitorizarea electronică;

l) în privința cărora au fost emise alte decizii judiciare relevante (decăderea de drepturi părintești).

2) în sensul sbp. 1), asigurarea evidenței agresorilor familiali, se prezumă introducerea noilor informații în sistem, precum și preluarea prin interoperabilitate din alte sisteme a informațiilor cu privire la:

a) planul de prevenire terțiară cu agresorul familial;

b) informația despre antecedente penale (certificatul de cazier detaliat), care se va consuma prin interoperabilitate cu Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”, în baza IDNP-ului agresorului;

c) informații despre antecedente contravenționale (cazierul contravențional), care se va consuma prin interoperabilitate cu Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții, în baza IDNP-ului agresorului;

d) informația privind posesia armamentului, care se va consuma prin interoperabilitate cu Sistemul informațional automatizat „Registrul de stat al armelor”, în baza IDNP-ului agresorului;

e) referința autorității publice locale;

f) chestionarul de constatare și evaluare a riscurilor/letalității;

g) mențiuni referitoare la declarațiile vecinilor, rudelor, membrilor de familie, privind comportamentul agresorului familial;

h) evaluarea condițiilor de trai (realizat în procesul managementului de caz);

i) ordonanțele de protecție emise de către instanța de judecată;

j) ordinele de restricție de urgență;

k) mențiuni privind intervențiile echipelor multidisciplinare în cazurile violenței în familie;

l) informații privind participarea la programele de resocializare sau consiliere în centrele specializate, birourile de probațiune, în care agresorul familial a fost obligat de a participa prin decizia instanței judecătorești.

3) integrarea cu servicii de suport pentru și protecție a victimelor (adăposturi, consiliere psihologică), pentru a oferi un suport direct și coordonat;

4) actualizarea datelor SI Agresor constă în reînnoirea sistematică a bazei de date a acestuia în cazul modificării sau completării atributelor obiectelor de evidență;

5) radierea din evidență (schimbarea statutului) a obiectului de evidență, prin transferarea acestuia în arhivă după expirarea perioadei de 6 ani (arhiva rămâne parte componentă a SI Agresor);

6) asigurarea la nivel de stat a evidenței unice;

7) organizarea accesului la date. Datele conținute în banca de date a Sistemului sunt puse la dispoziția participanților pentru organizarea procesului de schimb informațional. Fiecare utilizator de date al Sistemului va accesa și va utiliza aceste date numai în scopuri legale, în conformitate cu drepturile de utilizator atribuite;

8) implementarea unui sistem de audit pentru a monitoriza și verifica accesul la date, asigurându-se că numai persoanele autorizate au acces la informațiile sensibile;

9) asigurarea multilaterală a funcționării Sistemului. Funcția respectivă presupune o interacțiune și integrare cu alte sisteme informaționale de stat sau cu servicii electronice guvernamentale;

10) asigurarea schimbului de date prin intermediul platformei de interoperabilitate (MConnect) cu alte resurse informaționale de stat;

11) asigurarea funcționării complexului tehnic de program și a rețelelor informaționale utilizate în cadrul Sistemului;

12) asigurarea calității informației, veridicității și plenitudinii informației la colectarea datelor din sursele primare, care se realizează prin crearea și menținerea componentelor sistemului de calitate;

13) asigurarea/introducerea unui mecanism de feedback pentru utilizatori, care să permită raportarea erorilor și îmbunătățirea continuă a calității informațiilor;

14) administrarea informațională, care include următoarele acțiuni:

a) administrarea rolurilor și drepturilor utilizatorilor;

b) administrarea nomenclatoarelor;

c) alte activități de administrare și acces la funcționalitățile Sistemului;

15) asigurarea integrității, protecției și securizării informațiilor la toate etapele de formare a băncii de date a Sistemului;

16) pregătirea rapoartelor statistice. Sistemul va genera statistici cu privire la obiectul informațional la toate etapele de colectare, stocare, prelucrare și utilizare a acestora;

17) mentenanța. Sistemul trebuie asigurat în permanență cu suportul și mentenanța necesară conform nivelului agreat de servicii (SLA).

11. Sistemul include următoarele contururi funcționale:

1) Conturul „Cazul de violență în familie”

2) Conturul „Evidența agresorilor familiali”;

3) Conturul „Evidența ordinelor de restricție de urgență”;

4) Conturul „Gestionarea nomenclatoarelor Sistemului”

5) Conturul „Gestionarea utilizatorilor și a rolurilor utilizatorilor Sistemului”;

6) Conturul „Generarea rapoartelor statistice personalizate”.

12. Conturul „Cazul de violență în familie”, presupune:

1) evidența plângerilor, denunțurilor, autodenunțurilor, sesizărilor și altor informații despre actele de violență în familie parvenite de la cetățeni, organul de constatare, autorități, organizații și instituții cu privire la:

a) situațiile de conflict în familie, în special cele care au un caracter sistematic, chiar dacă acestea se încadrează sau nu în norma penală sau contravențională;

b) actele de violență în familie fizică, psihologică, sexuală, economică;

c) aplicarea măsurilor de protecție;

d) emiterea deciziilor judiciare.

2) Pentru obiectul informațional „Cazul de violență în familie”, împrumutat nemijlocit în SI Agresor, datele de identificare sunt preluate prin interoperabilitate din Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112, Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”, Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”, Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții, Sistemul informațional judiciar (Programul integrat de gestionare a dosarelor - PIGD), Sistemul informațional automatizat „Registrul persoanelor reținute, arestate și condamnate” și se referă la:

a) identificator, autoritatea sau instituția care a înregistrat cazul de violență în familie:

- IDNO;
- denumirea autorității;

b) data și locul înregistrării cazului;

c) data, ora și locul producerii cazului;

d) sesizare, mod de sesizare;

e) date despre încadrarea cazului în tipul de violență în familie:

- violență fizică;
- violență sexuală;
- violență psihologică;
- violență economică;

f) încadrarea juridică (penală sau contravențională);

g) etapa urmăririi penale/procesului contravențional;

h) decizia pe cauza penală/contravențională adoptată;

i) subiecții violenței:

- IDNP al agresorului;
- IDNP al victimei;

j) relația dinte subiecți:

1. în condiția de conlocuire:

- persoanele aflate în căsătorie;
- persoanele aflate în divorț;
- persoanele în privința cărora a fost instituită o măsură de ocrotire judiciară;
- rudele;
- afinii rudelor;
- soții rudelor;

- persoanele aflate în relații asemănătoare celora dintre soți (concubinaj);
- persoanele aflate în relații dintre părinți și copii.

2. în condiția de locuire separată:

- persoanele aflate în căsătorie;
- persoanele aflate în divorț;
- rudele;
- afinii rudelor;
- copiii adoptivi;
- persoanele în privința cărora a fost instituită o măsură de ocrotire judiciară;
- persoanele care se află ori s-au aflat în relații asemănătoare celora dintre soți (concubinaj).

k) măsurile de protecție aplicate prin ordonanța de protecție:

- obligarea de a părăsi temporar locuința comună sau de a sta departe de locuința victimei, fără a decide asupra modului de administrare și dreptului de dispoziție asupra bunurilor;
- obligarea de a sta departe de locul aflării victimei, la o distanță ce ar asigura securitatea acesteia, excluzând și orice contact vizual cu victima sau cu copiii acesteia, cu alte persoane dependente de ea;
- interzicerea oricărui contact, inclusiv telefonic, prin corespondență sau în orice alt mod, cu victima sau cu copiii acesteia, cu alte persoane dependente de ea;
- interzicerea să se apropie de anumite locuri: locul de muncă al victimei, locul de studii al copiilor, alte locuri determinate pe care persoana protejată le frecventează;
- obligarea, de a contribui la întreținerea copiilor pe care îi are în comun cu victima;
- limitarea drepturilor în privința bunurilor comune cu victima;
- obligarea de a participa la programe speciale de tratament sau de consiliere în vederea reducerii comportamentului violent;
- interzicerea de a păstra și a purta armă;
- stabilirea unui regim temporar de vizitare a copiilor săi minori;

l) reținerea, arestarea și condamnarea persoanei pentru actele de violență în familie

m) aplicarea monitorizării electronice;

n) aplicarea măsurilor de constrângere cu caracter medical (alcoolism/drog/tulburări mintale);

o) decăderea din drepturile părintești;

p) alte decizii judiciare.

13. Conturul „Evidența agresorilor familiali”, se referă la datele:

a) de identificare a agresorului:

- IDNP al agresorului;
- nume, prenume;
- data nașterii;
- domiciliul;

Pentru obiectul informațional „agresor familial”, împrumutat nemijlocit în SI Agresor, datele de identificare sunt preluate prin interoperabilitate din Sistemul informațional automatizat „Registrul de stat al populației”.

b) date despre profilul agresorului:

- sex;
- relația cu victima;
- cetățenie;

- religie;
- starea civilă;
- nivelul de studii;
- statutul de muncă;
- persoane aflate la întreținere;
- etnie;
- aflare la evidență narcologică și/sau psihiatrică;
- deciziile adoptate în privința agresorului;
- restricțiile aplicate.

c) date de identificare a victimei:
- IDNP al victimei;
- nume, prenume;
- data nașterii;
- domiciliul;

Pentru obiectul informațional „victima”, împrumutat nemijlocit în SI Agresor, datele de identificare sunt preluate prin interoperabilitate din Sistemul informațional automatizat „Registrul de stat al populației”.

d) date despre profilul victimei:
- sex;
- relația cu agresorul;
- cetățenie;
- religie;
- starea civilă;
- nivelul de studii;
- statutul de muncă;
- persoane aflate la întreținere;
- etnie;
- aflare la evidență narcologică și/sau psihiatrică;
- decizii emise în privința victimei;
- măsuri de protecție a victimei, aplicate.

14. Conturul „Evidența ordinelor de restricție de urgență” conține instrumentele de evaluare a riscurilor/letalității și de emitere a ordinelor de restricție de urgență;

15. Conturul „Gestionarea nomenclatoarelor Sistemului” conține instrumentele de creare și de modificare a listelor interne ale valorilor ce vor fi introduse în actele de evidență în procesul utilizării Sistemului în cazurile de violență în familie, pentru evitarea erorilor umane. Acestea includ articolele Codului penal, Codului contravențional, Codului de procedură civilă, Codului de executare, prevederile actelor normative, lista instituțiilor, organelor de stat, municipiilor, orașelor, străzilor și altele.

16. Conturul „Gestionarea utilizatorilor și a rolurilor utilizatorilor Sistemului” presupune că Sistemul conține informații de bază despre toți utilizatorii acestuia, grupurile de utilizatori și nivelurile de acces. Fiecărui utilizator îi este atribuit un singur rol;

17. Conturul „Generarea rapoartelor statistice personalizate” permite crearea rapoartelor statistice depersonalizate, cu/fără aplicarea anumitor filtre de dezagregare (data, localitatea (urban/rural), sexul, ocupația, studiile, vârsta, relația familială, decizii adoptate, instituția care a sesizat cazul, articolul, altele).

Capitolul IV

STUCTURA ORGANIZAȚIONALĂ A SISTEMULUI

18. Subiecții raporturilor juridice aferenți creării, administrării, mentenanței dezvoltării și utilizării SI Agresor sunt:

1) proprietarul sistemului informațional;

2) posesorul sistemului informațional;

3) deținătorul sistemului informațional;

4) administratorul tehnic al sistemului informațional;

5) utilizatorii sistemului informațional.

19. Proprietarul Sistemului este statul, care își realizează dreptul de proprietate, gestionare și utilizare a datelor din acesta.

20. Posesorul Sistemului informaționale este Ministerul Afacerilor Interne, ale cărui drepturi și obligații sunt stabilite în conformitate cu Legea nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat. Sistemul este înscris în Registrul resurselor și sistemelor informaționale de stat.

21. Deținătorul SI Agresor este Serviciul Tehnologii Informaționale al Ministerului Afacerilor Interne care asigură totalitatea activităților de suport, mentenanță și dezvoltare continuă a SI Agresor.

22. Administratorului tehnic al SI Agresor este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care administrează infrastructura tehnică (hardware și software), de întreținere și implementează politicile de securitate ale SI Agresor.

23. Utilizatorii SI Agresor sunt:

1) registratorii;

2) furnizorii de date;

3) destinatarii.

24. Registratorul datelor Sistemului este angajatul desemnat în cadrul entității pentru înregistrare și evidență statistică, operatorii unităților operaționale de coordonare din cadrul autorităților administrative și instituțiilor din subordinea Ministerului Afacerilor Interne, care înregistrează cazurile de violență în familie și în funcție de competențele funcționale are acces la următoarele conturi:

1) Conturul „Evidența cazului de violență în familie”;

2) Conturul „Evidența agresorilor familiali”;

3) Conturul „Evidența ordinelor de restricție de urgență”;

25. Furnizorul datelor Sistemului este autoritatea, instituția, organizația, persoana fizică sau persoana juridică de drept privat sau public care prezintă registratorului datele cu privire la cazurile de violență în familie în modul stabilit de lege sau de acord;

26. Funcțiile de furnizor al SI Agresor sunt exercitate de către:

1) Ministerul Afacerilor Interne, prin intermediul:

a) autorităților administrative din subordinea Ministerului Afacerilor Interne, care în funcție de competențele funcționale, înregistrează cazurile de violență în familie sesizate;

b) subdiviziunilor specializate și teritoriale ale Poliției, care identifică, înregistrează și actualizează în banca de date cu privire la cazurile de violență în familie sesizate;

c) angajaților Poliției, care furnizează informații privind cazurile de violență în familie, eliberarea ordinului de restricție de urgență, informarea agresorului despre restricțiile aplicate în privința acestuia;

2) Ministerul Muncii și Protecției Sociale, prin intermediul:

a) Agențiilor teritoriale de asistență socială, care implementează direct și prin intermediul structurilor teritoriale de asistență socială, politica de stat în domeniul prevenirii și combaterii violenței în familie;

b) Structurilor teritoriale de asistență socială, structurilor responsabile de asistența socială și protecția drepturilor copilului din municipiul Chișinău și din unitatea teritorială autonomă Găgăuzia, prin intermediul serviciului responsabil de domeniul prevenirii și combaterii violenței în familie și al reabilitării victimelor infracțiunii care înregistrează și actualizează informațiile în baza de date la nivel teritorial cu privire la cazurile de violență în familie;

c) Centrelor și serviciilor de reabilitare a victimelor și agresorilor, care furnizează informații privind serviciile acordate victimelor și agresorilor, asistența oferită victimelor prin ordonanța de protecție și restricțiile aplicate în privința agresorului;

3) Ministerul Educației și Cercetării, prin intermediul direcțiilor generale de învățământ, tineret și sport, care furnizează informații în adresa autorităților tutelare și Poliției privind sesizarea de către cadrele didactice a cazurilor de violență în familie, inclusiv despre cazurile de violență în familie împotriva copiilor;

4) Ministerul Sănătății, prin intermediul instituțiilor medicale de toate tipurile și nivelurile, care furnizează informații în adresa autorităților tutelare și Poliției privind sesizarea de către cadrele medicale a cazurilor de violență în familie;

5) Ministerul Justiției, prin intermediul:

a) Administrației Naționale a Penitenciarelor, care furnizează informații privind realizarea programelor de corecție pentru agresorii familiali în penitenciare, precum și informații cu privire la informarea victimei despre eliberarea din detenție a agresorului;

b) Inspectoratului Național de Probațiune, care furnizează informații privind realizarea programelor probaționale, aplicarea monitorizării electronice și tentativele de încălcare a măsurilor de protecție aplicate de către instanța de judecată.

6) Procuratura Generală, care prin intermediul procuraturilor teritoriale, furnizează registratorului informații cu privire la:

a) liberarea condiționată a persoanei de răspundere penală pentru actele de violență în familie;

b) expedierea cauzei penale în instanța de judecată.

7) Consiliul Național pentru Asistență Juridică Garantată de Stat, prin intermediul oficiilor teritoriale, care oferă asistență juridică gratuită victimelor violenței în familie. Aceste oficii asigură suport legal și reprezentare în instanță pentru a proteja drepturile și siguranța victimelor.

27. Destinatarul datelor Sistemului este autoritatea publică centrală, instituția, organizația, persoana fizică sau juridică, mandatată cu dreptul de a primi datele despre cazurile de violență în familie din Sistem, în modul și nivelul de acces stabilit de actele normative. Destinatarul are acces de vizualizare la următoarele contururi, cu restricționarea de a introduce unele date și de a modifica datele introduse:

1) Conturul „Evidența cazului de violență în familie”;

2) Conturul „Evidența agresorilor familiali”;

3) Conturul „Evidența ordinelor de restricție de urgență”;

4) Conturul „Generarea rapoartelor statistice personalizate”.

28. Destinatarii datelor SI Agresor sunt următoarele autorități și instituții abilitate cu funcții de prevenire și de combatere a violenței în familie:

1) autoritățile publice centrale de specialitate:

a) Agenția Națională de Prevenire și Combatere a Violenței împotriva Femeilor și a Violenței în Familie;

b) Ministerul Afacerilor Interne;

b) Ministerul Muncii și Protecției Sociale;

c) Ministerul Educației și Cercetării;

d) Ministerul Sănătății;

e) Ministerul Justiției.

2) agențiile teritoriale de asistență socială;

3) autoritățile de specialitate ale administrației publice locale de nivelul al doilea şi structurile desconcentrate:

a) subdiviziunile teritoriale ale poliției;

b) structurile teritoriale de asistență socială, structurile responsabile de asistența socială și protecția drepturilor copilului din municipiul Chișinău și din unitatea teritorială autonomă Găgăuzia;

c) direcțiile generale de învățământ, tineret și sport;

d) organele ocrotirii sănătății.

4) administrația publică locală de nivelul întâi;

a) comisiile pentru probleme sociale de pe lingă autoritățile administrației publice locale;

b) centrele/serviciile de asistență și protecție a victimelor violenței în familie și a copiilor lor și centrele/serviciile de asistență și consiliere pentru agresorii familiali.

5) procuraturile teritoriale;

6) instanțele de judecată;

7) inspectoratele regionale și birourile de probațiune;

8) penitenciarele;

9) alte organizații cu activități specializate în domeniu.

29. Nivelul de acces al registratorilor, furnizorilor și destinatarilor de informații în cadrul SI Agresor este reglementat de actele normative, în funcție de statutul lor juridic, precum și de statutul juridic al informației destinate identificării, înregistrării, furnizării și utilizării acesteia. Pentru asigurarea monitorizării conformității cu regulamentele de acces și pentru a identifica și preveni potențiale abuzuri sau neconformități, sistemul va fi supus misiunilor periodice de audit.

30. Procedurile de identificare, înregistrare și raportare a cazurilor de violență în familie, inclusiv asupra copiilor, precum și delimitarea funcțiilor de înregistrare și furnizare a informației în SI Agresor, inclusiv de utilizare a informațiilor de către destinatari, se stabilesc prin Regulamentul resursei informaționale formate de SI Agresor.

31. Regulamentul va include, de asemenea, un mecanism de colectare a feedback-ului de la utilizatori și va prevedea actualizări periodice pentru a reflecta schimbările legislative și pentru a răspunde nevoilor utilizatorilor, precum și cerințe pentru dezvoltarea planurilor de continuitate a activității și gestionarea crizelor. Aceste planuri vor asigura funcționarea neîntreruptă a SIA Agresor în cazul unor incidente majore sau de urgență și vor include măsuri de recuperare rapidă a datelor.

32. Drepturile și obligațiile deținătorului și al utilizatorilor SI Agresor se stabilesc, în conformitate cu cadrul normativ din domeniul informatizării și al resurselor informaționale de stat și a Regulamentului privind modul de ținere a resursei informaționale formate de SI Agresor.

Capitolul V
DOCUMENTELE SISTEMULUI

33. În cadrul SI Agresor se utilizează următoarele clasificări de documente:

1) documentele de intrare, care sunt fundamentale pentru introducerea datelor în sistem;

2) documentele de ieșire, obținute în urma funcționării sistemului;

3) documentele tehnologice.

34. Documente de intrare includ:

1) cererile și sesizările cetățenilor, instituțiilor abilitate cu competențe de prevenire și combatere a violenței în familie, centrelor de medicină legală privind conflictele familiale, actele de violență, amenințările cu moartea sau existența unui pericol iminent de realizare a acestora;

2) rapoartele de constatare ale subdiviziunilor polițienești (de sector/teritoriale/regionale) și organelor procuraturii despre cazurile de violență în familie, inclusiv actele aferente instrumentului de evaluare a riscurilor, instrumentului de evaluare a letalității

3) ordinele de restricție de urgență;

4) adresările către autoritățile judecătorești privind obținerea ordonanței de protecție

5) fișele de referire către alte autorități a cazurilor de violență în familie și fișele de sesizare în cazurile copiilor aflați în situație de risc;

6) deciziile comisiilor autorităților administrației publice locale asupra problemelor sociale despre existența violenței în familie sau pericolului pentru viața și sănătatea victimei ca urmare aplicării măsurilor de protecție;

7) cererile de plasament ale victimelor în cazul în care izolarea acestora de agresor se impune ca măsură de protecție;

8) cererile întemeiate ale victimelor de retragere a măsurilor de protecție;

9) ordonanțele de protecție emise de către instanța de judecată;

10) solicitările organelor de drept privind înlesnirea accesului agresorului la programele de reabilitare;

11 informațiile privind convocarea echipelor multidisciplinare în soluționarea cazului;

12 informațiile privind acordarea asistenței psihologice, pedagogice, sociale și juridice, îngrijirii medicale a membrilor de familie care sunt sau care pot fi victime;

13 informațiile privind asigurarea accesului agresorilor, inclusiv celor aflați în arest, la serviciile de reabilitare;

14) informațiile centrelor și serviciilor de reabilitare a agresorilor despre acordarea asistenței psihologice și sociale agresorilor, despre instruirea, recalificarea și plasarea în câmpul muncii a agresorilor, despre ridicarea măsurilor de protecție și de reintegrare în familii a agresorilor;

15) informațiile instituțiilor medicale de tratament specializat (alcoolism/droguri/ sănătate mintală), privind asistența acordată agresorilor familiali;

16) informațiile Administrației Naționale a Penitenciarelor, privind realizarea programelor de corecție pentru agresorii familiali în penitenciare;

17) informațiile Inspectoratului Național de Probațiune, privind organizarea programelor probaționale, aplicarea monitorizării electronice și tentativele de încălcare a măsurilor de protecție aplicate de către instanța de judecată.

18) informațiile procuraturilor teritoriale cu privire la liberarea condiționată a persoanei de răspundere penală pentru actele de violență în familie;

19) alte documente de identificare, constatare și instrumentare a cazurilor de violență în familie ale instituțiilor abilitate cu competențe în domeniul prevenirii și combaterii violenței în familie.

35. Documente de ieșire, sunt documente generate în baza datelor stocate în cadrul funcționării Sistemului, care includ:

1) rapoartele de studii și generalizare a cauzelor și condițiilor care au favorizat comiterea actelor de violență în familie;

2) rapoartele trimestriale ale actorilor (poliție, asistența socială, medicină) abilitați cu competențe în domeniul prevenirii și combaterii violenței în familie, despre activitățile desfășurate în teritoriu, conform parteneriatelor stabilite;

3) rapoartele analitice și statistice.

Documentele de ieșire vor fi utilizate pentru îmbunătățirea politicilor și măsurilor de prevenire a violenței în familie. Aceste documente vor fi distribuite către toate părțile interesate și vor fi utilizate în procesul de luare a deciziilor pentru optimizarea intervențiilor și strategiilor.

36. Documente tehnologice, includ:

1) Ghiduri, nomenclatoare, glosare:

a) ghidul de utilizare a SI Agresor

b) glosarul de termeni și definiții;

c) nomenclatorul restricțiilor aplicate prin ordinul de restricție de urgență;

d) nomenclatorul măsurilor aplicate agresorului prin ordonanța de protecție;

2) Registre, cereri, chestionare, tabele statistice și altele.

a) fișa de înregistrare a cazului de violență în familie;

b) proces verbal cu privire la contravenție;

c) registru de evidență nominală a agresorilor;

d) registrele cazurilor de violență în familie;

e) planul de prevenire terțiară cu agresorul familial

f) chestionare de evaluare a riscurilor;

g) chestionarul de evaluare a letalității;

h) informația despre antecedente penale (certificatul de cazier detaliat)

i) informații despre antecedente contravenționale (cazierul contravențional);

j) informația privind posesia armamentului

k) referința autorității publice locale;

l) chestionar de evaluare a condițiilor de trai (realizat în procesul managementului de caz);

m) ordonanțele de protecție emise de către instanța de judecată;

n) ordinele de restricție de urgență;

o) procese-verbale ale ședințelor echipelor multidisciplinare;

p) alte documente tehnologice necesare funcționării și dezvoltării sistemului.

Capitolul VI
SPAȚIUL INFORMAȚIONAL AL SISTEMULUI

37. Spațiul informațional al SI Agresor cuprinde totalitatea obiectelor informaționale, cu atributele și identificatorii lor și include:

1) Obiectul informațional „Cazul de violență în familie”;

2) Obiectul informațional „Agresor familial”;

3) Obiectul informațional „Victima violenței în familie”;

4) Obiectul Informațional „Ordin de restricție de urgență”.

38. Obiectul informațional „Cazul de violență în familie” include datele privind sesizările referitoare la actele de violență în familie, situațiile de conflict în familie, în special cele care au un caracter sistematic, chiar dacă acestea se încadrează sau nu în norma penală sau contravențională, cauzele penale/contravenționale pornite pentru actele de violență în familie.

39. Identificatorul obiectului informațional „Cazul de violență în familie” al SI Agresor este numărul de înregistrare în sistem și atributelor acestuia, împrumutate în SI Agresor, datele de identificare fiind preluate din Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112, Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”, Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”, Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții.

40. Obiectul informațional „Agresor familial”, include:

a) datele de identitate a agresorului familial, care se va consuma prin interoperabilitate din Sistemul informațional automatizat „Registrul de stat al populației:

- IDNP al agresorului;
- nume, prenume;
- data nașterii;
- domiciliul;

b) date privind profilul agresorului:

c) planul de prevenire terțiară cu agresorul familial;

d) date despre antecedente penale ale agresorului (certificatul de cazier detaliat), care se va consuma prin interoperabilitate cu Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”, în baza IDNP-ului agresorului;

e) date despre antecedente contravenționale ale agresorului (cazierul contravențional), care se va consuma prin interoperabilitate cu Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții, în baza IDNP-ului agresorului;

f) date despre posesia de către agresor a armamentului, care se va consuma prin interoperabilitate cu Sistemul informațional automatizat „Registrul de stat al armelor”, în baza IDNP-ului agresorului;

g) referința autorității publice locale, în privința agresorului familial;

h) evaluarea condițiilor de trai ale agresorului (realizat în procesul managementului de caz);

i) date despre măsurile de protecție aplicate prin ordonanța de protecție emisă de către instanța de judecată, care se va consuma prin interoperabilitate cu Programul Integrat de Gestionare a Dosarelor (PIGD), sau, după caz cu nomenclatorul intern al SI Agresor;

j) ordinele de restricție de urgență, se vor prelua nomenclatorul intern al SI Agresor;

k) date despre intervențiile echipelor multidisciplinare în cazurile violenței în familie;

l) date cu privire la participarea agresorului în cadrul programelor de resocializare sau consiliere în centrele specializate, birourile de probațiune, în care agresorul familial a fost obligat de a participa prin decizia instanței judecătorești.

41. Identificatorul obiectului informațional „Agresor familial” este numărul de ordine, generat de sistem cu următoarea structură:

A/X-NNNN/YYYY-OO, în care:

A – reprezintă identificatorul obiectului informațional „Agresor familial”;

X – este prima literă alfabetică a numelui agresorului familial;

NNNN – este numărul de ordine în anul curent;

YYYY – corespunde cu anul de înregistrare;

OO – reprezintă codul organului care a înregistrat agresorul.

Dacă identitatea agresorului familial este cunoscută, la acest identificator se vor conexa seturi de date generale, preluate prin interoperabilitate din Sistemul informațional automatizat „Registrul de stat al populației”:

- IDNP al agresorului;
- nume, prenume;
- data nașterii;
- domiciliul;

Alte informații cu privire la agresorul familial, sunt preluate din alte sisteme prin interoperabilitate in raport cu acest obiect informațional, precum și din alte obiecte informaționale din cadrul SI Agresor (spre exemplu: din obiectul informațional „Victima violenței în familie – în cazul în care pot fi înregistrate mai multe victime (soția și copilul), sau la obiectul informațional „Cazul de violență în familie” – în cazul în care agresorul comite mai multe acte de violență în familie).

În cazul în care numărul de identificare de stat IDNP al agresorului lipsește sau nu este cunoscut, se folosește un număr intern de identificare unic și repetabil generat automat de SI Agresor. În cazul în care numărul de identificare de stat IDNP devine cunoscut, acesta substituie automat numărul intern de identificare generat de sistem.

42. Obiectul informațional „Victima violenței în familie”, include:

a) datele de identitate a victimei violenței în familie, care se va consuma prin interoperabilitate din Sistemul informațional automatizat „Registrul de stat al populației:

- IDNP al victimei;
- nume, prenume;
- data nașterii;
- domiciliul;

b) date privind profilul victimei:

- sex;
- relația cu agresorul;
- cetățenie;
- religie;
- starea civilă;
- nivelul de studii;
- locul de muncă;
- persoane aflate la întreținere;
- etnie.

c) date cu privire la evaluarea condițiilor de trai a victimei (realizat în procesul managementului de caz);

d) date despre asistența specializată acordată:
- asistența juridică garantată de stat;
- asistența socială;
- asistența medicală;
- asistența psihologică;
- plasament/consiliere.

e) date despre măsurile de protecție de care beneficiază, aplicate prin ordonanța de protecție emisă de către instanța de judecată, care se va consuma prin interoperabilitate cu Programul Integrat de Gestionare a Dosarelor (PIGD), sau, după caz cu nomenclatorul intern al Sistemului;

f) date despre măsurile de protecție provizorie de care beneficiază, aplicate prin ordinul de restricție de urgență, se vor prelua din nomenclatorul intern al sistemului;

g) date despre intervențiile echipelor multidisciplinare în cazurile violenței în familie.

43. Identificatorul obiectului informațional „Victima violenței în familie” este numărul de ordine, generat de sistem cu următoarea structură:

V/X-NNNN/YYYY-OO, în care:

V – reprezintă identificatorul obiectului informațional „Victima violenței în familie”;

X – este prima literă alfabetică a numelui victimei violenței în familie;

NNNN – este numărul de ordine în anul curent;

YYYY – corespunde cu anul de înregistrare;

OO – reprezintă codul organului care a înregistrat victima.

Dacă identitatea victimei violenței în familie este cunoscută, la acest identificator se vor conexa seturi de date generale, preluate prin interoperabilitate din Sistemul informațional automatizat „Registrul de stat al populației”:

- IDNP al victimei;
- nume, prenume;
- data nașterii;
- domiciliul.

În cazul în care numărul de identificare de stat IDNP al victimei lipsește sau nu este cunoscut, se folosește un număr intern de identificare unic și repetabil generat automat de sistem. În cazul în care numărul de identificare de stat IDNP devine cunoscut, acesta substituie automat numărul intern de identificare generat de sistem.

44. Obiectul informațional „Ordine de restricție de urgență”, include date despre:

a) ordine de restricție de urgență în acțiune;

b) ordine de restricție de urgență expirate.

45. Identificatorul obiectului informațional „Ordine de restricții de urgență” al SI Agresor este numărul de înregistrare în sistem a ordinelor de restricție de urgență, conexat cu seturile de date generale, preluate prin interoperabilitate din Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”, Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții și Sistemul informațional automatizat „Registrul de stat al populației”.

46. Identificarea obiectului informațional „Ordine de restricții de urgență” se efectuează cu utilizarea numerelor de ordine și a anului emiterii, cu următoarea structură:

ORUYYYYOONNNNN, în care:

„ORU” – reprezintă identificatorul obiectului informațional „Ordine de restricție de urgență”;

„YYYY” – corespunde cu anul de înregistrare;

„OO” – codul organului care a înregistrat documentul;

„NNNNN” – numărul de ordine în anul curent.

47. Datele cu privite la „persoana juridică” reprezintă numărul de identificare de stat a persoanei juridice (IDNO) în calitate de utilizator al SI Agresor și sunt preluate prin operabilitate din Sistemul informațional automatizat „Registrul de stat al unităților de drept”.

48. Scenariile de bază reprezintă o listă de evenimente ce se produc cu obiectul informațional și se țin în evidență în SI Agresor. În prezentul Sistem, scenariul de bază include, pe de o parte, realizarea funcțiilor sale legate de introducerea, actualizarea și scoaterea informației din evidență cu transferarea acesteia în arhivă și, pe de altă parte, furnizarea informației ori generarea rapoartelor.

49. Grupa scenariilor legate de introducerea, actualizarea și scoaterea din evidență a informației, interacționează cu obiectele informaționale ale SI Agresor, după cum urmează:

1) pentru obiectul informațional „Cazul de violență în familie”:

1.1 introducerea în evidență primară a cazurilor de violență în familie se efectuează la:

a) recepționarea cererii sau sesizării cetățenilor privind conflictele familiale și actele de violență, inclusiv depuse prin e-mail sau pe pagina oficială;

b) preluarea apelului telefonic;

c) primirea corespondenței oficiale prin subdiviziunea de management documente;

d) depunerea raportului de autosesizare;

e) preluarea fișei semnalării din Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112;

f) recepționarea informațiilor instituțiilor medicale/centrelor de medicină legală;

g) preluarea rapoartelor de constatare ale subdiviziunilor polițienești (de sector/teritoriale/regionale) despre cazurile de violență în familie, inclusiv actele aferente instrumentului de evaluare a riscurilor, instrumentului de evaluare a letalității

h) recepționarea fișelor de referire parvenite de la alte autorități a cazurilor de violență în familie

i) recepționarea fișelor de sesizare în cazurile copilului aflat în situație de risc și victimă a violenței în familie;

j) preluarea sesizărilor direcțiilor generale de învățământ, tineret și sport despre cazurile de violență în familie, inclusiv despre cazurile de violență în familie asupra copiilor;

k) primirea sesizărilor structurilor teritoriale de asistență socială, structurilor responsabile de asistența socială și protecția drepturilor copilului din municipiul Chișinău și din unitatea teritorială autonomă Găgăuzia, prin intermediul serviciului responsabil de domeniul prevenirii și combaterii violenței în familie și al reabilitării victimelor infracțiunii;

l) primirea sesizărilor comisiilor autorităților administrației publice locale asupra problemelor sociale despre existența violenței în familie sau pericolului pentru viața și sănătatea victimei ca urmare aplicării măsurilor de protecție.

m) recepționarea informațiilor parvenite din partea centrelor de plasament pentru victimele violenței în familie, privind plasarea în centru a victimei și acordarea acesteia a asistenței calificate;

n) primirea sesizărilor din partea Consiliului Național de Asistență Juridică Garantată de Stat, în cazul în care victima nu s-a adresat inițial la Poliție;

o) primirea deciziilor instanțelor de judecată, privind aplicarea restricțiilor prin ordonanța de protecție, sau alte decizii cu caracter obligatoriu.

1.2 actualizarea datelor se efectuează la recepționarea informației suplimentare cu referință la sesizarea preluată anterior.

1.3 scoaterea din evidență a sesizării (schimbarea statutului) se efectuează la transferarea sesizării din statut activ în cel inactiv, cu transmiterea ulterioară în baza de date de evidență a cauzelor penale, contravenționale, în baza ordonanței procurorului (hotărârii judecătorului) de neîncepere a urmăririi penale ori semnare a încheierii de încetare a controlului sesizării, cu transmiterea în arhivă a sesizărilor înregistrate.

Pentru obiectul informațional „Cazul de violență în familie", scenariile de bază legate introducerea în evidență, actualizarea datelor și scoaterea din evidență se poate consuma prin interoperabilitate cu Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112, Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică", Sistemul informațional automatizat „Registrul informației criminalistice și criminologice", Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții, Sistemul informațional judiciar (Programul integrat de gestionare a dosarelor - PIGD) și alte sisteme cu care inter-operează SI Agresor.

2) pentru obiectul informațional „Agresor familial":

2.1 introducerea inițială se efectuează la:

a) înregistrarea cazului de violență în familie prevăzut la grupa scenariilor care fac obiectul informațional „Cazul de violență în familie";

b) pornirea urmăririi penale pentru infracțiunile prevăzute la pct. 10 alin. (1) lit. b);

c) întocmirea procesului-verbal cu privire la contravenție pentru contravențiile prevăzute la pct. 10 alin. (1) lit. c);

d) emiterea ordinului de restricție de urgență;

e) adoptarea deciziei instanțelor de judecată.

2.2 actualizarea datelor se efectuează la recepționarea informației suplimentare despre persoanele implicate într-o situație care face obiectul informațional;

2.3. scoaterea din evidență se efectuează în cazul:

a) stabilirii faptului că datele introduse inițial cu privire la agresorul familial sunt eronate;

b) adoptării deciziei cu privire la scoaterea din evidența specială;

c) decesului sau recunoașterii de către instanța de judecată a decesului persoanei;

d) clasării urmăririi penale pe motiv de reabilitare;

e) clasării cauzei contravenționale.

Pentru obiectul informațional „Agresor familial", scenariile de bază legate introducerea în evidență, actualizarea datelor și scoaterea din evidență se poate consuma prin interoperabilitate cu Sistemul informațional automatizat „Registrul de stat al populației", Sistemul informațional automatizat „Registrul informației criminalistice și criminologice", Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții, Sistemul

informațional judiciar (Programul integrat de gestionare a dosarelor - PIGD) și alte sisteme cu care inter-operează SI Agresor.

3) pentru obiectul informațional „Victima violenței în familie”:

3.1 introducerea inițială se efectuează la:

a) orice sesizare, în care există o bănuială rezonabilă că persoana (adultă/copil) a fost supusă actelor de violență în familie

b) acordarea asistenței specializate:

- asistența juridică garantată de stat;
- asistența socială;
- asistența medicală;
- asistența psihologică;
- plasament/consiliere.

c) aplicarea măsurilor de protecție prin ordonanța de protecție emisă de către instanța de judecată,

d) la acordarea protecției provizorie prin ordinul de restricție de urgență.

3.2 actualizarea datelor se efectuează la recepționarea informației suplimentare despre persoanele implicate într-o situație care face obiectul informațional;

3.3. scoaterea din evidență se efectuează în cazul:

a) stabilirii faptului că datele introduse inițial cu privire la victima violenței în familie sunt eronate;

b) adoptării deciziei cu privire la radierea din evidență;

c) decesului sau recunoașterii de către instanța de judecată a decesului persoanei;

d) clasării urmăririi penale/cauzei contravenționale.

Pentru obiectul informațional „Victima violenței în familie”, scenariile de bază legate introducerea în evidență, actualizarea datelor și scoaterea din evidență se poate consuma prin interoperabilitate cu Sistemul informațional automatizat „Registrul de stat al populației”, Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”, Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții, Sistemul informațional judiciar (Programul integrat de gestionare a dosarelor - PIGD) și alte sisteme cu care inter-operează SI Agresor.

4) pentru obiectului informațional „Ordine de restricții de urgență”:

4.1 introducerea în evidență primară se efectuează la:

a) întocmirea chestionarului de constatare și evaluare a riscurilor în cazurile de violență în familie;

b) aplicarea instrumentului de evaluare a letalității;

c) la emiterea ordinului de restricție de urgență;

4.2. actualizarea informației se efectuează la:

a) emiterea deciziei de către instanța de judecată, ca urmare a căilor de atac;

b) ordinului de restricție de urgență repetat;

c) eschivarea de la executare sau neexecutarea ordinului de restricție de urgență;

d) încetarea acțiunii ordinului de restricție odată cu aplicarea măsurilor de protecție stabilite de instanța de judecată.

4.3. scoaterea din evidență și transferarea în arhivă a datelor despre ordinul de restricție de urgență se efectuează la:

a) încetarea perioadei de evidență;

b) actul emis a fost clasat în instanța de judecată;

c) expirarea perioadei de gestionare.

50. Datele SI Agresor reprezintă o totalitate a atributelor obiectelor informaționale și includ:

1) date despre cazul de violență în familie:

a) numărul de înregistrare a sesizării despre violența în familie;

b) data și timpul înregistrării;

c) unde a fost înregistrată (Registrul 1, 2 etc.);

d) codul organului teritorial din subordinea Ministerului Afacerilor Interne care a înregistrat sesizarea;

e) data, ora și locul comiterii faptei;

f) datele despre subiecții violenței în familie (victima/agresor, nume, prenume, data nașterii, datele de contact și adresa de domiciliu, telefon);

g) date despre copii sau alte persoane cu dizabilități/în etate implicate (victime);

h) descrierea succintă a cazului (fabula);

i) conexarea cu alte sesizări/semnalări;

j) datele privind resursele care au participat la intervenție (solicitarea serviciilor specializate de urgență, plasarea victimei în Centrul de plasament, etc.);

k) statutul examinării sesizării;

l) încadrarea juridică penală/contravențională;

m) decizia adoptată;

n) măsurile de protecție aplicate prin ordonanța de protecție;

o) alte decizii cu caracter de consiliere, tratament sau de constrângere emise

Pentru obiectul informațional „Cazul de violență în familie”, se păstrează datele de identificare împrumutate din Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112, Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”, Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”, Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții, Sistemul informațional judiciar (Programul integrat de gestionare a dosarelor - PIGD), alte sisteme cu care inter-operează SI Agresor, precum și datele din nomenclatorul intern al SI Agresor.

2) datele despre agresorul familial:

a) date de identificare a agresorului:

- IDNP al agresorului;
- nume, prenume;
- data nașterii;
- domiciliul;

b) date despre profilul agresorului:

- sex;
- relația cu victima;
- cetățenie;
- religie;

- starea civilă;
- nivelul de studii;
- statutul de muncă;
- persoane aflate la întreținere;
- etnie;
- aflare la evidență narcologică și/sau psihiatrică;
- deciziile adoptate în privința agresorului;
- restricțiile aplicate

Pentru obiectul informațional „agresor familial”, împrumutat nemijlocit în SI Agresor, datele de identificare sunt preluate prin interoperabilitate din Sistemul informațional automatizat „Registrul de stat al populației”, alte sisteme cu care inter-operează SI Agresor, precum și datele din nomenclatorul intern al SI Agresor.

3) Date despre victima violenței în familie:

a) date de identificare a victimei:
- IDNP al victimei;
- nume, prenume;
- data nașterii;
- domiciliul;

d) date despre profilul victimei:
- sex;
- relația cu agresorul;
- cetățenie;
- religie;
- starea civilă;
- nivelul de studii;
- statutul de muncă;
- persoane aflate la întreținere;
- etnie;
- aflare la evidență narcologică și/sau psihiatrică
- decizii emise în privința victimei;
- măsuri de protecție a victimei, aplicate.

Pentru obiectul informațional „victima”, împrumutat nemijlocit în SI Agresor, datele de identificare sunt preluate prin interoperabilitate din Sistemul informațional automatizat „Registrul de stat al populației”, alte sisteme cu care inter-operează SI Agresor, precum și datele din nomenclatorul intern al SI Agresor.

4) date despre Ordinele de restricție de urgență:

4.1. datele cuprinse în Chestionarul de constatare și evaluare a riscurilor:

a) numărul de identificare a cazului – înregistrarea în Registrul nr. 1 sau 2 și se păstrează numărul de identificare din Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”.

b) data evaluării;

c) numele prenumele victimei;

d) data, luna, anul nașterii a victimei;

e) domiciliul victimei, date de contact;

f) locul de muncă al victimei;

g) numele, prenumele agresorului;

h) data, luna, anul nașterii agresorului;

i) domiciliul, date de contact;

j) locul de muncă al agresorului

k) natura relației dintre subiecți: *conlocuire, locuire separată, căsătoriți, divorțați, concubini, foști concubini, persoanele sub tutelă și/sau curatelă, afinii lor, copiii adoptivi, persoanele aflate în relații asemănătoare celora dintre părinți și copii, alte relații*;

l) descrierea primelor observații de la fața locului: *proprietate/bunuri distruse, pete de culoarea brună asemănătoare cu sânge, haine rupte etc.*;

m) numele prenumele altor victime prezente la cazul de violență: *copii, vârstnici, persoane cu dezabilități*;

n) numele prenumele altor victime prezente la cazul de violență care necesită asistență medicală primară/sau de urgență;

o) informații privind asistența medicală acordată: *nu necesită, va solicita asistență medicală individual, a refuzat de ajutorul medical, a fost acordat primul ajutor medical*;

p) locul, instituția medicală și medicul care a acordat primul ajutor medical;

q) descrierea periodicității actelor de violență în familie, în trecut: *este prima dată, zilnic, la 2-3 zile, săptămânal, lunar, la câteva luni, de 2 ori pe an, o dată pe an, o dată la câțiva ani, s-a mai întâmplat foarte mult timp în urmă (10-15 ani)*;

r) descrierea indicatorilor comportamentali/emoționali ai victimei: *furie, se scuză (exagerat), plânge, speriată, stare de isterie, irațională, nervoasă, stare de ebrietate (miros de alcool)*;

s) descrierea posibilelor leziuni invizibile, acuzare de dureri;

t) descrierea leziunilor vizibile: *răni, vânătăi, zgârieturi*;

u) descrierea indicatorilor comportamentali ai agresorului: *furios, se scuză (exagerat), plânge, speriat, stare de isterie, calm, irațional, nervos, amenință, stare de ebrietate (miros de alcool), altele*;

v) date despre posesia armei de foc: *agresorul este posesor de armă da/nu, dacă da, arma este deținută legal/ilegal, a folosit agresorul arme de foc, cuțite sau ale obiecte pentru a răni sau a amenințat verbal cu folosirea lor da/nu*;

w) detalierea actelor de violență fizică: *da/nu, dacă da, agresiunile fizice se manifestă prin: îmbrâncire/izbire, lovește peste diferite părți ale corpului, mușcă, aruncă cu diferite obiecte, înăbușă, trage de păr, alegare, lăsarea într-un loc periculos, alte acțiuni ce provoacă durere fizică*;

x) detalierea actelor de violență sexuală: *da/nu, dacă da, violența sexuală se manifestă prin: violul conjugal, acțiuni violente cu caracter sexual; interzicerea folosirii metodelor de contracepție, orice conduită sexuală nedorită, impusă; obligarea practicării prostituției; orice comportament sexual ilegal în raport cu un membru de familie minor, inclusiv prin: mângâieri, sărutări, pozare a copilului; prin atingeri nedorite cu tentă sexual, alte acțiuni cu efect similar*;

y) detalierea actelor de violență psihologică: *da/nu, dacă da, violența psihologică se manifestă prin: impunere a voinței sau a controlului personal, provocare a stărilor de tensiune și de suferință psihică prin: ofense, luare în derâdere, înjurare, insultare, poreclire, șantajare, distrugere demonstrativă a obiectelor, amenințări verbale, afișare ostentativă a armelor sau prin lovire a animalelor domestice, acte de gelozie obsesivă sau paranoidele, impunere a izolării prin detenție, inclusiv în locuința familiei lă: izolare de familie, de comunitate, de prieteni, interzicerea realizării profesionale, interzicerea frecventării instituției de învățământ, deposedare de acte de identitate, alte acțiuni cu efect similar*;

z) detalierea actelor de violență economică: *da/nu, dacă da, violența economică se manifestă prin: refuzul agresorului de a susține familia financiar, impunere la munci grele și nocive în detrimentul sănătății (a unui membru de familie minor), control din partea agresorului prin: lipsire de obiecte de primă necesitate (hrană, medicamente, mijloace economice), abuz de variate situații de superioritate pentru a sustrage bunurile persoanei; privarea dreptului la posesie, folosirea de bunurile comune, control inechitabil asupra bunurilor și resurselor comune, existența dependenței financiare față de agresor, alte acțiuni cu efect similar*;

aa) prezența indicatorilor semnificativi ai riscului: *da/nu, dacă da, există indicatori ai riscului de violență în familie: fizică, sexuală, psihologică, economică*;

bb) descrierea probabilității de abuz asupra copilului; *da/nu, dacă da, riscul este: scăzut, moderat, ridicat*;

cc) dacă victime ale violenței în familie sunt copii, cazul a foste referit: *da/nu, dacă da, data referirii Consiliului pentru Protecția Drepturilor Copilului, Direcției asistență socială și protecție a copilului, organizației neguvernamentală*;

dd) descrierea nivelului de risc stabilit în urma evaluării: *Scăzut, Moderat, Ridicat*;

ff) numele, prenumele, funcția evaluatorului.

Pentru datele cuprinse în Chestionarul de constatare și evaluare a riscurilor, informațiile specificate la lit. c) – k), în Sistem se păstrează datele de identificare din obiectul informațional „persoana fizică”.

4.2. datele cuprinse în Chestionarul de evaluare a riscurilor de letalitate a violenței în familie:

a) răspuns la întrebarea dacă victima crede că agresorul o va răni grav sau o va ucide pe ea, pe copiii ei sau pe cineva apropiat victimei: *da/nu*;

b) răspuns la întrebarea dacă victima este agresată sau abuzată fizic de agresor sistematic sau de mai multe ori pe parcursul săptămânii: *da/nu*;

c) răspuns la întrebarea dacă victima este controlată de agresor cu cine ea comunică, unde merge, ce haine poartă sau ce face, sau dacă agresorul vine neinvitat acasă sau la locul ei de muncă ori inițiază contacte nedorite în persoană, la telefon, prin mesaje text sau altă modalitate de comunicare electronică: *da/nu*;

d) răspuns la întrebarea dacă victima este intimidată sau amenințată de agresor, în cazul în care ea a încercat să întrerupă relația, să plece, să ceară ajutor sau să vorbească cu cineva apropriat despre abuzul trăit: *da/nu*;

e) răspuns la întrebarea dacă victima a fost sugrumată sau strangulată vreodată către agresor, ori dacă agresorul a folosit vreodată forța fizică astfel încât ea nu a mai putut să respire sau a leșinat: *da/nu*;

f) răspuns la întrebarea dacă victima a fost supusă violenței sau abuzului fizic în timpul sarcinii: *da/nu*;

g) răspuns la întrebarea dacă victima a fost vreodată amenințată sau împiedicată de agresor să solicite ajutor, în special din partea Poliției, a instanțelor de judecată sau a unui avocat: *da/nu*;

h) răspuns la întrebarea dacă recent, actele de violență din partea agresorului au devenit din ce în ce mai grave: *da/nu*;

i) răspuns la întrebarea dacă agresorul vreodată a forțat victima la acte cu caracter sexual nedorite: *da/nu*;

j) răspuns la întrebarea dacă agresorul a amenințat sau încercat vreodată să se sinucidă: *da/nu*.

4.3. datele cuprinse în Ordinul de restricție de urgență:

a) organului teritorial din subordinea Ministerului Afacerilor Interne care a emis ordinul de restricție de urgență;

b) numărul de înregistrare (în Sistem se păstrează numărul de identificare aferent identificatorului obiectului informațional „Ordine de restricție de urgență”;

c) data eliberării;

d) ora eliberării;

e) localitatea în care a fost dispusă eliberarea ordinului de restricție de urgență (corespunde cu locul unde a fost cercetat cazul);

f) funcția, numele și prenumele angajatului organului de constatare sau organului de urmărire penală care eliberează ordinul de restricție de urgență;

g) temeiul eliberării ordinului de restricție de urgență (persoana de la care a parvenit sesizarea cu privire la comiterea actelor de violență în familie);

h) numărul de înregistrare a cazului (în Sistem se păstrează numărul de identificare din Sistemul informațional automatizat „Registrul informației criminalistice și criminologice” (Registrul nr. 1. 2);

i) descrierea faptelor constatate, circumstanțele cazului;

j) rezultatele evaluării riscurilor;

k) secțiunea care citează temeiul legal și instrumentele juridice care au stat la baza eliberării ordinului de restricție de urgență;

l) partea dispozitivă în care se indică: *obligarea agresorului de a părăsi temporar locuința comună (se indică adresa) fără a decide asupra modului de proprietate asupra bunurilor*;

m) datele de identitate și de domiciliere a agresorului (în Sistem se păstrează datele de identificare din obiectul informațional „persoana fizică”);

n) restricțiile aplicate în privința agresorului *(interzicerea contactului vizual sau orice alt contact, inclusiv telefonic, prin corespondență sau în orice alt mijloc cu victima și cu copiii ei; interzicerea de a se apropia de anumite locuri, locul de muncă, de studii, alte locuri determinate pe care victima/victimele le frecventează; interzicerea de a purta sau păstra armă)*;

o) termenul de acțiune a ordinului de restricție de urgență (momentul din care începe decurgerea acțiunea și perioada de acțiune, dar nu poate depăși termenul de 10 zile);

p) mențiuni cu privire la: înmânarea unui exemplar agresorului, aducerea la cunoștință despre eliberarea ordinului de restricție de urgență, drepturile și obligațiile ce rezultă din acesta, informarea despre dreptul de contestare.

q) mențiuni cu privire la alte modalități de informare despre faptul emiterii ordinului de restricție de urgență, în cazurile când una din părți nu este la fața locului, fie a fost informat: verbal prin poștă, telefon, fax, poștă electronică, rețele de socializare, platforme de comunicare/mesagerie, etc.).

51. În scopul asigurării autenticității și reducerii volumului informației stocate în SI Agresor, precum și în vederea asigurării clasificării corecte a obiectelor în acesta, se utilizează sistemul de clasificatoare elaborate în baza clasificatoarelor naționale:

1) clasificatoarele internaționale;

2) clasificatoarele naționale;

3) clasificatoarele departamentale.

Clasificatoarele departamentale se elaborează și se utilizează în cadrul sistemului numai în cazurile lipsei clasificatoarelor internaționale și naționale aprobate.

52. Pentru asigurarea formării corecte a resurselor informaționale ale SI Agresor, a calității și actualității datelor, sistemul va interacționa, prin intermediul platformei de interoperabilitate (MConnect), cu următoarele resurse informaționale:

a) SIA „Registrul de stat al populației” – oferă accesul la datele despre agresorul familial și victima violenței în familie, precum și documentele care le-au fost eliberate;

b) SIA „Registrul informației criminalistice și criminologice” – oferă accesul la informațiile sistematizate de evidență a infracțiunilor, a cauzelor penale şi a persoanelor care au săvârșit infracțiuni;

c) SIA „Registrul de stat al contravențiilor” – oferă accesul la datele și informațiile de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții;

d) Sistemul informațional judiciar, prin componenta sa – Programul Integrat de Gestionare a Dosarelor (PIGD) – oferă accesul automatizat la datele despre dosarele judecătorești, materiale procesuale emise de instanțele de judecată și hotărârile adoptate;

e) SIA „Registrul procedurilor de executare” – oferă accesul la datele despre toate acțiunile întreprinse de executorii judecătorești pentru îndeplinirea integrală a documentelor executorii;

f) SIA „Registrul persoanelor reținute, arestate și condamnate” – oferă accesul la datele despre persoanele aflate în custodia statului pază (reținute, arestate și condamnate);

g) SIA „Registrul de stat al armelor” – oferă accesul la datele despre circulația armelor individuale (cu excepția celor militare) pe teritoriul țării, despre titularii lor de drepturi, precum și la datele ce țin de organizarea controlului circulației armelor;

h) SIA „Registrul dactiloscopic” – oferă accesul la datele despre particularitățile structurii desenelor papilare ale degetelor omului și despre identitatea lui;

i) Sistemul informațional integrat al Poliției de Frontieră – oferă accesul la datele despre traversarea frontierei de stat de către persoanele fizice și unitățile de transport;

j) Sistemul informațional geografic național – este destinat pentru stabilirea spațială a datelor despre locurile comiterii infracțiunilor și obiectele infrastructurii, oferă, de asemenea, posibilitatea de aplicare a metodelor de analiză spațială a evenimentelor și fenomenelor care au loc în sfera criminală;

k) Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență – care oferă accesul la datele despre toate apelurile și înștiințările de urgență, localizarea geografică a apelanților, transmiterea solicitărilor de intervenție către serviciile specializate de urgență, precum și rezultatele reacționării și intervenției acestora la fiecare apel de urgență;

l) Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică” – oferă accesul la informațiile cu privire la semnalări urgente și nonurgente parvenite/raportate prin mai multe canale;

m) Sistemul informațional automatizat „Registrul de stat al unităților administrativ-teritoriale și al adreselor” – oferă accesul la nomenclatorul unităților administrativ-teritoriale (raioane, orașe (municipii), sate (comune), localități, inclusiv cele desființate) și la elementele de bază ale infrastructurii urbane (artere de circulație, clădiri) calificate ca adrese ale obiectelor fizice din localitățile de pe teritoriul Republicii Moldova;

n) Sistemul informațional automatizat „Registrul de stat al unităților de drept” – acordă acces la datele despre toate categoriile de unități de drept, constituite în bază legală. Interacțiunea are loc în scopul preluării și validării datelor despre persoane juridice privind corectitudinea combinațiilor de IDNO, denumire, cod.

Registrul va fi interconectabil și integrat cu platforma de interoperabilitate (MConnect), prin intermediul căreia se va asigura schimbul de date între acesta și alte sisteme și resurse informaționale de stat, în conformitate cu cadrul normativ în domeniul schimbului de date și interoperabilității.

53. SI Agresor interacționează cu următoarele sisteme informaționale partajate:

1) platforma de interoperabilitate (MConnect) – pentru schimbul de date cu alte sisteme informaționale și registre de stat;

2) serviciul electronic guvernamental integrat de semnătură electronică (MSign) – pentru semnarea documentelor electronice;

3) serviciul electronic guvernamental de autentificare şi control al accesului (MPass) – pentru autentificarea şi controlul accesului în cadrul sistemului;

4) serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiunilor (evenimentelor) produse în cadrul sistemului;

5) serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea registratorilor;

6) serviciul guvernamental de plăți electronice (MPay) – destinat pentru a oferi persoanelor fizice și persoanelor juridice de drept public și de drept privat un mecanism de efectuare a plăților în contul unic trezorerial al Ministerului Finanțelor, precum și de distribuire a plăților de la bugetele componente ale bugetului public național și de restituire a plăților din acesta și din conturile instituțiilor publice la autogestiune către persoanele fizice;

7) Sistemul informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower) – sistem informațional constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune, destinate consemnării împuternicirilor de reprezentare în baza semnăturii electronice, acordate de către persoane fizice sau juridice altor persoane fizice sau juridice.

54. Datele recepționate din celelalte registre sunt utilizate în scopul documentării corecte și exhaustive a cazurilor de violență în familie, contravențiilor de violență în familie, a infracțiunilor de violență în familie, a cauzelor penale și a persoanelor care au săvârșit infracțiuni sau contravenții de violență în familie, a încălcării măsurilor de protecție aplicate, al acordării asistenței informaționale organelor de urmărire penală și agenților constatatori în soluționarea cazurilor de violență în familie, al colectării centralizate a datelor aferente cazurilor de violență în familie și deciziilor judecătorești.

55. Serviciile electronice guvernamentale sunt utilizate în baza acordurilor semnate cu deținătorul acestora.

Capitolul VII
INFRASTRUCTURA INFORMAȚIONALĂ DE COMUNICAȚII ELECTRONICE

56. SI Agresor va fi găzduit pe platforma tehnologică comună (MCloud).

57. Lista produselor software utilizate la crearea infrastructurii informaționale și de comunicații electronice a SI Agresor este determinată de către Serviciul Tehnologii Informaționale din subordinea Ministerului Afacerilor Interne.

Capitolul VIII

SPAŢIUL TEHNOLOGIC AL SISTEMULUI

58. Complexul informațional de program asigură funcționarea spațiului informațional unic și este compus din:

1) ***banca de date a Sistemului*** – asigură colectarea, acumularea, prelucrarea, păstrarea, actualizarea, securitatea și integritatea informației stocate, prezentate de către participanții la sistem, generează informație statistică și analitică organelor de drept - participanți la sistem, în limita competențelor sale, asigură apărarea, securitatea și integritatea informației care se păstrează în bancă, precum și interzice accesul neautorizat la această informație. Fiecare participant la sistem asigură introducerea informației în banca centrală de date, potrivit formatelor aprobate și în termenele stabilite.

2) ***depozitul de date*** – este destinat pentru păstrarea, organizarea și gestionarea datelor obiectelor informaționale, inclusiv a datelor privind documentele utilizate pentru actualizarea informațiilor și etapele procesării acestora. Acesta înregistrează toate modificările și actualizările aduse informațiilor, asigurând o trasabilitate completă a modificărilor. Depozitul de date include măsuri de securitate avansate, cum ar fi criptarea datelor și autentificarea utilizatorilor, și implementa proceduri de backup regulat și planuri de recuperare în caz de dezastru. Mecanismele eficiente de management și indexare permit căutarea rapidă și precisă a datelor. Sistemele de monitorizare și audit sunt integrate pentru a urmări accesul și utilizarea informațiilor, prevenind accesul neautorizat. Depozitul de date este conceput pentru a fi interoperabil cu alte componente ale sistemului și respectă legislația în vigoare și reglementările privind protecția datelor personale și confidențialitatea;

3) ***baza de formate*** – este destinată pentru asigurarea securității în procesul de lucru cu utilizatorii de la distanță și pentru gestionarea clasificatoarelor și formatării datelor într-un mod standardizat. Aceasta garantează prezentarea informațiilor într-un format uniform, facilitând interoperabilitatea și accesibilitatea. Baza de formate include clasificatoare care stabilesc ierarhia și categoriile de informații, precum și drepturile de acces ale fiecărui utilizator, protejând astfel confidențialitatea și integritatea datelor. Măsurile de securitate implementate, cum ar fi criptarea datelor și controlul accesului bazat pe roluri, asigură că informațiile sunt disponibile doar pentru utilizatorii autorizați. Baza de formate este integrată cu alte componente ale sistemului, asigurând compatibilitatea formatelor și clasificatoarelor. Procedurile de actualizare sunt reglementate pentru a reflecta modificările în politicile de securitate și cerințele legale. Baza de formate include formate standardizate pentru informații comune, dar permite și personalizarea acestora în funcție de necesitățile specifice. Este proiectată pentru a fi accesibilă și ușor de utilizat, facilitând interacțiunea eficientă a utilizatorilor cu informațiile;

4) ***bazele tehnologice de date*** – destinate pentru păstrarea provizorie a informațiilor parvenite de la nivele inferioare, care implică adoptarea unor decizii de către colaboratorii împuterniciți, precum și pentru realizarea tuturor verificărilor necesare la luarea deciziilor;

5) ***vitrina de date*** – reprezintă baze de date secționate din depozitul central și asigură utilizatorilor accesul rapid și oportun la informația necesară, fără a li se acorda acces la depozitul de date. Vitrinele de date pot furniza anumitor categorii de utilizatori informație în forma cea mai convenabilă pentru utilizare. Concomitent, acestea constituie unul dintre elementele de protecție a informațiilor de accesul neautorizat, deoarece conțin numai volumul de date accesibile utilizatorului. Actualizarea vitrinelor de date se efectuează automat, concomitent cu modificarea informațiilor din depozitul de date.

Schimbul de informații dintre componentele băncii centrale de date se efectuează prin anumite proceduri de securitate inaccesibile utilizatorilor externi, care este parte componentă a sistemului de protecție a băncii centrale de date.

Accesul la informația din banca centrală de date a sistemului îl au organele de urmărire penală sau alți furnizori de informație, în conformitate cu legislația în vigoare sau în baza unor acorduri separate.

59. SI Agresor utilizează standarde deschise și este compatibil cu tehnologii de „cloud computing" (nor informațional), care, la fel, utilizează standarde non proprietare, cât și cu standardele deja existente și asigură posibilitatea dezvoltării sale fără perturbarea continuității funcționării.

60. Arhitectura Sistemului este concepută după schema-tip a infrastructurii informaționale a sistemului informațional automatizat.

61. Sistemul utilizează sistemele informaționale partajate MPass, MLog, MNotify, MSign, MPower, MPay și este găzduit pe platforma tehnologică guvernamentală comună (MCloud).

62. În scopul asigurării interoperabilității și a schimbului de date a SI Agresor cu alte sisteme și resurse informaționale de stat, Ministerul Afacerilor Interne înregistrează activele semantice utilizate în Sistemul informațional „Catalogul semantic".

63. Arhitectura complexului software, lista produselor software și a mijloacelor tehnice utilizate la crearea infrastructurii informaționale se determină de posesor în etapele ulterioare de dezvoltare a sistemului, ținând cont de:

1) implementarea unei soluții bazate pe SOA (Service Oriented Arhitecture – *Arhitectură software bazată pe servicii*), care oferă posibilitatea reutilizării unor funcții ale sistemului cu noi funcționalități, fără a afecta funcționarea sistemului;

2) implementarea funcționalităților de arhivare (backup) și restabilirea datelor în caz de incidente.

64. SI Agresor poate fi extins pe verticală, prin extinderea resurselor utilizate, pentru a acomoda numărul necesar de utilizatori, atât în regim normal de lucru, cât și în perioadele de vârf.

65. Sistemul de comunicații se bazează pe infrastructura și echipamentul rețelelor guvernamentale care includ posibilitatea conectării la internet. Infrastructura existentă este planificată în mod corespunzător, pentru a oferi nivelele adecvate de performanță și capacitate.

66. Interfața de utilizare a sistemului se adaptează automat la diverse rezoluții de afișare și este disponibilă cel puțin în limba română și este implementată folosind tehnologii care asigură funcționarea serviciului pe dispozitivele mobile.

67. Având în vedere locul SI Agresor în cadrul resurselor informaționale departamentale ale Ministerului Afacerilor Interne, sunt necesare o disponibilitate înaltă și accesul neîntrerupt la sistem. Din acest motiv, întreaga soluție este construită în regim de înaltă disponibilitate (24 de ore pe zi, 7 zile pe săptămână).

Capitolul IX
ASIGURAREA SECURITĂȚII INFORMAȚIONALE A SISTEMULUI

68. Securitatea SI Agresor presupune protecția de către deținător a Sistemului, resurselor și infrastructurii informaționale la toate etapele proceselor de creare, procesare, stocare și transmitere a datelor, de acțiuni accidentale sau intenționate cu caracter artificial

sau natural, care au ca rezultat cauzarea prejudiciului posesorului și utilizatorilor resurselor informaționale și infrastructurii informaționale, prin care se asigură veridicitatea, integritatea, confidențialitatea, disponibilitatea și autenticitatea resurselor informaționale. Sistemul securității informaționale reprezintă o totalitate a acțiunilor juridice, organizatorice, economice și tehnologice orientate spre prevenirea pericolelor asociate resurselor și infrastructurii informaționale.

69. Asigurarea securității informației va fi realizată în conformitate cu Cerințele minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr. 201/2017, precum și cu bunele practici în domeniul securității. Pentru gestiunea riscurilor de securitate va fi implementată o politică generală de securitate. Personalul implicat în utilizarea și administrarea Sistemului va fi instruit în ceea ce privește riscurile de securitate la care poate fi expus. Politica de securitate va include prevederi referitoare la organizarea auditurilor periodice de securitate pentru a verifica politica și conformitatea cu regulile de securitate, precum și pentru a stabili domeniile care necesită a fi îmbunătățite.

70. Prin pericol pentru securitatea informațională se înțelege un eveniment sau o acțiune potențial posibilă, orientată spre cauzarea unui prejudiciu resurselor sau infrastructurii informaționale.

Principalele pericole pentru securitatea informațională a SI Agresor sunt:

1) colectarea și/sau utilizarea ilegală a informației;

2) încălcarea tehnologiei de prelucrare a informației;

3) încălcarea confidențialității informației;

4) încălcarea integrității logice și a integrității fizice a informației;

5) încălcarea funcționării infrastructurii informaționale;

6) acțiunea fizică asupra componentelor infrastructurii informaționale;

7) inserarea în produsele software a componentelor care realizează funcții neprevăzute în documentația cu privire la aceste produse;

8) elaborarea și răspândirea programelor care afectează funcționarea normală a sistemelor informaționale și de telecomunicații, precum și a sistemelor securității informaționale;

9) nimicirea, deteriorarea și suprimarea radioelectronică sau distrugerea mijloacelor și a sistemelor de prelucrare a informației, de telecomunicații și comunicații;

10) influența asupra sistemelor cu parolă-cheie de protecție a sistemelor automatizate de prelucrare și transmitere a informației;

11) compromiterea cheilor și mijloacelor de protecție criptografică a informației;

12) scurgerea informației prin canale tehnice;

13) implementarea dispozitivelor electronice pentru interceptarea informației în mijloacele tehnice de prelucrare, păstrare și transmitere a informației prin canalele de comunicații, precum și în încăperile de serviciu ale autorităților;

14) nimicirea, deteriorarea, distrugerea sau sustragerea suporturilor de informație mecanice sau a altor suporturi;

15) interceptarea informației în rețelele de transmitere a datelor și în liniile de comunicații, decodificarea acestei informații și/sau răspândirea informației false;

16) utilizarea tehnologiilor informaționale necertificate, a mijloacelor de protecție a informației, a mijloacelor de informatizare, de telecomunicații și comunicații necertificate în procesul creării și dezvoltării infrastructurii informaționale;

17) accesul neautorizat la resursele informaționale;

18) încălcarea restricțiilor legale privind accesul și divulgarea informației;

19) încălcarea prevederilor Legii nr. 133/2011 privind protecția datelor cu caracter personal.

71. Pericolul și vulnerabilitățile SI Agresor pot fi accesările ilegale de către infractori, accesările neautorizate, prestarea serviciilor neautorizate de către angajații instituțiilor și accesările nestandardizate ale utilizatorilor, care pot duce la pierderi informatizate.

72. Sistemul de securitate a infrastructurii este un serviciu ce asigură integritatea și disponibilitatea sistemelor hardware și software, protecția fluxurilor de date. Aceste servicii sunt desemnate pentru a corecta erorile din componentele hardware și software și includ soluții antivirus, anti-malware, de actualizare a produselor software, de conformare la politicile de licențiere, protocolare și audit.

73. Pentru asigurarea edificării sistemului eficient de asigurare a securității informaționale ale obiectelor sistemului sunt necesare:

1) identificarea cerințelor securității informației specifice pentru fiecare obiect al protecției în cauză;

2) respectarea cerințelor actelor normative;

3) utilizarea celor mai bune practici (standarde, metodologii) pentru asigurarea securității informaționale;

4) determinarea subdiviziunilor responsabile pentru asigurarea securității informaționale;

5) distribuirea între subdiviziuni a sferelor de responsabilitate în asigurarea securității informaționale;

6) determinarea cerințelor tehnice și organizatorice în baza gestionării riscurilor de securitate a informației, care constituie politica de securitate informațională a obiectului protecției;

7) realizarea cerințelor politicii de securitate informațională, prin implementarea metodelor software și a mijloacelor de protecție a informației corespunzătoare;

8) realizarea sistemului de management al securității informaționale.

74. Obiectivele de bază ale asigurării securității informaționale sunt:

1) asigurarea confidențialității informației, prevenirea accesului la informație fără drepturi și împuterniciri corespunzătoare – garantează că datele înregistrate în Sistem nu pot fi accesate de o parte terță neautorizată;

2) asigurarea integrității logice a informației, prevenirea introducerii, actualizării și nimicirii neautorizate a informației – garantează că utilizatorii autentificați pot accesa serviciile și datele care corespund drepturilor lor de acces;

3) asigurarea integrității fizice a informației - garantează că datele înregistrate în Sistem nu au fost modificate sau alterate de o parte terță neautorizată.;

4) asigurarea protecției infrastructurii informaționale – garantează protecția sistemului împotriva deteriorării și tentativelor de modificare a funcționării;

5) asigurarea autentificării – garantează că Sistemul va fi accesibil doar utilizatorilor autentificați și creați de către deținătorul Sistemului.

75. Pentru atingerea obiectivelor menționate, Sistemul dispune de mai multe mecanisme de securitate:

1) firewall – filtrul firewall face parte din arhitectura tehnică a platformei tehnologice (MCloud), pentru a asigura un mecanism de apărare împotriva utilizatorilor externi;

2) antivirus/antispam – soluțiile hardware și/sau software asigură protecția antivirus și antispam pentru toate serverele. Fișierele se scanează la încărcare în Sistem. În cazul detectării unui fișier infectat, procedura de încărcare este oprită și fișierul – respins;

3) sistem de detectare a intruziunilor – sistem de detectare a intruziunilor care include toți utilizatorii de pe toate serverele;

4) comunicare sigură (transferuri de date) dintre serverele web și utilizatori – schimbul de informații confidențiale este securizat;

5) backup sistematic al datelor păstrate – permite recuperarea rapidă și fiabilă a datelor în caz de incident care a dus la pierderea sau deteriorarea datelor;

6) instrument de înregistrare a evenimentelor de audit – toate activitățile desfășurate de către utilizatori, indiferent dacă au succes sau nu (cum ar fi conectările încercate, dar nereușite), sunt monitorizate și înregistrate în jurnalele Sistemului, cu acces limitat pentru utilizatorii neautorizați.

76. Mecanismele de bază ale asigurării securității informaționale sunt:

1) autentificarea și autorizarea;

2) controlul accesului;

3) înregistrarea acțiunilor și auditul;

4) criptarea informației;

5) analizarea și modelarea fluxurilor informaționale;

6) monitorizarea rețelelor;

7) detectarea și prevenirea intruziunilor;

8) prevenirea scurgerii informației confidențiale;

9) analizatorii de protocoale;

10) mijloacele de programare antivirus;

11) ecranele între rețele (firewall);

12) sistemele copierii de rezervă;

13) sistemele de alimentare fără întrerupere cu energie electrică;

14) organizarea pazei și securității;

15) mijloacele de prevenire a accesului neautorizat în clădiri și încăperi;

16) mijloacele de analiză a sistemelor de protecție;

17) alte mecanisme.

77. Organizarea sistemului de protecție a datelor cu caracter personal constituie o parte componentă a mecanismului de asigurare a securității informaționale a sistemului. Sistemul de protecție a datelor cu caracter personal se constituie în baza:

1) raportului privind rezultatele efectuării auditului intern;

2) datelor cu caracter personal prelucrate în cadrul acestui sistem informațional;

3) actului de clasificare a sistemului informațional care prelucrează date cu caracter personal;

4) modelelor de pericole pentru securitatea datelor cu caracter personal;

5) prevederilor privind delimitarea drepturilor de acces la datele cu caracter personal prelucrate;

6) documentelor de reglementare și politicilor de securitate elaborate.

78. Accesarea datelor cu caracter personal ale persoanei fizice din resursele și sistemele informaționale de stat, precum și păstrarea și actualizarea acestora în baza de date a sistemului este posibilă doar în cazurile stabilite de legislația națională în domeniul de competență al Ministerului Afacerilor Interne, autorităților administrative și instituțiilor din subordinea acestuia.

79. În cadrul operațiunilor de prelucrare a datelor, inclusiv a celor cu caracter personal, se asigură posibilitatea identificării și autentificării echipamentului folosit (prin

adresa unică IP – Internet Protocol), cu păstrarea acestor informații pentru o anumită perioadă.

80. Toți utilizatorii sistemului, precum și personalul care asigură mentenanța tehnică, administratorii de rețea, programatorii și administratorii bazelor de date vor avea un ID (Identity Document) al utilizatorului unic, care nu trebuie să conțină semnalmentele nivelului de accesibilitate ale utilizatorului sistemului. Administrarea ID-urilor utilizatorilor sistemului include identificarea univocă și verificarea autenticității fiecărui utilizator.

81. Stabilirea limitelor în privința drepturilor de acces persoanelor care au dreptul să vizualizeze informațiile stocate în sistem, să copieze, să descarce, să șteargă sau să modifice orice informație stocată se realizează conform prevederilor legislației naționale în domeniu.

82. Finalizarea sesiunii de lucru în Sistem se realizează la solicitarea utilizatorului sau automat, la expirarea timpului prestabilit pentru perioada inactivă, astfel că pentru a continua activitatea, utilizatorului i se va cere să treacă repetat procedurile de identificare și autentificare.

83. În cadrul Sistemului se asigură generarea și păstrarea înregistrărilor de audit ale securității pentru operațiile de prelucrare a datelor cu caracter personal, în condițiile cadrului normativ în materie de protecție a datelor cu caracter personal. Înregistrările de audit ale operațiilor și rezultatele acestora pot fi accesate în conformitate cu prevederile cadrului normativ aferent.

84. SI Agresor va utiliza funcționalitatea de autentificare doar prin intermediul serviciului electronic guvernamental de autentificare și control al accesului (MPass).

85. Utilizatorii SI Agresor vor fi autorizați să acceseze doar blocurile funcționale și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia. Utilizatorii și rolurile acestora vor fi gestionate prin intermediul serviciului MPass. SI Agresor va prelua rolurile utilizatorilor din serviciul electronic guvernamental de autentificare și control al accesului (MPass).

86. O necesitate importantă legată de securitate este necesitatea păstrării înregistrărilor de audit pentru analiza integrității SI Agresor și pentru monitorizarea activității utilizatorilor. SI Agresor se va baza pe un mecanism de înregistrări de audit dublu (intern și cu utilizarea serviciului electronic guvernamental de jurnalizare (MLog), ce urmează practicile internaționale.

Anexa nr. 2 la Hotărârea
Guvernului nr._____/2024

REGULAMENTUL
resursei informaționale formate de Sistemul informațional de evidență a agresorilor în cazurile de violență în familie

I. DISPOZIȚII GENERALE

1. Regulamentul resursei informaționale formate de Sistemul informațional de evidență a agresorilor în cazurile de violență în familie (în continuare – *Regulament*) stabilește modul de organizare și funcționare a resursei informaționale a Ministerului Afacerilor Interne, modul de asigurare informațională a activității subdiviziunilor Ministerului Afacerilor Interne, care au drept scop apărarea drepturilor și a libertăților fundamentale ale persoanei prin activități de prevenire și combatere a violenței împotriva femeilor și violenței în familie, precum și reglementarea cerințelor față de protecția datelor la colectarea, acumularea, actualizarea, păstrarea, prelucrarea și transmiterea informațiilor privind agresorii familiali în cazurile de violență în familie.

2. Noțiunile utilizate în prezentul Regulament au semnificația prevăzută în art. 2 din Legea nr. 45/2007 cu privire la prevenirea și combaterea violenței împotriva femeilor și a violenței în familie.

În sensul prezentului Regulament se definesc următoarele noțiuni:

administrator al resursei informaționale – subdiviziune din cadrul Serviciului Tehnologii Informaționale din subordinea Ministerului Afacerilor Interne care realizează nemijlocit atribuțiile aferente deținătorului al Sistemului informațional de evidență a agresorilor în cazurile de violență în familie;

autentificare – verificarea identificatorului atribuit subiectului de acces, confirmarea autenticității;

complex de mijloace software și hardware – totalitatea programelor și a mijloacelor tehnice care asigură realizarea proceselor informaționale;

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

integritatea informației – certitudinea, necontradictorialitatea și actualitatea informației, protecția ei împotriva distrugerii și modificării neautorizate;

participanți la resursa informațional – subdiviziunile teritoriale, specializate și administrative din subordinea Ministerului Afacerilor Interne, organele de urmărire penală, de conducere și de exercitare a urmăririi penale, organele de asistență socială, organele din domeniul ocrotirii sănătății, entitățile din domeniul educației, instanțele judecătorești, organele de probațiune și organele de executare a pedepsei penale;

stocarea datelor – păstrarea pe orice fel de suport a datelor cu caracter criminal;

suporturi materiale – suporturi magnetice, optice, laser sau alte suporturi ale informației electronice, pe care se creează, se fixează, se transmite, se recepționează, se păstrează sau se utilizează în alt mod informația electronică cu caracter criminal și care permit reproducerea și folosirea ulterioară a acesteia;

ținerea resursei informaționale – totalitatea măsurilor cu caracter tehnic îndreptate spre asigurarea funcționării complexului tehnic de program și administrarea resursei informaționale a sistemului informațional;

utilizator – persoana fizică sau juridică ale cărei atribuții de serviciu presupun acțiuni de prezentare, de primire, de păstrare, precum și de utilizare a informației din resursa informațională.

3. Resursa informațională ținută în cadrul Sistemului informațional de evidență a agresorilor în cazurile de violență în familie (în continuare – *SI Agresor)*, ca resursă informațională specializată, este destinată să asigure suportul informațional al activității organelor de drept din subordinea Ministerului Afacerilor Interne, în procesul de colectare și înregistrare a informațiilor despre persoanele care au săvârșit infracțiuni și contravenții de violență în familie, care creează sistematic situații de conflict în familie, aplică violență (fizică, psihologică, sexuală, economică) sau manifestă comportament violent (care nu se încadrează în limitele infracțiunii sau contravenției de violență în familie) față de membrii de familie, amenință membrii familiei cu moartea sau cu cauzarea vătămărilor corporale, persoanele liberate condiționat de răspundere penală sau condamnate cu suspendarea condiționată a executării pedepsei, persoanele în privința cărora sunt aplicate măsuri de constrângere cu caracter medical, restricții aplicate prin ordinul de restricție de urgență sau ordonanță de protecție, agresorii familiali în privința cărora este aplicată monitorizarea electronică sau cei obligați să participe la programe speciale de tratament sau de consiliere în vederea reducerii comportamentului violent, precum și alte decizii judiciare relevante, etc.

4. SI Agresor creează un spațiu informațional unitar departamental ale cărui date se consideră corecte și veridice până la proba contrarie.

II. SCOPUL ȘI CATEGORIILE DE DATE PRELUCRATE

5. SI Agresor, fiind integrat cu alte sisteme informaționale, asigură un mediu informațional securizat, exhaustiv și transparent.

6. În SI Agresor datele cu caracter personal sunt utilizate doar în scopul în care este notificat fără a se urmări obținerea unor informații în interes personal.

7. SI Agresor se ține în limba română.

8. Evidența obiectelor informaționale se asigură conform prevederilor Conceptului Sistemului informațional de evidență a agresorilor în cazurile de violență în familie, instrucțiunilor elaborate de posesorul SI Agresor și aprobate în comun cu registratorii implicați. În cazul depistării unor erori sau inexactități în documentele sau datele primite, administratorul SI Agresor este obligat să informeze despre aceasta furnizorul datelor SI Agresor și destinatarii cărora le-au fost transmise date eronate.

9. Dacă furnizorul datelor SI Agresor se adresează cu un demers argumentat privind rectificarea datelor eronate sau inexacte, registratorul datelor din cadrul resursei informaționale respective, execută corectările necesare și informează despre aceasta furnizorul datelor care a înaintat demersul.

10. Datele se păstrează în SI Agresor în ordine cronologică, ceea ce asigură posibilitatea obținerii datelor pentru o etapă determinată de timp.

11. Înlăturarea din evidență a datelor incorecte și neveridice din SI Agresor se efectuează de către registratorul care gestionează datele respective în baza documentelor confirmative, cu respectarea strictă a cerințelor privind protecția datelor cu caracter personal. Radierea datelor se operează prin inserarea unei note speciale și nu reprezintă excluderea fizică a datelor din SI Agresor.

12. Păstrarea SI Agresor este asigurată de deținător până la adoptarea deciziei despre lichidarea acestuia. În cazul lichidării resursei informaționale respective, datele și documentele conținute în acesta se transmit în arhivă conform legislației.

13. Datele din SI Agresor sunt din categoria specială a datelor cu caracter personal. Asigurarea securității, confidențialității și integrității datelor prelucrate în cadrul resursei informaționale respective se efectuează cu respectarea strictă a cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale, aprobate prin hotărâre de Guvern.

14. De la data încetării utilizării datelor din SI Agresor până la atribuirea statutului de document de arhivă, acestea se păstrează pe o perioadă nu mai mare de 2 ani, în scopul apărării naționale, securității statului, menținerii ordinii publice, protecției drepturilor și a libertăților omului.

15. Pentru asigurarea funcționării eficiente și neîntrerupte a SI Agresor, schimbul informațional de date între participanții la resursa informațională enunțată este asigurat în regim nonstop.

16. Schimbul informațional în cadrul SI Agresor se efectuează doar cu utilizarea complexului de mijloace software și hardware specializat, prin intermediul Sistemului de telecomunicații al autorităților administrației publice.

III. SUBIECȚII RAPORTURILOR JURIDICE ÎN DOMENIUL CREĂRII, ADMINISTRĂRII, MENTENANȚEI, DEZVOLTĂRII ȘI UTILIZĂRII SI AGRESOR ȘI ATRIBUȚIILE ACESTORA

17. Subiecții raporturilor juridice din domeniul creării, administrării, mentenanței, dezvoltării și utilizării conținutului SI Agresor sunt:

1) proprietarul;
2) posesorul;
3) deținătorul
a) administratorul tehnic;
5) utilizatorii.

18. Proprietarul SI Agresor este statul.

19. Posesorul SI Agresor este Ministerul Afacerilor Interne care asigură condițiile juridice, financiare și organizatorice pentru crearea, administrarea, mentenanța și dezvoltarea resursei informaționale respective.

20. Deținătorul SI Agresor este Serviciul Tehnologii Informaționale din subordinea Ministerului Afacerilor Interne, care asigură crearea sistemului, dezvoltarea acestuia și implementarea cerințelor de securitate stabilite de actele normative în domeniu.

21. Administratorului tehnic al sistemului informațional este Instituția publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, care își exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică, menținere a sistemului informațional.

22. Utilizatorii SI Agresor sunt:

1) registratorul;
2) furnizorul;
3) destinatarul.

23. Registratorii SI Agresor pot fi:

1) angajatul desemnat în cadrul entității pentru înregistrare și evidență statistică, operatorii unităților operaționale de coordonare din cadrul autorităților administrative și instituțiilor din subordinea Ministerului Afacerilor Interne, care înregistrează apelurile telefonice primite, mesajele primite prin fax, SMS, MMS, mesajele de pe portalul web, adresările și petițiile cetățenilor și organizațiilor referitoare la cazurile de violență în familie, precum și informațiile cu privire la:

a) cauzele penale și contravenționale de violență în familie și persoanele care au săvârșit infracțiuni și contravenții de violență în familie;

b) persoanele care au fost denunțate că creează sistematic situații de conflict în familie, aplică violență (fizică, psihologică, sexuală, economică) sau manifestă comportament violent față de membrii de familie;

c) personale care au fost denunțate că amenință membrii familiei cu moartea sau cu cauzarea vătămărilor corporale și există riscul eminent de realizare a acestor amenințări;

d) persoanele liberate condiționat de răspundere penală pentru actele de violență în familie;

e) persoanele condamnate cu suspendarea condiționată a executării pedepsei, pentru acte de violență în familie;

f) persoanele reținute, arestate și condamnate pentru actele de violență în familie;

g) agresorii familiali în privința cărora sunt aplicate măsuri de constrângere cu caracter medical;

h) agresorii familiali în privința cărora au fost emise decizii privind obligarea de a participa la programe speciale de tratament sau de consiliere în vederea reducerii comportamentului violent;

i) persoanele în privința cărora au fost aplicate restricții prin ordinul de restricție de urgență;

j) persoanele în privința cărora au fost aplicate restricții prin ordonanță de protecție;

k) agresorii familiali în privința cărora este aplicată monitorizarea electronică;

l) agresorii familiali în privința cărora au fost emise alte decizii judiciare relevante.

2) utilizatorii SI Agresor din cadrul autorităților administrative și instituțiilor din subordinea Ministerului Afacerilor Interne, care, conform competențelor, examinează adresările și sesizările cetățenilor referitoare la cazurile de violență în familie, înregistrează informațiile cu privire la cauzele penale și contravenționale de violență în familie și evoluțiile cazurilor înregistrate și deciziilor adoptate ca urmare a examinării, asigură evidența ordinelor de restricție de urgență și deciziilor judiciare emise.

24. Furnizorii de date ai SI Agresor sunt:

1) Ministerul Afacerilor Interne, prin intermediul:

a) autorităților administrative din subordinea Ministerului Afacerilor Interne, care în funcție de competențele funcționale, înregistrează cazurile de violență în familie sesizate;

b) subdiviziunilor specializate și teritoriale ale Poliției, care identifică, înregistrează și actualizează în banca de date cu privire la cazurile de violență în familie sesizate;

c) angajaților Poliției, care furnizează informații privind cazurile de violență în familie, eliberarea ordinului de restricție de urgență, emiterea ordonanței de protecție, informarea agresorului despre restricțiile aplicate în privința acestuia;

2) Ministerul Muncii și Protecției Sociale, prin intermediul:

a) Agențiilor teritoriale de asistență socială, care implementează direct și prin intermediul structurilor teritoriale de asistență socială, politica de stat în domeniul prevenirii și combaterii violenței în familie;

b) Structurilor teritoriale de asistență socială, structurilor responsabile de asistența socială și protecția drepturilor copilului din municipiul Chișinău și din unitatea teritorială autonomă Găgăuzia, prin intermediul serviciului responsabil de domeniul prevenirii și combaterii violenței în familie și al reabilitării victimelor infracțiunii care înregistrează și actualizează informațiile în baza de date la nivel teritorial cu privire la cazurile de violență în familie;

c) Centrelor și serviciilor de reabilitare a victimelor și agresorilor, care furnizează informații privind serviciile acordate victimelor și agresorilor, asistența oferită victimelor prin ordonanța de protecție și restricțiile aplicate în privința agresorului;

3) Ministerul Educației și Cercetării, prin intermediul direcțiilor generale de învățământ, tineret și sport, care furnizează informații în adresa autorităților tutelare și Poliției privind sesizarea de către cadrele didactice a cazurilor de violență în familie, inclusiv despre cazurile de violență în familie împotriva copiilor;

4) Ministerul Sănătății, prin intermediul instituțiilor medicale de toate tipurile și nivelurile, care furnizează informații în adresa autorităților tutelare și Poliției privind sesizarea de către cadrele medicale a cazurilor de violență în familie;

5) Ministerul Justiției, prin intermediul:

a) Administrației Naționale a Penitenciarelor, care furnizează informații privind realizarea programelor de corecție pentru agresorii familiali în penitenciare, precum și informarea victimei despre eliberarea din detenție a agresorului;

b) Inspectoratului Național de Probațiune, care furnizează informații privind realizarea programelor probaționale, aplicarea monitorizării electronice și tentativele de încălcare a măsurilor de protecție aplicate de către instanța de judecată.

6) Procuratura Generală, care prin intermediul procuraturilor teritoriale, furnizează registratorului informații cu privire la:

a) liberarea condiționată a persoanei de răspundere penală pentru actele de violență în familie;

b) expedierea cauzei penale în instanța de judecată.

7) Consiliul Național pentru Asistență Juridică Garantată de Stat, prin intermediul oficiilor teritoriale, care oferă asistență juridică gratuită victimelor violenței în familie. Aceste oficii asigură suport legal și reprezentare în instanță pentru a proteja drepturile și siguranța victimelor.

25. Destinatari ai datelor din SI Agresor sunt beneficiarii de servicii, persoanele fizice, autoritățile/instituțiile publice și persoanele juridice de drept public, mandatate cu dreptul de a primi datele respective, conform legislației privind accesul la informație și a celei în domeniul schimbului de date și interoperabilității, cu drept de acces deplin sau partajat, public sau intern în SI Agresor.

26. Destinatarii datelor SI Agresor sunt următoarele autorități și instituții abilitate cu funcții de prevenire și de combatere a violenței în familie:

1) autoritățile publice centrale de specialitate:

a) Agenția Națională de Prevenire și Combatere a Violenței împotriva Femeilor și a Violenței în Familie;

b) Ministerul Afacerilor Interne;

b) Ministerul Muncii și Protecției Sociale;

c) Ministerul Educației și Cercetării;

d) Ministerul Sănătății;

e) Ministerul Justiției.

2) agențiile teritoriale de asistență socială;

3) autoritățile de specialitate ale administrației publice locale de nivelul al doilea şi structurile desconcentrate:

a) subdiviziunile teritoriale ale poliției;

b) structurile teritoriale de asistență socială, structurile responsabile de asistența socială și protecția drepturilor copilului din municipiul Chișinău și din unitatea teritorială autonomă Găgăuzia;

c) direcțiile generale de învățământ, tineret și sport;

d) organele ocrotirii sănătății.

4) administrația publică locală de nivelul întâi;

a) comisiile pentru probleme sociale de pe lingă autoritățile administrației publice locale;

b) centrele/serviciile de asistență și protecție a victimelor violenței în familie și a copiilor lor și centrele/serviciile de asistență și consiliere pentru agresorii familiali.

5) procuraturile teritoriale;

6) instanțele de judecată;

7) inspectoratele regionale și birourile de probațiune;

8) penitenciarele;

9) alte organizații cu activități specializate în domeniu.

27. Destinatarul datelor poate raporta posesorului problemele ce țin de accesarea informației conținute în SI Agresor.

IV. DREPTURILE ŞI OBLIGAŢIILE SUBIECŢILOR LA CREAREA, EXPLOATAREA ŞI UTILIZAREA SI AGRESOR

28. Utilizatorii beneficiază de drepturi de acces la informația din SI Agresor conform atribuțiilor și funcțiilor deținute. Nivelul de acces la informație pentru fiecare participant corespunde funcției de serviciu și profilului de acces. Resursele informaționale ale SI Agresor se accesează în conformitate cu Legea nr. 148/2023 privind accesul la informațiile de interes public și în limitele stabilite de aceasta, cu Legea nr. 216/2003 cu privire la Sistemul informațional integrat automatizat de evidență a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni, Legea nr. 185/2020 cu privire la Sistemul informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții, Legea nr. 133/2011 privind protecția datelor cu caracter personal, precum și în conformitate cu alte acte normative.

29. Dreptul de acces la resursele informaționale ale SI Agresor este segmentat pe unități de conținut, atribuind prerogative partajate, și anume: vizualizare, adăugare, redactare și radiere.

Secțiunea 1
Drepturile și obligațiile posesorului SI Agresor

30. Posesorul SI Agresor are dreptul:

1) să dezvolte, în funcție de competența sa, cadrul normativ cu privire la SI Agresor;

2) să propună și să pună în aplicare soluții pentru perfecționarea și eficientizarea procesului de funcționare a SI Agresor;

31. Posesorul SI Agresor este obligat:

1) să supravegheze respectarea cerințelor de securitate a informației de către utilizatorii sistemului respectiv, să fixeze cazurile și tentativele de încălcare a acestora;

2) să asigure atribuirea rolurilor și a drepturilor de acces la interfață și date;

3) să efectueze monitorizarea și supravegherea accesărilor informației;

4) să identifice încălcările comise și să întocmească un raport privind datele accesate;

5) să asigure funcționarea și ținerea SI Agresor în conformitate cu cadrul normativ;

6) să asigure funcționarea neîntreruptă a SI Agresor;

7) să acorde suportul necesar utilizatorilor care au acces la SI Agresor privind folosirea complexului de mijloace software aferente acestuia;

8) să stabilească condițiile tehnice de funcționare a SI Agresor;

9) să efectueze măsurile organizatorico-tehnice necesare asigurării protecției și confidențialității informației stocate în SI Agresor, inclusiv împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate;

10) să asigure implementarea măsurilor organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal în conformitate cu legislația în materie de protecție a datelor cu caracter personal;

11) să asigure accesul securizat la informația conținută în SI Agresor, respectarea condițiilor de securitate și a regulilor de exploatare ale acestuia;

12) să suspende sau să revoce dreptul de acces la SIAgresor pentru utilizatorii care nu respectă condițiile de securitate și regulile de exploatare ale acestuia, precum și regulile, standardele și normele general acceptate în domeniul securității informaționale;

13) să utilizeze informația obținută din baza de date a SI Agresor doar în scopurile stabilite de legislație.

Secțiunea 2
Drepturile și obligațiile deținătorului SI Agresor

32. Deținătorul tehnic are dreptul:

1) să elaboreze și să dezvolte, în baza competențelor sale, cadrul normativ cu privire la SI Agresor;

2) să propună soluții de perfecționare, dezvoltare și eficientizare a procesului de funcționare a SI Agresor, precum și să le pună în aplicare;

3) să supravegheze respectarea cerințelor de creare a metadatelor de către registratorii SI Agresor;

4) să realizeze competențele privind dezvoltarea, menținerea și funcționarea SI Agresor;

5) să monitorizeze exploatarea SI Agresor de către utilizatori;

6) să solicite de la registratori și de la furnizori actualizarea sau corectarea datelor în baza de date a SI Agresor, în cazul depistării omisiunilor și a erorilor;

7) să suspende sau să revoce dreptul de acces la SI Agresor pentru utilizatorii care nu respectă condițiile de securitate și regulile de exploatare a acestuia, precum și regulile, standardele și normele general acceptate în domeniul securității informaționale;

8) să înainteze posesorului propuneri de eficientizare a activității SI Agresor;

9) să realizeze alte activități necesare pentru asigurarea bunei funcționări a SI Agresor.

33. Deținătorul este obligat:

1) să asigure condițiile organizatorice și financiare pentru crearea și funcționarea SI Agresor;

2) să asigure dezvoltarea continuă a SI Agresor, prin adăugarea noilor componente ce pot fi utilizate de către participanți;

3) să autorizeze, să suspende și să revoce dreptul de acces pe SI Agresor în condițiile prezentului Regulament;

4) să stabilească măsurile tehnice și organizatorice de protecție și securitate a SI Agresor;

5) să organizeze seminare și instruiri de utilizare a SI Agresor pentru Registratori;

6) să asigure securitatea și protecția datelor din SI Agresor;

7) să asigure păstrarea metadatelor din SI Agresor și imposibilitatea modificării neautorizate a acestora;

8) să asigure acordarea suportului metodologic și practic registratorilor în procesul de creare sau actualizare a metadatelor din SI Agresor;

9) să asigure elaborarea și menținerea ghidului utilizatorilor SI Agresor;

10) să monitorizeze și să supravegheze accesările din SI Agresor;

11) să efectueze măsurile organizatorico-tehnice necesare pentru a asigura protecția și confidențialitatea informației stocate în SI Agresor, inclusiv împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, menite să asigure un nivel de securitate adecvat față de riscurile prezentate de prelucrarea și de caracterul datelor prelucrate;

12) să exercite alte atribuții necesare pentru asigurarea bunei funcționări a SI Agresor.

Secțiunea 3
Drepturile și obligațiile administratorului tehnic al SI Agresor

34. Administratorul tehnic are următoarele drepturi:

1) dreptul să monitorizeze utilizarea resurselor de către SI Agresor;

2) dreptul să administreze componentele tehnologice.

35. Administratorul tehnic are următoarele obligații:

1) să asigure funcționarea în conformitate cu legislația Republicii Moldova;

2) să asigure un nivel de securitate și confidențialitate adecvat ceea ce privește riscurile prezentate de prelucrare și caracterul datelor.

Secțiunea 4
Drepturile și obligațiile registratorului SI Agresor

36. Registratorul are dreptul:

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

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

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

4) să înainteze posesorului propuneri privind modificarea actelor normative care reglementează funcționarea SI Agresor;

5) să solicite și să primească de la posesor, deținător și administratorul tehnic susținere metodologică și practică privind funcționarea SI Agresor;

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

7) să înainteze posesorului, deținătorului și administratorului tehnic propuneri privind îmbunătățirea și sporirea eficacității funcționării SI Agresor;

37. Registratorul este obligat:

1) să asigure corectitudinea, autenticitatea și veridicitatea datelor introduse în SI Agresor;

2) să asigure actualizarea datelor introduse în SI Agresor;

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

4) să utilizeze funcționalitățile SI Agresor în exclusivitate conform destinației acestora și în strictă conformitate cu legislația;

5) să utilizeze informația obținută din SI Agresor doar în scopurile stabilite de legislație.

Secțiunea 5
Drepturile și obligațiile furnizorului de date ale SI Agresor

38. Furnizorul are dreptul:

1) să participe la implementarea și dezvoltarea SI Agresor;

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

3)să înainteze posesorului propuneri privind îmbunătățirea și sporirea eficacității funcționării SI Agresor.

39. Furnizorul este obligat:

1) să implementeze măsuri organizatorice și tehnice necesare pentru furnizarea datelor din sistemele informaționale pe care le deține;

2) să asigure, în conformitate cu cadrul normativ în materie de schimb de date și interoperabilitate, disponibilitatea datelor din registrele și sistemele informaționale pe care le deține, prin servicii informaționale web expuse în platforma de interoperabilitate (MConnect);

3) să asigure corectitudinea, autenticitatea, veridicitatea și integritatea datelor furnizate;

4) să asigure actualitatea datelor furnizate;

5) să efectueze acțiunile de asigurare a securității informației, să documenteze cazurile și tentativele de încălcare a acesteia, precum și să întreprindă măsurile ce se impun pentru prevenirea și lichidarea consecințelor.

Secțiunea 6
Drepturile și obligațiile destinatarului datelor din SI Agresor

40. Destinatarul are dreptul:

1) să participe la implementarea și dezvoltarea SI Agresor;

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

3) să solicite și să primească de la posesorul, deținătorul și administratorul tehnic SI Agresor 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 SI Agresor în conformitate cu scopul prelucrării și rolul atribuit;

6) să vizualizeze datele/informațiile/documentele din SI Agresor în conformitate cu drepturile de acces stabilite, pornind de la atribuțiile și funcțiile deținute, fără dreptul de a modifica aceste date/informații/documente;

7) să prezinte posesorului SI Agresor propuneri privind perfecționarea și eficientizarea funcționării acestuia;

41. În funcție de rolurile atribuite, destinatarul este obligat:

1) să asigure corectitudinea, autenticitatea și confidențialitatea datelor/ informațiilor/documentelor prezentate;

2) să asigure actualizarea datelor/informațiilor/documentelor prezentate;

3) să asigure accesarea și utilizarea datelor/informațiilor/documentelor din SI Agresor în conformitate cu rolurile atribuite și scopul legitim de utilizare a acestora;

4) să efectueze acțiunile de asigurare a securității informației, să documenteze cazurile și tentativele de încălcare a acesteia, precum și să întreprindă măsurile ce se impun pentru prevenirea și lichidarea consecințelor;

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

6) să ia măsurile organizatorice și tehnice necesare pentru asigurarea regimului de confidențialitate și securitate a datelor cu caracter personal, în conformitate cu instrucțiunile posesorului SI Agresor;

7) să utilizeze informația obținută din baza de date a SI Agresor doar în scopurile stabilite de legislație;

8) să aducă la cunoștința posesorului SI Agresor, 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.

42. Accesul la datele din SI Agresor se realizează prin acordarea accesului utilizatorilor interni.

43. Actele se eliberează de către registratori. Se interzice utilizarea și dezvăluirea datelor cu caracter personal extrase din SI Agresor în scopuri contrare legii.

44. Exploatarea SI Agresor fără autorizare nominală este interzisă și urmează a fi considerată ca acces neautorizat la un sistem informațional public.

45. Dreptul de acces la SI Agresor nu este unul permanent, acesta poate fi suspendat sau revocat. Introducerea și/sau modificarea datelor în SI Agresor de pe un nume sau profil de utilizator străin este interzisă, urmând a fi considerată ca acces neautorizat. Utilizatorii urmează să se asigure de faptul că profilul de utilizator, precum și semnătura electronică, sunt confidențiale.

46. Revocarea/suspendarea dreptului de acces la SI Agresor se efectuează la cererea/demersul registratorului către 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 SI Agresor;

3) la constatarea de către posesor a încălcării securității informaționale;

4) în alte cazuri, în limitele legislației.

47. Lucrările profilactice planificate în complexul de mijloace software și hardware se efectuează după notificarea, în scris sau prin email, a registratorilor de către deținător, în baza planului coordonat cu administratorul tehnic, cu cel puțin două zile lucrătoare înainte de începerea lucrărilor, cu indicarea termenului de finalizare a acestora, după caz, dacă aceasta este posibil. Lucrările profilactice neplanificate se efectuează la solicitarea utilizatorilor și coordonarea prealabilă cu posesorul în situația nefuncționării sau funcționării necorespunzătoare a complexului de mijloace software și hardware.

V. INTEROPERABILITATEA CU ALTE SISTEME INFORMAȚIONALE

48. Pentru asigurarea actualizării operative și automate a conținutului informațional al SI Agresor 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 SI Agresor.

49. SI Agresor este găzduit pe platforma tehnologică guvernamentală comună (MCloud).

50. Pentru preluarea de date relevante în conținutul informațional, SI Agresor interacționează, prin intermediul platformei de interoperabilitate (MConnect), cu următoarele sisteme și resurse informaționale de stat:

1) SIA „Registrul de stat al populației”;
2) SIA „Registrul informației criminalistice și criminologice”;
3) SIA „Registrul de stat al contravențiilor”;
4) Programul Integrat de Gestionare a Dosarelor (PIGD);
5) SIA „Registrul procedurilor de executare”;
6) SIA „Registrul persoanelor reținute, arestate și condamnate”;
7) SIA „Registrul de stat al armelor”;
8) SIA „Registrul dactiloscopic”;
9) Sistemul informațional integrat al Poliției de Frontieră;
10) Sistemul informațional geografic național;
11) SIA al Serviciului național unic pentru apelurile de urgență 112;
12) Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”;
13) SIA „Registrul de stat al unităților administrativ-teritoriale și al străzilor din localitățile de pe teritoriul Republicii Moldova”;
14) SIA „Registrul de stat al unităților de drept”.

51. SI Agresor utilizează următoarele sisteme informaționale partajate:

1) platforma de interoperabilitate (MConnect);
2) serviciul electronic guvernamental integrat de semnătură electronică (MSign);
3) serviciul electronic guvernamental de autentificare şi control al accesului (MPass);
4) serviciul electronic guvernamental de jurnalizare (MLog);
5) serviciul electronic guvernamental de notificare (MNotify);
6) serviciul guvernamental de plăți electronice (MPay);
7) Sistemul informațional automatizat „Registrul împuternicirilor de reprezentare în baza semnăturii electronice” (MPower).

VI. ASIGURAREA PROTECȚIEI ȘI SECURITĂȚII INFORMAȚIEI SI AGRESOR

52. Datele din SI Agresor fac parte din categoria datelor care necesită a fi protejate. Asigurarea securității, confidențialității și a integrității datelor prelucrate în cadrul SI Agresor 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.

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

54. Obiecte ale asigurării protecției și securității datelor din SI Agresor se consideră tot 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 SI Agresor;

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

55. Securitatea informațională a SI Agresor se efectuează prin aplicarea metodelor și efectuarea acțiunilor descrise în Planul de continuitate al acestuia și, după caz, a procedurilor operaționale.

56. Posesorul/deținătorul SI Agresor asigură măsurile organizatorice și tehnice necesare pentru protecția datelor cu caracter personal împotriva distrugerii, modificării, blocării, copierii, răspândirii, precum și împotriva altor acțiuni ilicite, măsuri menite să asigure un nivel de securitate adecvat în ceea ce privește riscurile prezentate de prelucrare și caracterul datelor prelucrate. În cazul incidentelor de securitate, posesorul/deținătorul SI Agresor întreprinde măsurile necesare pentru depistarea sursei de producere a incidentului, efectuează analiza acestuia și înlătură cauzele incidentului de securitate cu informarea Centrului Național pentru Protecția Datelor cu Caracter Personal al Republicii Moldova.

57. Protecția datelor din SI Agresor 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 SI Agresor prin intermediul mecanismului de jurnalizare efectuat de deținătorul tehnic al acestuia.

58. Subiecții, la utilizarea și exploatarea SI Agresor, asigură implementarea normelor de securitate, aceasta 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 SI Agresor;

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

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

5) procedurile de control intern al subiectului SI Agresor privind respectarea condițiilor de securitate informațională.

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

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

61. 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, procedurile pe care trebuie să le respecte în strictă concordanță cu politica de securitate.

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

VII. ASIGURAREA CONTROLULUI INTERN ȘI EXTERN AL SI AGRESOR

63. Ținerea SI Agresor este supusă controlului intern și extern. Controlul intern privind organizarea și funcționarea SI Agresor se efectuează de către posesor. Controlul extern asupra respectării cerințelor privind crearea, ținerea, exploatarea și reorganizarea SI Agresor se efectuează de către instituțiile abilitate și certificate în domeniul auditului.

64. SI Agresor se înregistrează în Registrul resurselor și sistemelor informaționale de stat.

65. Responsabilitatea pentru organizarea funcționării SI Agresor aparține posesorului/deținătorului acestuia.

66. Anual, până la data de 31 ianuarie, posesorul prezintă Centrului Național pentru Protecția Datelor cu Caracter Personal un raport generalizat despre incidentele de securitate din cadrul SI Agresor, în conformitate cu pct. 90 din Cerințele față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal, aprobate prin Hotărârea Guvernului nr. 1123/2010.

67. Controlul legalității operațiilor de prelucrare a datelor cu caracter personal desfășurate în SI Agresor se efectuează de către Centrul Național pentru Protecția Datelor cu Caracter Personal.

68. Pentru asigurarea funcționalității eficiente și neîntrerupte a SI Agresor, schimbul informațional de date SI Agresor este asigurat în regim nonstop.

69. Funcționarea SI Agresor se suspendă de către administratorul tehnic, la inițiativa proprie sau la demersul persoanei responsabile din cadrul unității centrale de specialitate sau din cadrul Ministerului Afacerilor Interne, care asigură funcționalitatea sistemului informațional și a resurselor informaționale la nivel central și/sau local, după coordonarea prealabilă cu posesorul, în caz de apariție a uneia dintre următoarele situații:

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

2) la apariția impedimentului justificator;

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

4) în cazul apariției dificultăților tehnice în funcționarea complexului de mijloace software și hardware ale SI Agresor;

5) la cererea scrisă a posesorului.

70. În cazul apariției circumstanțelor excepționale și a dificultăților tehnice în funcționarea complexului de mijloace software și hardware al SI Agresor din vina persoanelor terțe, poate fi sistată funcționarea SI Agresor, cu informarea subiecților SI Agresor prin mijloacele tehnice disponibile.