



GUVERNUL REPUBLICII MOLDOVA

HOTĂRÂRE nr. ____

din _____ 2023

Chișinău

Cu privire la aprobarea Conceptului Sistemului informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”

În temeiul art. 22 lit. c), d) și e) 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 departamental „Evidența semnalărilor și evenimentelor de ordine publică”.
2. Se aprobă Conceptul Sistemului informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”, conform anexei.
3. Administrarea, mentenanța și dezvoltarea Sistemului informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică” vor fi asigurate de către Ministerul Afacerilor Interne.
4. Realizarea prevederilor prezentei hotărâri se va efectua din contul și în limitele mijloacelor financiare prevăzute în bugetul de stat și altor mijloace, conform legislației.
5. Ministerul Afacerilor Interne, în termen de 6 luni din momentul intrării în vigoare a prezentei hotărâri:
 - 1) va elabora și prezenta Guvernului pentru aprobare Regulamentul resursei informaționale formată de Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”;
 - 2) va asigura aducerea actelor normative în concordanță cu prezenta hotărâre.

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

Prim-ministru

NATALIA GAVRILIȚA

Contrasemnează:

Ministrul afacerilor interne

Ana Revenco

Aprobat
prin Hotărârea Guvernului nr.

CONCEPTUL
Sistemului informațional departamental
„Evidența semnalărilor și evenimentelor de ordine publică”

INTRODUCERE

Conceptul Sistemului informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică” (în continuare – *Concept*) este elaborat în conformitate cu Reglementarea tehnică RT 38370656-002:2006 „Procesele ciclului de viață al software-ului”, aprobată prin Ordinul ministrului Dezvoltării Informaționale nr. 78/2006.

Conceptul specifică cerințele de bază privind Sistemul informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică” (în continuare – *SID Semnalări*), definește scopul creării acestuia, funcțiile de bază, reieșind din sarcinile de principale ale Ministerului Afacerilor Interne (în continuare – MAI) în calitate de organ central de specialitate al administrației publice centrale, care realizează prerogativele constituționale ale Guvernului privind elaborarea, promovarea și realizarea politicii statului, în vederea asigurării legalității, ordinii și securității publice, protecției civile, apărării împotriva incendiilor, precum și respectării drepturilor și libertăților fundamentale ale cetățenilor.

Din perspectiva performanței instituționale, SID Semnalări permite optimizarea activităților subdiviziunilor MAI, care au drept scop apărarea drepturilor și libertăților fundamentale ale persoanei prin activități de menținere, asigurare și restabilire a ordinii și securității publice, de prevenire, investigare și de descoperire a infracțiunilor și contravențiilor.

Capitolul I
INFORMAȚII GENERALE

1. Resursa informațională formată de SID „Evidența semnalărilor și evenimentelor de ordine publică” cuprinde date sistematizate referitoare la:

1) informațiile cu privire la semnalări urgente și nonurgente parvenite/raportate prin mai multe canale, după cum urmează:

a) semnalări recepționate la unitățile operaționale de coordonare (sesizări și alte informații);

b) semnalări primite la telefon (prin intermediul Serviciului național unic pentru apelurile de urgență 112, la Dispecerate, la unitățile operaționale de coordonare sau pe linii directe);

c) petiții cu referire la fapte contravenționale sau infracțiuni, transmise online (prin portal web și email);

d) petiții depuse la Subdiviziunea de management documente (cu referire la fapte contravenționale sau infracțiuni);

e) documente (solicitări) transmise de alte instituții (cu referire la fapte contravenționale sau infracțiuni);

g) autosesizări;

h) semnalări recepționate prin intermediul sistemelor automatizate.

2) Informațiile cu privire la gestiunea evenimentelor desfășurate în spațiul public cu incidență pe domeniul de ordine și securitate publică și a fenomenului infracțional sau social;

3) Informațiile cu privire la legitimări și verificări auto realizate de angajații MAI și instituțiilor din subordinea acestuia în contextul realizării atribuțiilor funcționale.

2. În sensul prezentului Concept, noțiunile și termenii utilizați semnifică următoarele:

concept – document tehnic, prevăzut de Reglementarea tehnică RT 38370656-002:2006 „Procese ciclului de viață al software-ului” „*aprobată prin Ordinul ministrului dezvoltării informaționale nr.78/2006*”, care descrie ideologia creării și funcționării sistemului informațional automatizat;

eveniment - starea de fapt creată – fie prin succesiunea de mai multe incidente sau prin gravitatea incidentului, fie prin amploarea impactului în viața comunității – prin gestionarea căroră, forțele de ordine publică/situații de urgență desfășoară un ansamblu de măsuri suplimentare planificate și/sau aprobate;

semnalare – anunț sau înștiințare parvenită în adresa aparatului central al MAI ori autorității administrative sau instituției din subordinea sa, indiferent de canalul prin care acestea ajung (comunicate prin telefon, transmise online prin portal web și/sau email, documente și petiții depuse la Subdiviziunea de management documente sau transmise de la alte instituții) ce vizează fapte cu caracter contravențional sau infracțional, inclusiv o situație de urgență.

unitate operațională de coordonare – subdiviziune structurală din cadrul autorităților administrative și instituțiilor din subordinea MAI, precum și din cadrul subdiviziunilor subordonate acestora, cu program permanent de muncă (24/7), abilitată cu atribuții de monitorizare a situației operative și/sau de asigurare a managementului fluxului informațional (dispecerat, serviciu de gardă, serviciu de coordonare operațională, centru operativ de dispecerat republican, serviciu de dispecerat).

3. SID Semnalări este destinat să asigure, în conformitate cu funcțiile ce-i revin, suportul informațional al activității organelor de drept, din sfera de competență a MAI, în scopul menținerii ordinii de drept și combaterii infracționalității, precum și formarea unui echivalent digital al dosarului pe

suport de hârtie despre sesizarea cu privire la comiterea unei infracțiuni sau contravenții, actele procesuale întocmite în contextul examinării până la formularea propunerii de a nu porni urmărirea penală ori adoptarea ordonanței de intentare a cauzei penale sau pornirea procesului contravențional cu referire la gestiunea unui eveniment din sfera de competență a MAI.

4. Obiectivele SID Semnalări sunt:

- 1) asigurarea unei interfețe unice de înregistrare și documentare a semnalărilor, evenimentelor și legitimărilor;
- 2) organizarea interacțiunii eficiente și a schimbului de informații dintre autoritățile administrative și instituțiile din subordinea MAI;
- 3) colectarea și prelucrarea operativă a informației privind recepționarea semnalărilor, evenimentelor și legitimărilor, precum și altor date de referință;
- 4) formarea resursei informaționale departamentale pe domeniul de competență instituțional;
- 5) evidența statistică și analitică privind activitățile realizate și resursele implicate pentru activitățile asociate gestiunii semnalărilor, evenimentelor și legitimărilor;
- 6) asigurarea respectării prevederilor legislației naționale în domeniul protecției datelor cu caracter personal;
- 7) dezvoltarea soluțiilor tehnice flexibile și modulare care ar permite îmbunătățirea activității MAI;
- 8) sporirea transparenței activității;
- 9) îmbunătățirea condițiilor de activitate în cadrul MAI.

5. SID Semnalări are următoarele sarcini:

- 1) asigurarea recepționării, înregistrării și prelucrării tuturor informațiilor privind semnalările, evenimentele și legitimările pe domeniul de competență al MAI, autoritățile administrative și instituțiile din subordinea acestuia;
- 2) asigurarea interacțiunii informaționale cu sistemele informaționale de stat, departamentale, teritoriale, în special cu Registrul de stat al populației, Registrul de stat al unităților de drept, Registrul de stat al conducătorilor de vehicule, Registrul de stat al transporturilor, Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112, Sistemul informațional integrat al organelor de drept;
- 3) asigurarea securității informaționale la formarea și exploatarea resursei informaționale.

6. SID Semnalări este creat în baza următoarelor principii:

- 1) *principiul legitimității* – funcțiile și operațiile realizate în SID Semnalări de utilizatorii acestuia sunt de natură legală, în conformitate cu drepturile omului și legislația națională;

2) *principiul autenticității datelor* – datele stocate și prezentate de către SID Semnalări sunt autentice. Autenticitatea datelor este certificată de prezența înregistrării de creare a acestora, precum și de semnătura electronică aplicată acestor documente electronice. Autenticitatea documentelor electronice asigură, de asemenea, și nonrepudierea datelor;

3) *principiul temeinicieii datelor* – introducerea datelor în SID Semnalări se efectuează doar în baza înscrierilor din documentele acceptate drept surse de informații;

4) *principiul confidențialității informației* – răspunderea personală, în conformitate cu legislația, a persoanelor responsabile de prelucrarea informației în SID Semnalări pentru utilizarea și difuzarea neautorizată a acesteia;

5) *principiul extensibilității* – componentele SID Semnalări oferă facilități de ajustare și de extindere a funcționalităților existente pentru conformare cu necesitățile viitoare;

6) *principiul securității* – asigurarea nivelului dorit de integritate, exclusivitate, accesibilitate și eficiență a protecției datelor împotriva pierderii, denaturării, distrugerii și utilizării neautorizate. Securitatea sistemului presupune rezistența la atacuri și protecția caracterului confidențial, a integrității și a pregătirii pentru lucru atât a SID Semnalări, cât și a datelor acestuia.

Capitolul II

CADRUL NORMATIV-JURIDIC

AL SISTEMULUI INFORMAȚIONAL

7. Actele normative de reglementare a creării și funcționării SID Semnalări sunt:

- 1) Acte ce reglementează activitatea instituțiilor MAI:
 - a) Codul penal nr. 985/2002;
 - b) Codul civil nr. 1107/2002;
 - c) Codul de procedură penală nr. 122/2003;
 - d) Codul de procedură civilă nr. 225/2003;
 - e) Codul contravențional nr. 218/2008;
 - f) Legea nr. 50/2012 privind prevenirea și combaterea criminalității organizate;
 - g) Legea nr. 59/2012 privind activitatea specială de investigații;
 - h) Legea nr. 320/2012 cu privire la activitatea Poliției și statutul polițistului;
 - i) Legea nr. 288/2016 privind funcționarul public cu statut special din cadrul Ministerului Afacerilor Interne;
 - j) Codul administrativ al Republicii Moldova nr. 116/2018;

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

l) Hotărârea Guvernului nr. 1340/2001 cu privire la Comisia pentru Situații Excepționale a Republicii Moldova;

m) Hotărârea Guvernului nr. 1109/2010 pentru aprobarea Concepției de reformare a Ministerului Afacerilor Interne și a structurilor subordonate și desconcentrate ale acestora;

n) Hotărârea Guvernului nr. 914/2014 cu privire la aprobarea Regulamentului de organizare și funcționare, a structurii și a efectivului-limită ale Biroului migrație și azil din subordinea Ministerului Afacerilor Interne;

o) Hotărârea Guvernului nr. 693/2017 cu privire la organizarea și funcționarea Ministerului Afacerilor Interne;

p) Hotărârea Guvernului nr. 1145/2018 cu privire la organizarea și funcționarea Inspectoratului General al Poliției de Frontieră;

q) Hotărârea Guvernului nr. 120/2019 cu privire la organizarea și funcționarea Inspectoratului de Management Operațional al MAI;

r) Hotărârea Guvernului nr. 547/2019 cu privire la organizarea și funcționarea Inspectoratului General al Poliției;

s) Hotărârea Guvernului nr. 317/2020 cu privire la organizarea și funcționarea Serviciului Tehnologii Informaționale.

2) Acte normative ce reglementează accesul la informație:

a) Legea nr. 982/2000 privind accesul la informație;

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

c) Legea nr. 245/2008 cu privire la secretul de stat;

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

e) Hotărârea Guvernului nr. 1176/2010 pentru aprobarea Regulamentului cu privire la asigurarea regimului secret în cadrul autorităților publice și al altor persoane juridice.

3) Acte normative în domeniul securității informației și TIC:

a) 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;

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

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

d) Hotărârea Guvernului nr. 1202/2006 cu privire la aprobarea Concepției Sistemului integrat al organelor de drept;

e) Hotărârea Guvernului nr. 834/2008 cu privire la Sistemul informațional integrat al Poliției de Frontieră;

- f) 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;
- g) Hotărârea Guvernului nr. 709/2011 cu privire la unele măsuri în domeniul e-Transformare a guvernării;
- h) Hotărârea Guvernului nr. 710/2011 cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare);
- i) Hotărârea Guvernului nr. 1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass);
- j) Hotărârea Guvernului nr. 128/2014 privind platforma tehnologică guvernamentală comună (MCloud);
- k) Hotărârea Guvernului nr. 708/2014 privind serviciul electronic guvernamental de jurnalizare (MLog);
- l) Hotărârea Guvernului nr. 201/2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;
- m) Hotărârea Guvernului nr. 211/2019 privind platforma de interoperabilitate (MConnect);
- n) 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);
- o) Hotărârea Guvernului nr. 405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign);
- p) Ordinul Interdepartamental al Procurorului General / Ministerului Afacerilor Interne / Directorului Serviciului Vamal / Directorului Centrului Național Anticorupție nr. 121/254/286-O/95 din 18 iulie 2008, cu privire la evidența unică a infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni;
- q) Standardul SM 12207:2005 „Procese ciclului de viață al software-ului”;
- r) Ordinul ministrului Dezvoltării Informaționale nr. 78/2006 cu privire la aprobarea reglementării tehnice „Procese ciclului de viață al software-ului” RT 38370656 - 002:2006.

Capitolul III

SPAȚIUL FUNCȚIONAL AL SID SEMNALĂRI

8. Funcțiile de bază ale SID Semnalări sunt următoarele:

- 1) *Formarea resursei informaționale.* Funcțiile de bază în procesul de formare a bazei de date a SID Semnalări sunt funcțiile de înregistrare, actualizare a datelor și scoaterea din evidență a obiectelor informaționale (schimbarea statutului obiectului). Aceste funcții se execută în funcție de îndeplinirea unor sau altor scenarii de bază:

a) înregistrarea inițială a obiectelor informaționale se efectuează după ce registratorul ia decizia de a include obiectul în SID Semnalări. Fiecărui obiect informațional luat la evidență i se atribuie un identificator unic (cu excepția obiectelor informaționale împrumutate), care rămâne neschimbat pe toată perioada existenței obiectului în SID Semnalări, iar în baza de date a SID Semnalări se introduc date despre obiectul de evidență și atributele acestuia;

b) actualizarea datelor SID Semnalări constă în reînnoirea sistematică a bazei de date a acestuia în cazul modificării sau completării atributelor obiectelor de evidență;

c) scoaterea din evidență a obiectului informațional constă în schimbarea statutului obiectului, în baza deciziei registratorului, la intervenirea unor evenimente, prin aplicarea unei mențiuni speciale, fapt care nu semnifică eliminarea fizică a datelor despre obiect din SID Semnalări;

d) informația se elimină din SID fizic numai după expirarea termenului de păstrare a informației în arhiva electronică (5 ani).

Informația se introduce în SID Semnalări doar în baza deciziei registratorului. Toate schimbările în sistem se păstrează în ordine cronologică.

2) *Organizarea suportului informațional.* Informațiile din baza de date a SID Semnalări sunt oferite în funcție de nivelul de acces stabilit. Utilizatorii datelor din sistem sunt obligați să le folosească doar în scopuri legale.

Nivelul accesului utilizatorului datelor SID Semnalări la informația solicitată este stabilit de legislație, în funcție de statutul său juridic și regimul juridic al informației. În cazul depistării neconcordanțelor dintre datele care se conțin în documentele emise în cadrul funcționării SID Semnalări și datele din baza de date a SID Semnalări, informația din baza de date a SID Semnalări se consideră de bază.

3) *Asigurarea securității și protecției informațiilor.* Asigurarea securității și protecției informațiilor la toate etapele de colectare, stocare și utilizare a resurselor informaționale de stat care se referă la domeniul de competență al SID Semnalări.

4) *Asigurarea calității informației.* Calitatea informației se asigură prin crearea și susținerea componentelor sistemului de calitate, bazate pe materia procesuală.

5) *Asigurarea interacțiunii SID Semnalări cu alte sisteme informaționale.* Funcția respectivă presupune o interacțiune și integrare cu alte sisteme informaționale de stat, departamentale sau sisteme informaționale partajate.

9. Spațiul funcțional al SID Semnalări reprezintă un set de funcții realizate de module funcționale separate, care interacționează reciproc.

În cadrul SID Semnalări sunt realizate următoarele module funcționale:

1) gestiunea semnalărilor urgente și non-urgente parvenite/raportate prin mai multe canale;

2) gestiunea evenimentelor desfășurate în spațiul public cu incidență în domeniul ordinii și securității publice și a fenomenului infracțional sau social;

3) gestiunea legitimărilor cetățenilor și verificărilor auto realizate de angajații MAI și autoritățile administrative și instituțiile din subordinea acestuia, în contextul realizării atribuțiilor funcționale.

10. În cadrul SID Semnalări sunt realizate următoarele contururi funcționale:

1). Conturul funcțional privind interacțiunea informațională a tuturor componentelor SID Semnalări „Administrarea și monitorizarea acțiunilor participanților la SID Semnalări”, care reprezintă un sistem integrat de control și monitorizare privind formarea și utilizarea resursei informaționale în domeniul evidenței tuturor semnalărilor, care sunt furnizate prin apelurile de urgență și a solicitărilor de intervenție din partea Serviciului național unic pentru apelurile de urgență 112, primite la unitățile operaționale de coordonare de la cetățeni, primite la telefon (prin intermediul Dispeceratelor, unităților operaționale de coordonare sau liniilor directe/speciale), ce se conțin în petiții depuse la Subdiviziunea de management documente cu referire la fapte contravenționale sau infracțiuni transmise online (inclusiv parvenite prin portal web sau email), autosesizări, alte documente și solicitări transmise de alte instituții (cu referire la fapte contravenționale sau infracțiuni), după caz, alerte recepționate prin intermediul sistemelor automatizate, evidenței informațiilor și activităților întreprinse de instituțiile și organizațiile din subordinea MAI, în contextul realizării atribuțiilor de asigurare a ordinii și securității publice conexe evenimentelor desfășurate în spațiul public cu incidență pe domeniul de ordine și securitate publică și a fenomenului infracțional sau social, asigurarea evidenței activităților care presupun prelucrarea datelor cu caracter personal, în legătură cu realizarea legitimărilor cetățenilor și verificări auto realizate de angajații MAI și instituțiilor din subordinea acestuia, precum și documentelor în format electronic și/sau copiilor documentelor întocmite/colectate în cadrul activităților menționate supra.

Acest contur asigură:

- 1) integritatea logică a SID Semnalări;
- 2) administrarea bazelor de date ale SID Semnalări;
- 3) delimitarea drepturilor de acces pentru utilizatori, introducerea sistemului de parole;
- 4) securitatea, protecția și păstrarea informației în sistem conform standardelor internaționale SM ISO/CEI 27002 „Tehnologii informaționale. Cod de bună practică pentru managementul securității informaționale” și SM ISO/CEI 15408 „Tehnologii Informaționale. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informației”;
- 5) respectarea cerințelor SID Semnalări privind protecția datelor cu caracter personal.

2). Conturul funcțional „Înregistrarea apelurilor de semnalări” asigură:

- 1) recepționarea, înregistrarea și prelucrarea semnalărilor;
- 2) filtrarea semnalărilor (în scopul identificării competenței teritoriale și materiale), direcționarea acestora în regim automat către instituțiile, organizațiile și subdiviziunile competente;
- 3) recepționarea, înregistrarea și documentarea semnalărilor parvenite în adresa autorităților administrative și instituțiilor din subordinea MAI, precum formarea resursei informaționale unice a acestora;
- 4) schimbul de informații dintre locurile de lucru automatizate ale utilizatorilor în scopul obținerii datelor suplimentare despre activitățile întreprinse și rezultatele acestora.

3). Conturul funcțional „Informația de referință” asigură:

- 1) înregistrarea solicitărilor;
- 2) evidența informațiilor, materialelor colectate sau prezentate la solicitarea autorităților publice, persoanelor fizice sau juridice, conform prevederilor actelor normative.

Funcția comună pentru toate contururile funcționale este formarea rapoartelor statistice.

Capitolul IV

SPAȚIUL ORGANIZATORIC AL SID SEMNALĂRI

11. Posesorul SID Semnalări este MAI.

12. Deținătorul și administratorul tehnic SID Semnalări este Serviciul Tehnologii Informaționale din subordinea MAI, care asigură crearea, administrarea, mentenanța și dezvoltarea sistemului informațional, își exercită atribuțiile în conformitate cu cadrul normativ în materie de administrare tehnică și menținere a sistemelor informaționale ale MAI.

13. Registratorii SID Semnalări sunt:

- 1) angajatul desemnat în cadrul entității pentru înregistrare și evidență statistică, operatorii unităților operaționale de coordonare, precum liniilor directe din cadrul autorităților administrative și instituțiilor din subordinea MAI, care înregistrează apelurile telefonice primite, mesajele primite prin fax, SMS, MMS, mesajele de pe portalul web, mesajele comunicate prin intermediul sistemelor de supraveghere video, al sistemelor de alarmă, de avertizare, adresările și petițiile cetățenilor și organizațiilor;
- 2) utilizatorii SID Semnalări din cadrul autorităților administrative și instituțiilor din subordinea MAI, care conform competențelor, examinează adresările cetățenilor, înregistrează informațiile cu privire la evoluțiile situațiilor de urgență și ordine publică, precum și rezultatele reacționării și intervenției.

14. Furnizorii de informații în SID Semnalări, care oferă informația ce se referă la gestiunea semnalărilor, evenimentelor și legitimărilor, sunt:

- 1) autoritățile administrative și instituțiile din subordinea MAI;
- 2) Ministerul Sănătății, inclusiv Agenția Națională pentru Sănătate Publică;
- 3) autoritățile administrației publice centrale și locale.

Capitolul V

DOCUMENTELE SID SEMNALĂRI

15. În cadrul SID Semnalări se utilizează documente de intrare și documente de ieșire și documente tehnologice.

16. Documente de intrare sunt documentele cu privire la semnalări urgente și non-urgente parvenite/raportate prin mai multe canale enumerate în subpunctul 1) al pct. 1, din prezentul Concept.

17. Documente de ieșire includ rapoarte analitice și statistice referitoare la evidența informațiilor, materialelor colectate sau prezentate la solicitarea autorităților publice, persoanelor fizice sau juridice, conform prevederilor actelor normative.

18. Documente tehnologice includ:

- 1) regulamentele de interacțiune între autoritățile administrative și instituțiile din subordinea MAI sau acordurile încheiate;
- 2) regulamentele de interacțiune între autoritățile administrative și instituțiile din subordinea MAI și alte persoane juridice sau acorduri încheiate;
- 3) regulamentele interne și instrucțiunile care stabilesc ordinea acțiunilor angajaților diferitor subdiviziuni ale autorităților administrative și instituțiilor din subordinea MAI;
- 4) registrele, rapoartele, documentele de însoțire;
- 5) alte documente, conform cerințelor actelor normative.

19. Lista și conținutul documentelor se determină de actele normative ce reglementează raporturile juridice care apar în contextul realizării atribuțiilor conform domeniului de competență a MAI, autorităților administrative și instituțiilor din subordinea acestuia.

Capitolul VI

SPAȚIUL INFORMAȚIONAL AL SISTEMULUI

20. Resursa informațională a SID Semnalări cuprinde următoarele obiecte informaționale:

- 1) semnalări:
 - a) semnalări primite la unitățile operaționale de coordonare (sesizări și alte informații);
 - b) semnalări recepționate prin telefon (prin dispecerate, unitățile operaționale de coordonare sau pe linii directe);
 - c) petiții transmise online (prin portal web și email);
 - d) petiții depuse la Subdiviziunea de management documente;
 - e) documente (solicitări) transmise de alte instituții;
 - f) autosesizări;
 - g) semnalări recepționate prin intermediul sistemelor automatizate.
- 2) eveniment și/sau situația de urgență (desfășurate în spațiul public cu incidență în planul ordinii publice și a fenomenului infracțional sau social);
- 3) legitimare a cetățeanului/cetățenilor și/sau verificări auto:
 - a) persoanele fizice (*obiect împrumutat din Registrul de stat al populației*);
 - b) persoanele juridice (*obiect împrumutat din Registrul de stat al unităților de drept*);
- 4) documentele din următoarele categorii:
 - a) certificatele și extrasele din SID Semnalări;
 - b) instrucțiunile și regulamentele interne.

21. Identificarea obiectelor informaționale se efectuează prin utilizarea numărului de identificare unic pentru fiecare obiect al SID Semnalări în parte:

1) identificator al obiectului informațional „Semnalări” este numărul de identificare, care are următoarea structură:

YY NNNNNN, unde:

YY – ultimele două cifre ale anului în care este înregistrată semnalarea;

NNNNNN – numărul de ordine al apelării Serviciului 112 în anul respectiv.

Numărul în cauză este generat în mod automat în SID Semnalări și este atribuit fiecărei semnalări;

2) identificator al obiectului informațional „eveniment” este numărul de identificare, care are următoarea structură:

XX NNNNNN, unde:

XX – ultimele două cifre ale anului în care este înregistrată situația de urgență;

NNNNNN – numărul de ordine al situației de urgență, înregistrat în SID Semnalări în anul respectiv;

3) identificator al obiectului informațional „legitimare” este numărul de identificare, care are următoarea structură:

XX NNNNNN, unde:

XX – ultimele două cifre ale anului în care este înregistrată situația de urgență;

NNNNNN – numărul de ordine al situației de urgență, înregistrat în SID Semnalări în anul respectiv;

4) identificator al obiectului informațional „persoană fizică” este numărul de identificare de stat al persoanei fizice din Registrul de stat al populației (IDNP);

5) identificator al obiectului informațional „persoană juridică” este numărul de identificare de stat al unității de drept din Registrul de stat al unităților de drept (IDNO);

6) identificator al obiectului informațional „document”, format din: „tipul documentului” + „numărul” + „seria”.

22. Scenariile de bază reprezintă o listă de evenimente ce se produc cu obiectul informațional și se țin în evidență în SID Semnalări. Acestea se divizează în două grupe:

1). înregistrarea inițială, actualizarea și scoaterea obiectelor informaționale din evidență;

2). furnizarea informației.

Grupa scenariilor legate de înregistrarea inițială și actualizarea informației interacționează cu obiectele informaționale ale SID Semnalări, după cum urmează:

1) pentru obiectul informațional „semnalare”, „eveniment” și „legitimare”.

Înregistrarea inițială în evidență a semnalărilor:

a) la preluarea apelului telefonic;

b) la preluarea corespondenței oficiale, prin Subdiviziunea de management documente;

c) la depunerea raportului de autosesizare;

d) la recepționarea sesizării cetățeanului, inclusiv, depuse prin email sau pagina oficială;

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

Înregistrarea inițială în evidență a evenimentelor:

a) la preluarea corespondenței oficiale, prin Subdiviziunea de management documente;

b) la depunerea raportului de către angajații subdiviziunii competente.

Înregistrarea inițială în evidență a legitimării:

a) la inițiativa angajatului care a realizat legitimarea cetățeanului/cetățenilor și/sau verificări auto;

b) în baza raportului/informației verbale (prin sistemul de comunicații speciale sau apel telefonic) sau în formă scrisă a angajatului instituției sau organizație din subordinea MAI, de către angajatul desemnat pentru înregistrare sau operatorul Dispeceratului.

Actualizarea datelor: la recepționarea informației suplimentare cu referință la semnalarea preluată anterior.

Scoaterea din evidență a semnalării (schimbarea statutului): la transferarea semnalării din statut activ în cel inactiv, cu transmiterea ulterioară în baza de date de evidență a cauzelor penale, contravenționale, în baza ordonanței procurorului (hotărârii judecătorești) de neîncepere a urmăririi penale ori semnare a încheierii de încetare a controlului semnalării, cu transmiterea în arhivă a semnalărilor înregistrate.

Scoaterea din evidență a evenimentului (schimbarea statutului): la transferarea evenimentului din statut activ în cel inactiv, cu transmiterea ulterioară în baza de date în arhivă a evenimentelor înregistrate.

Scoaterea din evidență a legitimării (schimbarea statutului): la transferarea legitimării din statut activ în cel inactiv, cu transmiterea ulterioară în baza de date în arhivă a legitimărilor înregistrate.

2) pentru obiectul informațional „persoană fizică”:

Înregistrarea inițială în evidență:

a) la înregistrarea semnalării, evenimentului ori legitimării în SID Semnalări în cazul în care persoana este vizată în calitate de martor, bănuț, victimă, reprezentant, contravenient, persoana verificată.

Actualizarea datelor: la recepționarea informației suplimentare cu privire la persoanele fizice implicate într-o situație care face obiectul de evidență în cadrul SID Semnalări.

Scoaterea din evidență:

a) în cazul în care se stabilește că datele introduse inițial cu privire la persoana fizică sunt eronate;

b) la transferarea semnalării, evenimentului sau legitimării din statut activ în cel inactiv, adică transferarea informației în baza de date de arhivă.

3) pentru obiectul informațional „persoană juridică”:

Înregistrarea inițială în evidență:

a) la înregistrarea semnalării, evenimentului ori legitimării în SID Semnalări, în cazul în care persoana juridică, este identificată și vizată în legătură cu obiectul de evidență în cadrul SID Semnalări;

b) la înregistrarea altor apeluri la Serviciul național unic pentru apelurile de urgență 112, în cazul în care unul dintre subiecții situației de urgență este o persoană juridică.

Actualizarea datelor se efectuează: la recepționarea informației suplimentare despre persoanele juridice implicate într-o situație de urgență, despre care Serviciul național unic pentru apelurile de urgență 112 a fost înștiințat anterior.

Scoaterea din evidență se efectuează:

a) la corectarea datelor introduse anterior privind persoana juridică, în cazul stabilirii faptului că datele introduse inițial sunt greșite;

b) la transferarea apelului/situației de urgență din statut activ în cel inactiv, cu transferarea informației în baza de date de arhivă a situațiilor de urgență.

4) pentru obiectul informațional „document”:

Înregistrarea inițială în evidență:

- a) la ținerea evidenței documentelor din SID Semnalări;
- b) la ținerea evidenței regulamentelor și instrucțiunilor interne.

Actualizarea datelor:

- a) la introducerea modificărilor într-un document întocmit;
- b) la introducerea modificărilor într-o instrucțiune sau regulament.

Scoaterea din evidență:

- a) la nimicire;
- b) la transmiterea documentului persoanei care l-a solicitat;
- c) la anularea instrucțiunii sau regulamentului.

Eliminarea fizică din baza de date a informației privind toate obiectele informaționale are loc după expirarea termenului de 5 ani de aflare a informației în arhivele electronice ale SID Semnalări.

23. Datele SID Semnalări reprezintă o totalitate a atributelor obiectelor informaționale și includ:

1) semnalarea:

- a) autoritatea din subordinea MAI cu competență de examinare a cazului;
- b) tip și categorie semnalare;
- c) tip eveniment;
- d) locul cazului semnalat;
- e) date despre mijloace de transport implicate (tip transport și vehicul, numărul de înregistrare, detalii);
- f) date despre bunuri implicate (tip bun, numărul, relația cu persoana, descriere, valoarea prejudiciu);
- g) date despre persoane implicate/vizate (calitatea, nume, prenume, data nașterii, datele de contact și adresa de domiciliu, telefon);
- h) date despre caz (clasificare caz, tip caz, gravitate caz, număr de înregistrare după Registrul de evidență a sesizărilor cu privire la infracțiuni nr. 1/Registrul de evidență a altor informații cu privire la infracțiuni și incidente nr. 2, numărul cauzei penale sau procesului contravențional conex);
- i) conexare cu alte semnalări;
- j) datele privind informația suplimentară prezentată la solicitarea serviciilor specializate de urgență;
- o) statutul examinare semnalare.

datele de bază cu privire la rezultatele intervenției:

- a) resursele care au participat la intervenție;
- b) măsuri întreprinse de cercetare a cazului;
- c) decizie adoptată.

Pentru obiectul informațional „semnalarea”, împrumutat nemijlocit în SID Semnalări, se păstrează doar numărul de identificare din Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112 (pentru cazul respectiv). Toate datele suplimentare necesare referitoare la semnalare pot

fi accesate din Sistemul informațional automatizat al Serviciului național unic pentru apelurile de urgență 112, Sistemul informațional automatizat „Registrul informației criminalistice și criminologice” și Sistemului informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții.

2) date referitoare la persoana fizică:

- a) datele generale: nume, prenume, data nașterii, telefon, adresa;
- b) numărul de identificare (IDNP);
- c) categoria persoanei (apelant, victimă, martor, membru al echipajului de intervenție, persoană cu dizabilități);
- d) informațiile suplimentare despre starea fizică sau psihică a persoanei fizice;
- e) statutul.

3) date referitoare la persoana juridică:

- a) numărul de identificare (IDNO);
- b) categoria persoanei (parte vătămată, parte implicată, solicitant, apelant);
- c) informațiile suplimentare despre persoana juridică (de ex. datele de contact ale persoanelor responsabile);
- d) statutul.

4) documente:

- a) numărul de identificare al documentului;
- b) tipul documentului;
- c) seria;
- d) numărul;
- e) data eliberării;
- f) de către cine a fost eliberat/executat;
- g) statutul documentului.

Pentru obiectele informaționale „persoană fizică” și „persoană juridică”, împrumutate nemijlocit în SID Semnalări, se păstrează doar numerele de identificare de stat (IDNP sau IDNO, respectiv). Toate datele suplimentare necesare referitoare la persoanele fizice și unitățile de drept pot fi accesate din Registrul de stat al populației sau Registrul de stat al unităților de drept.

24. În vederea asigurării veridicității și reducerii volumului informației păstrate în SID Semnalări, precum și pentru o clasificare corectă a obiectelor în acesta, se utilizează sistemul de clasificatoare elaborate în baza clasificatoarelor naționale:

- 1) clasificatoarele internaționale;
- 2) clasificatoarele naționale;
- 3) clasificatoarele intrasistemice, elaborate în baza clasificatoarelor internaționale și a clasificatoarelor naționale.

Clasificatoarele intrasistemice se elaborează și se utilizează în cadrul SID Semnalări doar în cazurile absenței clasificatoarelor naționale și internaționale aprobate.

25. SID Semnalări interacționează cu următoarele sisteme informaționale automatizate:

- 1) Sistemul informațional automatizat „Registrul de stat al populației”;
- 2) Sistemul informațional automatizat „Registrul de stat al unităților de drept”;
- 3) Sistemul informațional automatizat „Registrul de stat al transporturilor”;
- 4) Sistemul informațional automatizat „Registrul de stat al conducătorilor de vehicule”;
- 5) Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”;
- 6) Sistemului informațional automatizat de evidență a contravențiilor, a cauzelor contravenționale și a persoanelor care au săvârșit contravenții;
- 7) Sistemului informațional automatizat al Serviciului național unic pentru apelurile de urgență 112;
- 8) Sistemul informațional automatizat „Registrul accidentelor rutiere”;
- 9) Sistemul automatizat de supraveghere a circulației rutiere „Controlul traficului”;
- 10) Sistemul informațional automatizat „Registrul de stat al unităților administrativ-teritoriale și al străzilor din localitățile de pe teritoriul Republicii Moldova”.

26. SID Semnalări 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 și control al accesului (MPass) – pentru autentificarea și controlul accesului în cadrul sistemului;
- 4) serviciul electronic guvernamental de jurnalizare (MLog) – pentru asigurarea evidenței operațiunilor (evenimentelor) produse în cadrul SID Semnalări;
- 5) serviciul electronic guvernamental de notificare (MNotify) – pentru notificarea registratorilor.

Datele recepționate din celelalte registre sunt utilizate în scopul documentării corecte și exhaustive a contravențiilor, infracțiunilor, a cauzelor penale și a persoanelor care au săvârșit infracțiuni sau contravenții, acordării

asistenței informaționale organelor de urmărire penală și agenților constatatori în soluționarea cauzelor până la întocmirea procesului-verbal cu privire la contravenției și/sau adoptarea deciziei de pornire a cauzei penale, colectării centralizate a datelor aferente cazului, evenimentelor cu risc pentru ordine și securitate publică, legitimărilor cetățenilor și/sau controlului mijloacelor de transport.

Capitolul VII

INFRASTRUCTURA INFORMAȚIONALĂ DE COMUNICAȚII ELECTRONICE

27. Nivelurile de infrastructură.

SID Semnalări va fi găzduit pe platforma tehnologică comună (MCloud).

28. Complexul software.

Lista produselor software utilizate la crearea infrastructurii informaționale și de comunicații electronice a SID Semnalări este determinată de către Serviciul Tehnologii Informaționale din subordinea MAI.

Capitolul VIII

SPAȚIUL TEHNOLOGIC AL SID SEMNALĂRI

29. La dezvoltarea SID Semnalări se aplică arhitectura multinivel (având cel puțin următoarele nivele - baza de date, logica de aplicație și interfața cu utilizatorul) și principiile agile. Utilizarea unei astfel de arhitecturi și principii permite o cuplare redusă între componente, în care responsabilitățile fiecărei componente sunt specializate, precum și implementarea interactivă, operarea modificărilor și flexibilitate în implementare.

30. SID Semnalări utilizează standarde deschise și este compatibil cu sisteme care, la fel, utilizează standarde non-proprietare, cât și cu standardele deja existente.

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

1) implementarea unei soluții bazate pe SOA (Service Oriented Architecture – 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 restabilire a datelor, în caz de incidente.

32. SID Semnalări poate fi ușor 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.

33. 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.

34. Interfața de utilizare a SID Semnalări se adaptează automat la diverse rezoluții de afișare și este disponibilă cel puțin în limba de stat.

35. Interfața de utilizare a SID Semnalări este implementată, folosind tehnologii care asigură funcționarea serviciului pe dispozitivele mobile.

36. Având în vedere locul SID Semnalări în cadrul resurselor informaționale departamentale ale MAI, este necesară 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

SECURITATEA ȘI PROTECȚIA SID SEMNALĂRI

37. Securitatea SID Semnalări presupune starea de protecție a resurselor 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.

38. 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 SID Semnalări 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 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.

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

39. Pentru asigurarea edificării sistemului eficient de asigurare a securității informaționale ale obiectelor SID Semnalări 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) în baza gestionării riscurilor de securitate a informației, determinarea cerințelor tehnice și organizatorice, 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.

Sarcinile de bază ale asigurării securității informaționale sunt:

1) asigurarea confidențialității informației, prevenirea accesului la informație fără drepturi și împuterniciri corespunzătoare;

2) asigurarea integrității logice a informației, prevenirea introducerii, actualizării și nimicirii neautorizate a informației;

3) asigurarea integrității fizice a informației;

4) asigurarea protecției infrastructurii informaționale împotriva deteriorării și tentativelor de modificare a funcționării.

Mecanismele de bază ale asigurării securității informaționale sunt:

1) autentificarea și autorizarea;

2) controlul accesului;

3) înregistrarea acțiunilor și auditul;

4) criptarea informației;

5) analiza și modelarea fluxurilor informaționale;

6) monitorizarea rețelelor;

7) detectarea și prevenirea intruziunilor;

8) prevenirea scurgerii informației confidențiale;

9) analizatori de protocoale;

10) mijloacele de programare antivirus;

11) ecrane între rețele (firewall);

12) sistemele copierii de rezervă;

13) sistemele de alimentare fără întrerupere cu energie electrică;

14) organizarea pazei, securității;

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

16) mijloacele de analiză a sistemelor de protecție;

17) alte mecanisme.

Utilizarea mecanismelor de asigurare a securității informaționale se planifică la etapa de proiectare a sistemelor și infrastructurii informaționale.

Una dintre cele mai vulnerabile verigi ale sistemului securității informaționale o constituie factorul uman și respectarea procedurilor stabilite.

Un element important al securității informaționale se consideră instruirea personalului privind metodele și procedeele de asigurare a securității informaționale.

40. Organizarea sistemului de protecție a datelor cu caracter personal constituie o parte componentă a mecanismului de asigurare a securității informaționale a SID Semnalări.

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.

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 SID Semnalări este posibilă doar în cazurile stabilite de legislația națională pe domeniul de competență al MAI, autorităților administrative și instituțiilor din subordinea acestuia.

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 menținerea acestor informații pentru o perioadă de timp.

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.

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 stabilite de legislația națională în domeniu.

NOTA INFORMATIVĂ

la proiectul hotărârii Guvernului cu privire la aprobarea Conceptului tehnic al Sistemului informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică” al Ministerului Afacerilor Interne

1. Autorul proiectului

Proiectul hotărârii Guvernului cu privire la aprobarea Conceptului tehnic al Sistemului informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică”, a fost elaborat de către Ministerul Afacerilor Interne (*în continuare – MAI*).

2. Condițiile ce au impus elaborarea proiectului de act normativ și finalitățile urmărite

Necesitatea elaborării Proiectului hotărârii Guvernului cu privire la aprobarea Conceptului tehnic al Sistemului informațional departamental „Evidența semnalărilor și evenimentelor de ordine publică” (*în continuare – SID Semnalări*) rezultă din Planul de acțiuni al Guvernului pentru anii 2021-2022, aprobat prin Hotărârea Guvernului nr. 235/2021 (*compartimentul XXIV Afaceri interne, Obiectivul 24.4. E-transformarea proceselor, operațiunilor și activităților interne ale Ministerului Afacerilor Interne, acțiunea 24.4.6. Elaborarea proiectului de hotărâre a Guvernului cu privire la aprobarea Conceptului tehnic al Sistemului informațional automatizat „Evidența semnalărilor și evenimentelor”*).

Subsidiar această activitate se aliniază la implementarea recomandărilor Curții de Conturi conform HCC nr. 82 din 28.12.2020, înaintate în rezultatul efectuării auditului performanței „În ce mod activitățile realizate pentru crearea/elaborarea, implementarea și gestionarea sistemelor informaționale în sectorul public contribuie la utilizarea eficientă a resurselor alocate în acest scop?”, prin care s-a solicitat Ministerului, pe domeniul de competență, să revadă, după caz, să elaboreze, să ajusteze/consolideze și să înainteze spre aprobare cadrul normativ (concept, regulament) pentru reglementarea creării și funcționării resurselor și sistemelor informaționale din posesie/gestiune (subpct. 3.2.7).

Scopul proiectului constă în instituirea Registrului departamental pentru automatizarea proceselor operaționale realizate de instituțiile și organizațiile din subordinea Ministerului, beneficiari de bază fiind:

- Inspectoratul General al Poliției (IGP);
- Inspectoratul General de Carabinieri (IGC);
- Serviciul protecție internă și anticorupție (SPIA);
- Inspectoratul de Management Operațional (IMO);

Subsidiar, în calitate de beneficiari secundari pot apărea și alte instituții și organizații din subordinea Ministerului, și anume:

- Biroul Migrație și Azil (BMA);
- Inspectoratul General pentru Situații de Urgență (IGSU);
- Inspectoratul General al Poliției de Frontieră (IGPF);

Proiectul realizat de către MAI este orientat la implementarea unui sistem informatic integrat, obiectivele de bază ale căruia sunt:

1. Înregistrarea într-un registru unic, în format electronic, a tuturor semnalărilor

primite de subdiviziunile din cadrul MAI, indiferent de tipul semnalării (urgente sau non-urgente) și de sursa informației;

2. Înregistrarea informațiilor importante cu privire la situațiile de interes pentru MAI (evenimente) în vederea gestionării lor ulterioare;

3. Gestionarea evenimentelor și înregistrarea măsurilor preliminare planificate și derulate;

4. Furnizarea informațiilor în format structurat unitar pentru toate categoriile de fapte (cu caracter penal, contravențional sau abateri disciplinare).

Totodată, implementarea sistemului informațional în cauză contribuie la realizarea unor obiective specifice instituționale, cum ar fi:

- Crearea suportului informatic unitar pentru gestionarea într-o formă consolidată a necesarului de date și informații pentru fundamentarea deciziei pe timpul desfășurării activităților de planificare, coordonare și conducere a acțiunilor specifice la nivelul tuturor structurilor de ordine publică din subordinea Ministerului;

- Implementarea unui sistem modern de management al datelor și al ciclului lor de viață, cu posibilitatea înregistrării și afișării on-line în dinamica evoluției situației operative, inclusiv a detaliilor descriptive ale evenimentelor, precum și, după caz, a informațiilor de reprezentare geospațială a acestora.

- Proiectarea și implementarea unor metode avansate de analiză strategică, operațională și tactică a evenimentelor desfășurate în spațiul public cu incidență în planul ordinii publice și a fenomenului infracțional, pe baza intercorelării între incidentele înregistrate în baza de date națională, inclusiv prin folosirea unor instrumente inovatoare de analiză utilizând criterii geospațiale.

- Realizarea schimbului de informații în timp real pe timpul derulării evenimentelor, transmiterea operativă a dispozițiilor pentru adaptarea dispozitivelor funcție de evoluția situației operative și înregistrarea cronologică a acestora.

- Asigurarea interoperabilității la nivel organizațional și a integrării la nivel tehnic între structurile de ordine publică, precum și cu alte structuri cu competențe în domeniu care au implementate / sau care au în curs de implementare sisteme similare, în vederea schimbului informațional privind evenimentele de ordine publică, pentru relaționarea datelor disponibile în vederea elaborării unor analize statistice și a unor analize previzionale cu privire la evoluția situației operative pe genuri de fapte și făptuitori și în funcție de distribuția geospațială a acestora.

Este important de menționat că, proiectul propune și o nouă abordare în ceea ce privește instituirea platformei informatice instituționale ce va integra informații prin care conducerea ministerului și celelalte structuri ale MAI cu competențe în gestionarea evenimentelor din domeniul de competență, vor beneficia de:

- posibilitatea informării în timp real despre evenimentele/incidentele înregistrate la nivelul fiecărei structuri;

- crearea unei baze de date la nivel central al MAI cu privire la evoluția situației infracționale și a modului de desfășurare a unor evenimente;

- realizarea automată a unor hărți GIS privind distribuția evenimentelor/incidentelor pe un anumit areal geografic;

- implementarea unor instrumente de analiză și evaluare care să permită realizarea operativă a unor sinteze și rapoarte necesare fundamentării deciziei;

- elaborarea unor rapoarte predefinite periodice cu privire la evoluția evenimentelor sau a activităților în dinamica lor;
- planificarea judicioasă a resurselor umane și materiale în procesul de planificare a misiunilor și implicit pe timpul derulării acestora;
- simplificarea procesului de jurnalizare a datelor și informațiilor transmise pe timpul desfășurării misiunilor;
- crearea unui mecanism flexibil pentru înregistrarea, stocarea și arhivarea datelor și informațiilor, atât în ceea ce privește raportarea evenimentelor cât și a documentelor aferente procesului de planificare și management al acțiunilor

Necesitatea elaborării proiectului dat, rezidă și din prevederile Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, Legii nr. 71/2007 cu privire la registre și Hotărârea Guvernului nr. 562/2006 cu privire la crearea sistemelor și resurselor informaționale automatizate de stat, care stipulează că, Guvernul aprobă concepția creării sistemului informațional național și a resurselor informaționale de stat și în scopul formării spațiului informațional unic al autorităților administrației publice centrale și locale, procesului de creare a sistemelor și resurselor informaționale automatizate de stat se va realiza pe baza unei hotărâri de Guvern, indiferent de sursele de finanțare.

Finalitatea urmărită prin aprobarea proiectului în cauză este realizarea prevederilor legale prin aprobarea actelor normative necesare funcționării unui sistem informațional departamental național.

3. Descrierea gradului de compatibilitate pentru proiecte care au ca scop armonizarea legislației naționale cu legislația Uniunii Europene

Proiectul nu conține norme de armonizare a legislației naționale cu legislația Uniunii Europene.

4. Principalele prevederi ale proiectului și evidențierea elementelor noi

Pornind de la dispozițiile Legii nr. 71/2007 cu privire la registre și ale Legii nr. 467/2003 cu privire la informatizare și la resursele informaționale de stat, proiectul prevede instituirea SID Semnalări al MAI și aprobarea acestuia.

Calitatea de posesor al SIA Semnalări va fi deținută de către MAI. Calitatea de deținător și administrator tehnic îi va reveni Serviciului Tehnologii Informaționale de comun cu Serviciul Tehnologii Informației și Securitate Cibernetică.

Autoritățile și instituțiile din subordinea Ministerului, care, în limitele competențelor atribuite în conformitate cu actele normative, realizează activități de combatere a criminalității și corupției prin utilizarea informației operative și veridice despre infracțiuni, cauze penale, precum și despre persoanele care au săvârșit infracțiuni și alte obiecte supuse evidenței, urmează să utilizeze SID Semnalări pentru colectarea, acumularea, actualizarea, păstrarea, prelucrarea și transmiterea informațiilor cu caracter criminal, contravențional sau infracțional, inclusiv privind situații de urgență..

În Conceptul SID Semnalări au fost descrise următoarele:

- cadrul normativ care a stat la baza elaborării acestuia;
- spațiul funcțional al Registrului;
- structura organizațională a Registrului (inclusiv subiecții acestuia);
- documentele Registrului;
- spațiul informațional (obiectele informaționale, scenariile de bază aferente

<p>obiectelor informaționale, interacțiunea cu alte sisteme informaționale și platforme electronice guvernamentale);</p> <ul style="list-style-type: none"> - spațiul tehnologic al sistemului (infrastructura informațională de comunicații electronice); - asigurarea securității informaționale. <p>Reieșind din cele enunțate, concluzionăm că, aprobarea actului normativ în proiect va oferi posibilitatea de a asigura o abordare de integrare a tuturor datelor într-o bază de date logic unică și a tuturor fluxurilor operaționale într-un sistem informațional unificat logic, toate acestea fiind realizate la nivel instituțional/departamental.</p>
<p>5. Fundamentarea economico-financiară</p> <p>Aprobarea prezentului proiect de Hotărâre de Guvern nu implică la moment cheltuieli financiare suplimentare. Sistemul informațional este creat, dezvoltat și implementat în baza contractului nr. 155/AP dintre Ministerul Afacerilor Interne și compania „Bass systems” SRL, încheiat la data de 08 decembrie 2016 în contextul realizării proiectului „Automatizarea Business Proceselor Cheie MAI și soluții IT&C (Etapa II)”.</p> <p>Aprobarea cadrului de reglementare respectiv este condiția de operaționalizare a sistemului informațional în cauză și punere a acestuia în aplicare.</p>
<p>6. Modul de încorporare a actului în cadrul normativ în vigoare</p> <p>Prezentul proiect de Hotărâre de Guvern nu necesită după sine modificarea altor acte normative în vigoare și se încadrează perfect în cadrul normativ actual.</p>
<p>7. Avizarea și consultarea publică a proiectului</p> <p>În scopul respectării prevederilor Legii nr. 239/2008 privind transparența în procesul decizional, proiectul a fost plasat pe pagina oficială a Ministerului Afacerilor Interne www.mai.gov.md, directoriul „Transparența”, rubrica „Consultări publice”.</p> <p>De asemenea, proiectul a fost înregistrat de către Cancelaria de Stat cu numărul unic 188/MAI/2021 și supus avizării de către toate autoritățile și instituțiile a căror avizare este necesară (inclusiv Agenția Guvernare Electronică, Centrul Național pentru Protecția Datelor cu Caracter Personal și Serviciul Tehnologie Informației și Securitate Cibernetică). Propunerile și obiecțiile au fost luate în considerație și operate ajustările corespunzătoare. Informația detaliată a fost reflectată în sintezele obiecțiilor și propunerilor/recomandărilor, care se anexează.</p>
<p>8. Constatările expertizei anticorupție</p> <p>A fost asigurată, transmiterea proiectului, către Centrul Național Anticorupție, în vederea efectuării expertizei anticorupție. Conform avizului Centrului Național Anticorupție proiectul menționat mai sus nu este supus expertizei anticorupție.</p>
<p>9. Constatările expertizei de compatibilitate</p> <p>Proiectul de Hotărâre de Guvern nu are drept scop armonizarea legislației naționale cu legislația Uniunii Europene, drept urmare nu a fost supus expertizei de compatibilitate.</p>
<p>10. Constatările expertizei juridice</p> <p>Proiectul a fost supus expertizei juridice, de către Ministerul Justiției, fiind ajustat conform obiecțiilor înaintate.</p>