Aprobat prin
Hotărârea Guvernului nr. ___
din_____ 2018

CONCEPȚIA TEHNICĂ
a Sistemului informațional automatizat de informare și comunicare privind prevenirea şi combaterea spălării banilor

CAPITOLUL I

INFORMAŢII GENERALE

Concepția tehnică a Sistemului informațional automatizat de informare și comunicare privind prevenirea și combaterea spălării banilor (în continuare „Concepție") stabilește cerințele de bază ale sistemului informațional automatizat de informare și comunicare privind prevenirea și combaterea spălării banilor (în continuare - *SIA ICCSB*), cum ar fi destinația și scopul creării sale, funcțiile de bază și circuitele funcționale, documentele principale, obiecte informaţionale şi datele sistemului, identificatorii entității de informare de bază, scenariile de bază, inclusiv procesele de informare de bază, descrierea conceptuală a infrastructurii informațional-tehnologice, amenințările la adresa securității informațiilor și cerințele privind securitatea și protecția datelor. Această concepție a fost dezvoltată în conformitate cu Regulamentul tehnic RT 38370656-002: 2006 „Procesele ciclului de viață al software-ului", aprobat prin Ordinul Ministerului Dezvoltării Informaționale nr. 78 din 1 iunie 2006.

1. Dispoziții generale

SIA ICCSB, reprezintă un sistem informațional automatizat de informare și comunicare al Serviciului Prevenirea și Combaterea Spălării Banilor, ce include date sistematizate privind activitățile și tranzacțiile suspecte în ceea ce privește spălarea banilor, infracțiunile ce vizează acest domeniu și finanțarea terorismului, precum și alte informații relevante colectate de Serviciul prevenirea şi combaterea spălării banilor în conformitate cu prevederile Legii nr. 308 din 22 decembrie 2017 Cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

2. Definiții

În sensul prezentului concept, noțiunile și termenii utilizați înseamnă următoarele:

analiza bazată pe risc - o componentă tehnologică a SIA ICCSB, care permite obținerea informațiilor cu risc sporit conform criteriilor stabilite în momentul apariției, identificării sau primirii acestora;

solicitare/răspuns EGMONT - totalitatea acțiunilor efectuate în vederea schimbului rapid de informații operative cu serviciile similare din statele-membre a Grupului Egmont, utilizând canalul securizat de comunicare al Grupului Egmont;

EGMONT - Grupul Egmont este organizaţia internaţională a Unităţilor de Informaţii Financiare (FIU), având ca scop îmbunătăţirea interacţiunii între FIU-uri în domeniul comunicaţiilor, al schimbului de informaţii şi al coordonării activităţilor de instruire;

entități raportoare - persoane fizice și juridice obligate în conformitate cu prevederile Legii nr. 308 din 22 decembrie 2017 Cu privire la prevenirea și combaterea spălării banilor și a finanțării terorismului să furnizeze informații SIA ICCSB în scopul prevenirii spălării banilor;

resursă analitică de informare - totalitatea informațiilor colectate și prelucrate de Serviciul Prevenirea şi Combaterea Spălării Banilor stocate în bazele de date SIA ICCSB;

formular special - totalitatea informațiilor structurate destinate informării Serviciul Prevenirea şi Combaterea Spălării Banilor cu privire la bunurile suspecte, activităţile sau tranzacţiile suspecte de spălare a banilor, de infracţiuni asociate acestora şi de finanţare a terorismului.

3. Destinația SIA ICCSB.

SIA ICCSB are ca scop colectarea, verificarea și analizarea informațiilor privind relațiile financiare și economice ale persoanelor fizice și juridice care pot fi legate de activitatea de spălare a banilor, infracțiunile asociate acestora şi de acţiunile de finanţare a terorismului, activităţi ce ţin de identificarea, stabilirea sursei şi urmărirea bunurilor utilizate, obţinute din aceste infracţiuni, a fondurilor teroriştilor şi a altor bunuri care sînt sau pot fi obiect al măsurilor asigurătorii şi/sau al confiscării, precum şi activităţilor de investigare financiară.

4. Scopurile și obiectivele SIA ICCSB

1) Scopurile SIA ICCSB:
   a) colectarea și procesarea promptă a informațiilor necesare privind relațiile financiare și economice în scopul prevenirii și combaterii spălării banilor și finanțării terorismului;
   b) crearea unei resurse analitico-informaţionale departamentale a Serviciului Prevenirea și Combaterea Spălării Banilor;
   c) organizarea unei colaborări eficiente și a schimbului de informații între Serviciul Prevenirea și Combaterea Spălării Banilor, entitățile raportoare, organele cu funcții de

supraveghere a entităților raportoare, organele de drept, judiciare și alte autorități competente la nivel național și internațional;

d) organizarea evidenței analitice și statistice, analiza informațiilor și evaluarea riscurilor de spălare a banilor și de finanțare a terorismului.

2) Obiectivele SIA ICCSB:

a) asigurarea recepționării, înregistrării și prelucrării informațiilor necesare privind prevenirea și combaterea spălării banilor și finanțării terorismului;

b) asigurarea procesului de acumulare și actualizare permanentă a datelor statistice sub forma unei versiuni consolidate, care va include cel puțin:

- date care măsoară amploarea și importanța diferitor sectoare, reglementate de Legea nr. 308 din 22 decembrie 2017 Cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului, inclusiv numărul de entități și persoane, precum și date privind semnificația economică a fiecărui sector;
- date de măsurare a dimensiunii şi a importanţei diferitor sectoare care intră în domeniul de aplicare al prezentei legi, inclusiv numărul de entităţi şi persoane, precum şi date privind importanţa economică a fiecărui sector;
- date de măsurare a etapelor de raportare, de investigare, de urmărire penală, precum şi a celor judiciare ale regimului naţional de combatere a spălării banilor şi a finanţării terorismului, inclusiv numărul de rapoarte privind tranzacţiile suspecte, acţiunile întreprinse ca urmare a rapoartelor respective şi, anual, date privind numărul de cazuri investigate, numărul de persoane urmărite penal, numărul de persoane condamnate pentru infracţiuni de spălare a banilor sau de finanţare a terorismului, tipul de infracţiuni asociate spălării banilor, precum şi valoarea în lei a bunurilor sistate, sechestrate sau confiscate;
- date privind numărul de solicitări transfrontaliere de informaţii care au fost efectuate, primite, respinse ori parţial sau complet soluţionate.

c) asigurarea schimbului de informații transfrontalier, colectarea și analiza informațiilor primite;

d) asigurarea schimbului de date cu sistemele și resursele informaționale de stat, departamentale și teritoriale, în special cu Registrul de stat al populației, Registrul de stat al persoanelor juridice, Registrul de stat al conducătorilor auto, Registrul de stat al transportului, Sistemul informațional geografic național, inclusiv „Cadastrul bunurilor imobiliare”, Sistemul informațional integrat vamal, Sistemul informațional al Serviciului fiscal de stat, Sistemul informațional integrat al Poliției de Frontieră, Sistemul informațional automatizat „Registrul informației criminalistice și criminologice”.e)

asigurarea schimbului de date cu entitățile raportoare, colectarea și analizarea informațiilor primite;

e) asigurarea colectării, stocării și arhivării tuturor informațiilor documentate și a altor informații primite de SIA ICCSB pentru o perioadă de cel puțin zece ani.

f) asigurarea accesului prompt, continuu și calitativ la informațiile analitice acumulate, oferirea informațiilor autorităţilor interesate în conformitate cu legislația în vigoare și competența acestora;

g) asigurarea securității informațiilor și protecția datelor cu caracter personal în procesul de formare și exploatare a resurselor informaționale privind prevenirea și combaterea spălării banilor, asigurarea evidenței și controlul accesului la informațiile primite, colectate și informațiile analitice, precum și la orice alte resurse SIA ICCSB.

5. Principiile de creare a SIA ICCSB

SIA ICCSB se bazează pe următoarele principii:

1) *coerență* - elaborarea pe etape și implementarea proiectului;
2) *extensibilitate și scalabilitate* - posibilitatea extinderii și modernizării ca urmare a creșterii numărului de servicii furnizate și a acțiunilor întreprinse;
3) *productivitate* - asigurarea nivelului necesar de productivitate și eficiență a Sistemului;
4) *siguranța și erorile admisibile* - asigurarea și garantarea unui sistem sigur;5) *arhitectura deschisă* - integrarea simplă nu doar la nivel național, dar și la nivel internațional;
5) *transparență* - proiectarea și implementarea conform principiului modular, folosind standarde în domeniul tehnologiilor informației și telecomunicațiilor;
6) *gestionare centralizată* - asigurarea gestionării și controlului conform listei dedicate de adrese IP;
7) *legalitatea* - crearea și exploatarea SIA ICCSB în conformitate cu legislația în vigoare a Republicii Moldova;
8) *protecția datelor cu caracter personal* - prelucrarea datelor cu caracter personal în conformitate cu cerințele actelor normative existente;
9) *identificator unic al entităților raportoare* - utilizarea numărului de identificare SIA ICCSB atribuite fiecărei entități raportoare;
10) *securitatea datelor* - asigurarea integrității și confidențialității informațiilor, disponibilitatea resurselor și a serviciilor de informare;
11) *utilizarea produselor, programelor și metodelor certificate şi licențiate;*
12) *auditul sistemului* - înregistrarea informației despre schimbările care au loc, pentru a face posibilă reconstituirea istoriei unui document sau starea lui la o etapă anterioară.

Capitolul II

BAZA DE REGLEMENTARE A SIA ICCSB

6. Acte normative care reglementează crearea și activitatea SIA ICCSB:

1) Constituția Republicii Moldova din 29 iulie 1994;
2) Legea nr. 171-XIII din 6 iulie 1994 cu privire la secretul comercial;
3) Legea nr. 308 din 22 decembrie 2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

7. Acte normative de bază în domeniul informatizării

1) Legea nr. 982-XIV din 11 mai 2000 cu privire la accesul la informații;
2) Legea nr. 1069-XIV din 22 iunie 2000 cu privire la informatică;
3) Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare și la resursele informaționale de stat;
4) Legea nr. 71-XVI din 22 martie 2007 cu privire la registre;
5) Legea nr. 241-XVI din 15 noiembrie 2007 cu privire la comunicațiile electronice;
6) Legea nr. 133 din 8 iulie 2011 cu privire la protecția datelor cu caracter personal;
7) Legea nr. 91 din 29 mai 2014 cu privire la semnătura electronică și documentul electronic;
8) Legea nr. 142 din 19 iulie 2018 cu privire la schimbul de date și interopabilitate;
9) Hotărârea Guvernului nr.735 din 11 iunie 2002 „Cu privire la sistemele speciale de telecomunicații ale Republicii Moldova”;
10) Hotărârea Guvernului nr. 1123 din 14 decembrie 2010 „Cu privire la aprobarea Cerințelor față de asigurarea securității datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaționale de date cu caracter personal”;
11) Hotărârea Guvernului nr. 656 din 5 septembrie 2012 „Cu privire la aprobarea Programului-cadru de interoperabilitate”;
12) Hotărârea Guvernului nr. 857 din 31 octombrie 2013 „Cu privire la Strategia națională de dezvoltare a societății informaționale” Moldova Digitală 2020”;
13) Hotărârea Guvernului nr. 1090 din 31 decembrie 2013 „Cu privire la Serviciul electronic guvernamental de autentificare și control al accesului (MPass)”;
14) Hotărârea Guvernului nr. 404 din 2 iunie 2014 „Cu privire la pilotarea platformei de interoperabilitate”;
15) Hotărârea Guvernului nr. 405 din 2 iunie 2014 „Cu privire la serviciul electronic guvernamental integrat de semnătură electronică (MSign)”;

16) Hotărârea Guvernului nr. 708 din 28 august 2014 „Cu privire la serviciul electronic guvernamental de jurnalizare (MLog)”;
17) Hotărîrea Guvernului nr. 128 din 22 februarie 2014 privind platforma tehnologică guvernamentală comună (MCloud);
18) Hotărîrea Guvernului nr.201 din 28 martie 2017 privind aprobarea Cerințelor minime obligatorii de securitate cibernetică;
19) Hotărârea Guvernului nr. 414 din 08 mai 2018 „Cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat”.

8. Regulamente și standarde tehnice în domeniul tehnologiei informației și comunicațiilor electronice

1) Regulamentul tehnic RT 38370656-002: 2006 „Procesele ciclului de viață al software-ului” aprobat prin Ordinul Ministerului Dezvoltării Regionale nr. 78 din 1 iunie 2006;
2) SM ISO / CEI 15288 „Sisteme și programe software”.
3) SM ISO / CEI 12207 „Sisteme și programe software. Procesele ciclului de viață al software-ului”;
4) SM ISO / IEC 27002 „Tehnologia informației. Tehnici de siguranță. „Cod de bune practici în managementul securității informațiilor”;
5) SM ISO / IEC 15408-1 „Tehnologia informației. Tehnici de asigurare a securității informației. Criterii de evaluare a securității tehnologiei informației. Partea 1: Introducere și model comun”;
6) SM ISO / CEI 15408-2 „Tehnologia informației. Măsuri de asigurare a securității informației. Criterii de evaluare a securității tehnologiei informației. Partea 2: Cerințe privind securitatea funcțională”;
7) SM ISO / IEC 15408-3 „Tehnologia informației. Măsuri de asigurare a securității informației. Criterii de evaluare a securității tehnologiei informației. Partea 3: Cerințe privind securitatea”.

Capitolul III

FUNCȚIILE SIA ICCSB

9. Funcțiile de bază ale SIA ICCSB

Funcțiile de bază ale SIA ICCSB:

1) formarea unei resurse analitico-informaționale departamentale a Serviciului Prevenirea și Combaterea Spălării Banilor;
2) stabilirea unui sistem de eficient a schimbului de informații între Serviciul Prevenirea și Combaterea Spălării Banilor și entitățile raportoare, organele cu funcții de supraveghere a entităților raportoare, organele de drept, judiciare și alte autorități competente la nivel național și internațional;
3) crearea unui sistem de obținere rapidă a informațiilor necesare pentru prevenirea și combaterea spălării banilor și finanțării terorismului din toate sursele posibile la nivel național și internațional;
4) procesarea promptă a informațiilor privind relațiile financiare și economice necesare prevenirii și combaterii spălării banilor și finanțării terorismului;
5) organizarea circulației documentelor și păstrarea evidenței Serviciului Prevenirea și Spălarea Banilor;
6) organizarea funcționării circuitului analitic și statistic care asigură analiza informațiilor și evaluează riscurile de spălare a banilor și finanțare a terorismului;
7) organizarea suportului informațional și informarea persoanelor și organizațiilor conform competenței lor în legătură cu prevenirea și combaterea spălării banilor;
8) asigurarea securității și protecției informațiilor care se desfășoară la toate etapele de acumulare, stocare și utilizare a resurselor informaționale guvernamentale care se referă la funcționarea SIA ICCSB.
9) asigurarea calității informațiilor prin crearea și menținerea componentelor sistemului de calitate, bazat pe abordarea procedurală.

10. Spațiul funcțional SIA ICCSB

Spațiul funcțional SIA ICCSB reprezintă o totalitate de funcții realizate de subsisteme automatizate și / sau automate separate care interacționează între ele.

În cadrul funcționării SIA ICCSB se realizează următoarele funcții specifice ale sistemului, grupate în circuite funcționale speciale:

1) Circuitul funcțional al interacțiunii informaționale a tuturor componentelor SIA ICCSB este un sistem integrat de control și monitorizare pentru formarea și utilizarea resursei informaționale a Serviciului Prevenirea și Combaterea Spălării Banilor.

Acest circuit include următoarele funcții:

a) asigurarea integrității logice a SIA ICCSB;
b) asigurarea accesului SIA ICCSB;
c) administrarea bazelor de date SIA ICCSB;

d) administrarea subsistemelor contururilor funcționale ale SIA ICCSB;
e) administrarea drepturilor de acces ale utilizatorilor, implementarea mecanismelor de identificare, autentificare și a controlului accesului;
f) asigurarea securității, protecției și păstrării informațiilor în sistem pe baza standardelor internaționale ISO / IEC 27002: 2014 „Tehnologii informaționale. Metode și mijloace de asigurare a securității. Set de norme și reguli de gestionare a securității informației" și ISO / IEC 15408: 2014 „Tehnologii informaționale. Metode și mijloace de asigurare a securității. Criterii de evaluare a securității TI";
g) asigurarea respectării cerințelor SIA ICCSB în ceea ce privește protecția datelor cu caracter personal.

2) Circuitul funcțional „Informarea privind activități sau tranzacții și schimbul de informații cu serviciile competente ale altor țări (jurisdicții) și cu organizațiile internaționale de profil" este un subsistem de interacțiune cu entitățile raportoare și cu organizațiile internaționale de profil și alte organizații competente, și include următoarele funcții::
a) primirea, înregistrarea și procesarea informației parvenite la Serviciul Prevenirea și Combaterea Spălării Banilor, de la entitățile raportoare cu privire la o proprietate dubioasă activității sau tranzacții care sunt suspecte în ceea ce privește spălarea banilor, infracțiunile legate de spălarea banilor și finanțarea terorismului;
b) gestionarea formularelor speciale;
c) gestionarea mecanismului asincron de informare bazat pe evenimente, care permite entităților raportoare să se conecteze la SIA ICCSB și să transmită informațiile necesare în timp real;
d) schimbul de informații între Serviciul prevenirea și combaterea spălării banilor și entitățile raportoare în vederea obținerii datelor sau informațiilor suplimentare necesare;
e) crearea și gestionarea subsistemului de schimb internațional de informații;
f) primirea, înregistrarea și procesarea informației parvenite, la Serviciul Prevenirea și Combaterea Spălării Banilor de la organizațiile internaționale despre activitățile și tranzacțiile suspecte în ceea ce privește spălarea banilor, infracțiunile ce vizează acest domeniu și finanțarea terorismului;
g) furnizarea către organizațiile internaționale a informațiilor privind activitățile și tranzacțiile suspecte în ceea ce privește spălarea banilor, infracțiunile ce vizează acest domeniu și finanțarea terorismului;
h) schimbul de informații între Serviciul Prevenirea și Combaterea Spălării Banilor și organizațiile internaționale pentru a obține informații sau date suplimentare necesare.

3) Circuitul funcțional „asigurarea interacțiunii informaționale cu resursele informaționale guvernamentale, departamentale și teritoriale“ este un subsistem care permite Serviciului Prevenirea și Combaterea Spălării Banilor de a obține de la autoritățile publice informațiile necesare, inclusiv accesul on-line la resursele informaționale, inclusiv informații, ce conțin date cu caracter personal și include următoarele funcții:

a) interacțiunea SIA ICCSB cu resursele informaționale externe indicate la pct. 4, subpct. 2), lit. d) prin intermediul platformei de interoperabilitate (MConnect);

b) crearea și gestionarea mecanismului flexibil de autentificare și de control al accesului utilizatorilor SIA ICCSB în sistemele de informații de stat, utilizând serviciul electronic guvernamental de autentificare și control al accesului (Mpass);

c) asigurarea unui mecanism flexibil și sigur de protocolare și audit, care să garanteze evidența evenimentelor în contextul utilizării sistemelor și resurselor informaționale guvernamentale atât ca mecanisme interne tehnologice SIA ICCSB, cât și cu ajutorul Serviciului electronic guvernamental de protocolare (MLog);

4) Circuitul funcțional „Asigurarea informațională și suportul informativ“ este o resursă analitico-informaţională internă de acumulare şi reactualizare continuă a Serviciului Prevenirea și Combaterea Spălării Banilor, și include următoarele funcții:

a) formarea bazei de date SIA ICCSB cu includerea informației de bază.

Funcțiile de bază în formarea unei baze de date sunt înregistrarea și actualizarea datelor primite de la entităţile raportoare, precum și excluderea obiectelor de informare (schimbarea statutului obiectului):

- evidența primară constă în atribuirea unui cod unic de identificare entității supuse evidenței și introducerea în baza de date a volumului stabilit de date;
- actualizarea datelor. Actualizarea datelor SIA ICCSB înseamnă actualizarea sistematică a bazei de date a sistemului atunci când datele sunt modificate sau completate;

b) formarea bazei de date SIA ICCSB prin adăugarea informațiilor suplimentare.

Funcțiile suplimentare în procesul de formare a bazei de date sunt înregistrarea și actualizarea datelor obținute pe parcursul activității Serviciului prevenirea și combaterea spălării banilor.

5) Circuitul funcțional „Evidența electronică a investigațiilor financiare” presupune un sistem informațional modular de producere care asigură punerea în aplicare și desfășurarea

investigațiilor financiare pentru a stabili sursa de proprietate, suspectă în sensul spălării banilor și finanțării terorismului, și include următoarele funcțiile:

a) evidența și prelucrarea informațiilor primite, a documentelor analitice și a altor documente;
b) formarea, evidenţa și procesarea documentelor administrative interne, informative și analitice, formarea și gestionarea fluxurilor interne de informații;
c) selecția automatizată și automată, inteligentă, bazată pe evenimente, a informațiilor primite și stocate în baza de date și formarea documentelor analitice pe baza acestora;
d) asigurarea activității de informare a angajaților Serviciului în timpul desfășurării investigației financiare, precum și la îndeplinirea altor atribuții de serviciu;
e) pregătirea documentelor informative și analitice de ieșire.

6) Circuitul funcțional „Analitica" reprezintă un sistem informațional modular de producere, care asigură efectuarea analizei informației, inclusiv prelucrarea şi analiza datelor statistice, precum și evaluarea riscurilor de spălare a banilor și finanțare a terorismului și include funcțiile:

a) desfășurarea analizei operaționale - studierea continuă a informațiilor primite, în vederea identificării anumitor cazuri suspecte în ceea ce privește spălarea banilor și finanțarea terorismului, în funcție de tipul și suma primită de la entităţile raportoare, precum și din orice alte surse de informații;
b) asigurarea analizei automatizate, automate, inteligente și bazată pe evenimente a informației primite și stocate în baza de date;
c) desfășurarea unei analize strategice bazate pe evaluarea generală a tendințelor pe termen mediu și lung, precum și a previziunilor și estimărilor destinate să justifice deciziile strategice și de management pentru a preveni și a combate spălarea banilor și finanțarea terorismului;
d) evaluarea riscurilor de spălare a banilor și finanțare a terorismului;
e) desfășurarea analizei materialului statistic și evaluarea eficienței sistemului de prevenire și combatere a spălării banilor și finanțării terorismului.

7) Circuitul funcțional „Supraveghere" este un sistem informațional care asigură următoarele funcții de supraveghere în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului:

a) primirea, prelucrarea și analiza informației cu privire la spălarea banilor și finanțarea terorismului;

b) identificarea informației necesare pentru desfășurarea activității de supraveghere a Serviciului prevenirea și combaterea spălării banilor;
c) pregătirea documentelor necesare legate de activitatea de supraveghere a Serviciului Prevenirea și Combaterea Spălării Banilor, în conformitate cu competențele sale;
d) gestionarea deciziilor de sancționare;
e) gestionarea informației legate de activitatea de supraveghere, informarea autorităţilor de supraveghere.

8) Circuitul funcțional „Notificarea, informarea și transmiterea informației“ reprezintă un sistem informațional modular de producere care asigură pregătirea și transmiterea informației către organizațiile competente interesate, forțele de ordine, entitățile raportoare, precum și organizațiile internaționale competente în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului, precum și altă informație corespunzătoare colectată de Serviciul Prevenirea și Combaterea Spălării Banilor în conformitate cu competențele sale, și include funcțiile:
a) pregătirea și distribuirea, inclusiv într-un mod automatizat și / sau automat, autorităților competente a informației prezentate de entitățile raportoare, privind activitățile și tranzacțiile care sunt suspecte în ceea ce privește infracțiunile de spălare a banilor și finanțării terorismului, precum și altă informație corespunzătoare colectată în conformitate cu Legea nr. 308 din 22 decembrie 2017 privind prevenirea și combaterea spălării banilor și finanțării terorismului;
b) asigurarea informării automatizate și automate a autorităților competente, și a forțelor de ordine imediat după apariția unor suspiciuni justificate de spălare a banilor, de finanțare a terorismului, inclusiv prin transmiterea informațiilor în sistemul informațional al forțelor de ordine sau al altor organizații competente;
c) asigurarea notificării automatizate, precum și automate a entităților raportoare și a organelor cu funcții de supraveghere și alte autorități competente cu privire la aspectele legate de prevenirea și combaterea spălării banilor și finanțării terorismului;
d) furnizarea informației în regim automatizat precum și automat organelor naționale și organelor și instituțiilor altor țări (jurisdicții), precum și organizațiilor internaționale în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

Capitolul IV

STRUCTURA ORGANIZAȚIONALĂ A SIA ICCSB

11. Proprietarul SIA ICCSB

Proprietarul SIA ICCSB este Statul.

12. Posesorul SIA ICCSB

Posesorul SIA ICCSB este Serviciul Prevenirea și Combaterea Spălării Banilor.

13. Deținătorul SIA ICCSB

Deținătorul SIA ICCSB este Serviciul Pentru Prevenirea și Combaterea Spălării Banilor.

Rolul deținătorului reflectă aspectele administrative și tehnice ce se referă la competența Serviciului Prevenirea și Combaterea Spălării Banilor, în conformitate cu Legea nr. 308 din 22 decembrie 2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului. Serviciul este responsabil pentru crearea, funcţionarea neîntreruptă, administrarea, securitatea și dezvoltarea infrastructurii complexă de informare și comunicare a SIA ICCSB.

14. Furnizorii de date către SIA ICCSB

Furnizorii de date către SIA ICCSB sunt:

1) entitățile raportoare - următoarele persoane fizice și juridice:
   a) băncile specificate în Legea nr. 202 din 06 octombrie 2017 privind activitatea băncilor;
   b) unitățile de schimb valutar (altele decît băncile);
   c) societățile de registru, societățile de investiții, Depozitarul central unic, operatorii de piață, operatorii de sistem, asigurătorii (reasigurătorii), intermediarii în asigurări și/sau în reasigurări persoane juridice, Biroul Național al Asigurătorilor de Autovehicule, fondurile nestatale de pensii, organizațiile de microfinanțare, asociațiile de economii și împrumut, asociațiile centrale ale asociațiilor de economii și împrumut;
   d) organizatorii de jocurilor de noroc;
   e) agenții imobiliari;
   f) persoanele fizice și juridice care desfășoară activități cu metale prețioase și pietre prețioase;
   g) avocații, notarii și alți liber-profesioniști, în perioada participării, în numele clientului, la orice tranzacție financiară și imobiliară sau în perioada acordării asistenței pentru planificarea ori efectuarea tranzacțiilor pentru client ce țin, în ambele cazuri, de vînzarea-

cumpărarea imobilelor, donația bunurilor, gestionarea mijloacelor financiare, valorilor mobiliare și altor bunuri ale clientului, deschiderea și gestionarea conturilor bancare, crearea și gestionarea persoanelor juridice, gestionarea bunurilor aflate în administrare fiduciară, precum și de procurarea și vînzarea acestora;

h) locatorii persoane juridice care practică activitate de întreprinzător și transmit, în condițiile contractului de leasing, locatarilor, la solicitarea acestora, pentru o anumită perioadă, dreptul de posesiune și/sau de folosință asupra unui bun ai cărui proprietari sînt, cu sau fără transmiterea dreptului de proprietate asupra bunului la expirarea contractului;
i) societățile de plată, societățile emitente de monedă electronică și furnizorii de servicii poștale care activează în conformitate cu Legea nr. 114 din 18 mai 2012 cu privire la serviciile de plată și moneda electronică;
j) furnizorii de servicii poștale care activează în conformitate cu Legea comunicațiilor poștale nr. 36 din 17 martie 2016;
k) entitățile de audit, persoanele juridice și întreprinderile individuale care prestează servicii de contabilitate;
l) alte persoane fizice și juridice care comercializează bunuri în sumă de cel puțin 200000 de lei sau echivalentul acesteia numai în cazul în care plățile sînt efectuate în numerar, indiferent dacă tranzacția este efectuată printr-o operațiune sau prin mai multe operațiuni care par a avea legătură între ele.

2) Serviciul vamal furnizează informație în conformitate cu Legea privind prevenirea și combaterea spălării banilor și finanțării terorismului Nr. 308 din 22 decembrie 2017;
3) persoanele fizice sau juridice, altele decât cele menționate în alin. 1), pot informa Serviciul Prevenirea și Combaterea Spălării Banilor, despre cazurile de spălare a banilor și finanțării terorismului, devenite cunoscute, utilizând canalele obișnuite de comunicare, precum și canale de comunicare și serviciile oferite de SIA ICCSB;
4) serviciile competente din alte țări (jurisdicții) și organizații internaționale de profil.

15. Destinatarii datelor SIA ICCSB

Destinatarii datelor SIA ICCSB sunt:

1) organele de drept, judiciare și alte autorități competente - primesc informații privind activitățile și tranzacțiile suspectate de spălare de bani, infracțiuni conexe și finanțare a terorismului de la entitățile raportoare, precum și alte informații relevante colectate în conformitate cu prevederile Legii nr. 308 din 22 decembrie 2017 privind prevenirea și combaterea spălării banilor și finanțării terorismului;

2) entitățile raportoare - informații privind modul de raportare și corectitudinea introducerii datelor în sistem
3) autoritățile cu funcții de supraveghere a entităților raportoare și alte autorități competente - cu privire la riscurile asociate spălării banilor și finanțării terorismului, noile tendințe și tipologii de spălare a banilor și finanțării terorismului, stabilite în domeniile de competență ale încălcărilor și lacunelor din actele normative privind prevenirea riscurilor de spălare a banilor și de finanțare a terorismului;
4) autoritățile competente din alte țări (jurisdicții), precum și organizațiile internaționale, în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului în conformitate cu prevederile Legii nr. 308 din 22 decembrie 2017 privind prevenirea și combaterea spălării banilor și finanțării terorismului.

Capitolul VI

RESURSE INFORMAŢIONALE

16. Documente de bază utilizate de SIA ICCSB

1) Documente de bază:

a) documentele de intrare, înregistrate în SIA ICCSB, referitor la activitățile și tranzacțiile suspecte în ceea ce privește spălarea banilor, infracțiunile ce vizează acest domeniu și finanțarea terorismului;
b) materiale și informații documentate privind prevenirea și combaterea spălării banilor și finanțării terorismului;
c) formular special de la entitățile raportoare;
d) referințe analitice;
e) raport privind investigația financiară;
f) cererile adresate autorităților competente, forțelor de ordine și de supraveghere, organizațiilor naționale și entităților raportoare;
g) cererile adresate organizațiilor internaționale;
h) răspunsurile la cererile organizațiilor internaționale;
i) documente ce vizează blocarea tranzacţiilor cu bunuri;
j) solicitări și permisiuni de divulgare și transfer de informații;
k) documente de informare și referință;
l) documente de informare;
m) rapoartele finale;
n) raport de analiză strategică;
o) documente analitice și statistice;

p) documente referitoare la evaluarea riscurilor;
q) documente referitoare la activități de supraveghere;
r) decizii de sancționare;
s) documente și materiale cu caracter informativ emise de către Serviciu.

2) Documente tehnologice de baza ale sistemului:

Categoria documentelor tehnologice stocate în SIA ICCSB include:

a) documente administrative, de reglementare, procedurale și tehnologice;
b) profilurile utilizatorilor;
c) înregistrarea fișierelor - registru cu privire la acțiuni, solicitări și interacțiunea utilizatorilor cu SIA ICCSB;
d) certificate electronice de utilizator și alte informații de documentare a utilizatorilor.

17. Obiectele informaționale de bază ale SIA ICCSB

Obiectele informaționale de bază ale SIA ICCSB sunt:

1) Nota Analitică;
2) Raport Investigație Financiară;
3) Diseminarea de materiale și informații;
4) Răspuns la Diseminarea de materiale și informații;
5) Solicitări către Entități Raportare;
6) Răspuns de la Entități Raportare;
7) Solicitare EGMONT ieșire;
8) Răspuns EGMONT intrare;
9) Solicitare EGMONT intrare;
10) Răspuns EGMONT ieșire;
11) Decizie de sistare;
12) Decizie de anulare a sistării;
13) Solicitare de permisiune de diseminare ieșire;
14) Răspuns Permisiune de diseminare intrare;
15) Solicitare de permisiune de diseminare intrare;
16) Răspuns Permisiune de diseminare ieșire;
17) Informare generală;
18) Raport Final;
19) Raport de inițierea a analizei strategice;
20) Raport supravegherea conformitate;
21) Decizie de sancționare.

18. Identificarea obiectelor informaţionale

În SIA ICCSB se utilizează următorii identificatori ai obiectelor informaţionale:

1) identificatorul obiectului informațional ***„persoană fizică”*** - numărul de identificare de stat al persoanei (IDNP);
2) identificatorul obiectului informațional ***„entitate juridică”*** - numărul de identificare de stat al entității juridice (IDNO) din Registrul de Stat al Persoanelor Juridice și al Întreprinzătorilor Individuali;
3) identificatorul obiectului informațional **„Nota Analitică”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

NAN-AAAA-NNNNN, unde:

NAN - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

4) identificatorul obiectului informațional **„Raport Investigație Financiară”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

RIF-AAAA-NNNNN, unde:

RIF - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

5) identificatorul obiectului informațional **„Diseminarea de materiale și informații”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

DSM-AAAA-NNNNN, unde:

DSM - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

6) identificatorul obiectului informațional **„Răspuns la Diseminarea de materiale și informații”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

DES-AAAA-NNNNN, unde:

DES - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

7) identificatorul obiectului informațional **„Solicitări către Entități Raportoare”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

SER-AAAA-NNNNN, unde:

SER - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

8) identificatorul obiectului informațional „**Răspuns de la Entități Raportoare”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

RER-AAAA-NNNNN, unde:

RER - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

9) identificatorul obiectului informațional **„Solicitare EGMONT ieșire”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

EQO-AAAA-NNNNN, unde

EQO - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

10) identificatorul obiectului informațional **„Răspuns EGMONT intrare)”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

EPI-AAAA-NNNNN, unde

EPI - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

11) identificatorul obiectului informațional **“Solicitare EGMONT intrare”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

EQI-AAAA-NNNNN, unde

EQI - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

12) identificatorul obiectului informațional **„Răspuns EGMONT ieșire”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

EPO-AAAA-NNNNN, unde

EPO - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

13) identificatorul obiectului informațional **„Decizie de sistare”** este un cod unic de identificare generat și atribuit de sistem având următoarea structură:

PPA-AAAA-NNNNN, unde

PPA - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

14) identificatorul obiectului informațional **„Decizia de anulare a sistării”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

PPC-AAAA-NNNNN, unde:

PPC - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

15) identificatorul obiectului informațional **„Solicitare de permisiune de diseminare ieșire”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

DQO-AAAA-NNNNN, unde

DQO - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

16) identificatorul obiectului informațional **„Răspuns Permisiune de diseminare intrare”** - cod unic de identificare generat și atribuit de sistem având următoarea structură:

DPI-AAAA-NNNNN, unde:

DPI - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

17) identificatorul obiectului informațional **„Solicitare adresată Serviciului de prevenire și combatere a spălării banilor pentru permisiunea de a dezvălui și a transmite informații (Solicitare de permisiune de diseminare intrare)”** - unic de identificare generat și atribuit de sistem, având următoarea structură:

DQI-AAAA-NNNNN, unde

DQI - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

18) identificatorul obiectului informațional **”Răspunsul Serviciului pentru prevenirea și combaterea spălării banilor la cererea de permisiune de divulgare și de transfer de informații (Răspuns Permisiune de diseminare ieșire)”** - cod unic de identificare, generat și atribuit de sistem, care are următoarea structură:

DPO-AAAA-ID-NNNNN, unde:

DPO - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

19) identificatorul obiectului informațional **„Informarea autorităților de supraveghere, competente și unitățile de raportare (Informare generală)”** - cod unic de identificare, generat și atribuit de sistem, care are următoarea structură:

IGE-AAAA-NNNNN, unde:

IGE - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

20) identificatorul obiectului informațional **„Raport final (Raport Final)”** - cod unic de identificare, generat și atribuit de sistem, care are următoarea structură:

RFN-AAAA-NNNNN, unde:

RFN - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

21) identificatorul obiectului informațional **”Raport de inițierea a analizei strategice”** - cod unic de identificare, generat și atribuit de sistem, care are următoarea structură:

RAS-AAAA-NNNNN, unde:

RAS - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

22) identificatorul obiectului informațional **„Raport în urma rezultatelor supravegherii (Raport supravegherea conformitate)”** - cod unic de identificare, generat și atribuit de sistem, care are următoarea structură:

RSC-AAAA-NNNNN, unde:

RSC - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă;

23) identificatorul obiectului informațional **„Decizie de sancționare”** - cod unic de identificare, generat și atribuit de sistem, care are următoarea structură:

DES-AAAA-NNNNN, unde:

DES - identificatorul tipului de document;

AAAA - anul în cifre;

NNNNN - numărul consecutiv de ordine al documentului, emis de sistem conform înregistrării la data curentă.

19. Datele SIA ICCSB

Datele SIA ICCSB reprezintă principala sursă de formare a atributelor obiectelor informaționale. Datele SIA ICCSB se formează prin primirea și prelucrarea:

1) informației furnizate de către entitățile raportoare prin intermediul unui formular special:
   a) seria, numărul și data eliberării documentului, actul de identitate de identitate, adresa, datele procurii și alte date necesare pentru a stabili identitatea persoanei care a efectuat o tranzacţie;
   b) numele / prenumele, codul fiscal / numărul de identificare de stat al persoanei fizice, sediul/domiciliul, seria și numărul documentului, actul de identitate, necesare pentru a stabili identitatea persoanei în numele căreia s-a efectuat tranzacţia, precum și datele de contact;

c) date privind identificarea juridică, conturile și jurisdicțiile persoanelor care participă la o activitate sau o tranzacție, inclusiv date privind conturile instituțiilor financiare;
d) tipul de activitate sau tranzacție;
e) adresa IP a clientului pentru tranzacţii la distanță;
f) scopul plății și obiectul contractului;
g) date privind entitatea raportoare care a efectuat o tranzacție;
h) data și ora tranzacției sau perioada de activitate, suma tranzacției;
i) numele și funcția persoanei care a înregistrat activitatea sau tranzacţia;
j) motive de suspiciune;
k) alte date necesare.

2) informației obținute din registrele de stat, instituționale teritoriale, de informare;
3) informației primite de la instituţiile naționale competente, precum și de la autoritățile competente din alte țări (jurisdicții) și organizațiile internaționale specializate;
4) informației primite de la alte surse posibile, în conformitate cu prevederile Legii nr. 308 din 22 decembrie 2017cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului.

20. Scenarii fundamentale

Scenariile fundamentale reprezintă o listă de bază, legate de obiectele informaționale și datele SIA ICCSB, evenimente privind prevenirea spălării banilor și combaterea finanțării terorismului. Scenariile fundamentale sunt împărțite în următoarele grupuri:

1) obținerea de informații de la entitățile raportoare, introducerea și acumularea datelor, actualizarea și radierea obiectelor informaţionale în conformitate cu ciclul de viață al unui formular special;
2) primirea informației de la sistemele guvernamentale și departamentale de informații și registre;
3) primirea informației de la serviciile naționale competente, precum și de la serviciile competente ale altor țări (jurisdicții) și organizațiile internaționale specializate, procesarea documentelor primite;
4) primirea informației din alte surse de informare;
5) proces analitic operațional;
6) procesele de analiză strategică;
7) procesele de supraveghere;
8) pregătirea și furnizarea de informații.

Scenariul A - primirea informației de la entitățile raportoare, introducerea și acumularea datelor, actualizarea și ștergerea obiectelor informaționale în conformitate cu ciclul de viață al unui formular special:

1) Regimul automatizat:
   a) pregătirea unui formular special;
   b) transmiterea unui formular special către entitățile raportoare pentru completarea acestuia;
   c) completarea de către entitățile raportoare a unui formular special și transmiterea lui printr-un canal securizat, în format electronic, în adresa Serviciului Prevenirea și Combaterea Spălării Banilor în conformitate cu procedura stabilită;
   d) verificarea și introducerea datelor în baza de date SIA ICCSB.
2) Regimul automat:
   a) oferirea unui API specializat (interfața software a unei aplicații de integrare specializată sau a subsistemului SIA) entităților raportoare;
   b) integrarea pe partea sistemului de informare și comunicare a entităților raportoare, a interfeței software a unei aplicații de integrare specializate sau a subsistemului SIA;
   c) oferirea informației on-line în regim asincron bazat pe evenimente la momentul apariției în sistemul informațional al entității raportoare a unei informații suspecte;
   d) prelucrarea și introducerea datelor privind tranzacției în baza de date SIA ICCSB.

Scenariul B - primirea informațiilor de la instituțiile publice, departamentele și sistemele teritoriale de informare și registre:

1) obținerea datelor din sistemele informaționale automatizate:
   a) „Registrul de Stat al populației" - oferă acces la datele persoanelor fizice;
   b) „Registrul de Stat al Persoanelor Juridice și al Întreprinzătorilor Individuali", date privind persoanele juridice înregistrate;
   c) „Cadastrul bunurilor imobile" - oferă date privind bunurile imobiliare și drepturile asupra acestora, și de asemenea, evaluarea costului acestor obiecte;
   d) „Sistemul informațional integrat vamal" - informații privind valorile valutare, care sunt declarate de persoane fizice și juridice;
   e) Sistemul informațional al Serviciului Fiscal de Stat;
   f) „Sistemul informațional integrat al Poliției de Frontieră";
   g) alte sisteme informaționale automatizate ale autorităților publice naționale și organelor cu funcții de supraveghere a entităților raportoare - Obținerea informațiilor în conformitate cu prevederile Legii nr. 308 din 22 decembrie 2017 privind prevenirea și combaterea spălării banilor și finanțării terorismului;

Scenariul C - primirea informației de la autoritățile competente din țară, precum și de la autoritățile competente din alte țări (jurisdicții) și organizațiile internaționale specializate, procesarea documentelor primite:

1) primirea informațiilor sub forma documentelor de intrare;
2) introducerea documentelor în sistem;
3) analiza și executarea documentului;
4) verificarea datelor și dacă este necesar, introducerea datelor în baza de date SIA ICCSB.

Scenariu D - primirea informațiilor din alte surse de informații:

1) forma electronică de comunicare cu persoane juridice și persoane fizice pe site-ul oficial al Serviciului Prevenirea și Combaterea Spălării Banilor:
   a) completarea și transmiterea de către persoana juridică sau fizică a formularului de comunicare electronică - formularul de notificare specială, postat pe site-ul oficial al Serviciului Prevenirea și Combaterea Spălării Banilor pentru a transmite informații despre cazurile de spălare a banilor și finanțare a terorismului care le-au devenit cunoscute;
   b) analiza informațiilor primite prin comunicarea electronică;
   c) verificarea datelor și dacă este necesar, introducerea datelor în baza de date SIA ICCSB.

Forma electronică de comunicare cu persoane juridice și persoanele fizice trebuie să prevadă posibilitatea de a transmite informații, inclusiv prin e-mail.

Scenariu E - proces operațional analitic:

1) crearea unei referințe analitice în mod automatizat:
   a) analiza informațiilor acumulate în baza de date SIA ICCSB;
   b) analiza informațiilor furnizate de autoritățile competente din țară, precum și autoritățile competente din alte țări (jurisdicții) și organizațiile internaționale specializate;
   c) analiza informațiilor primite din orice sursă posibilă;
   d) formarea unei referințe analitice, pe baza analizei efectuate și identificarea cazurilor potențiale suspecte în ceea ce privește spălarea banilor și cazurile de finanțare a terorismului;
2) crearea unei referințe analitice în mod automat:
   a) analiza automată a informațiilor, acumulate în baza de date a SIA ICCSB;
   b) analiza automată a informațiilor primite din orice surse posibile;
   c) generarea automată a proiectului de referință analitică pe baza unei analize automatizate și cazurile identificate prin criterii care ar putea fi suspecte în sensul spălării banilor și finanțării terorismului, precum și notificarea angajatului Serviciului Prevenirea și

Combaterea Spălării Banilor, inclusiv în formă electronică (E-mail, SMS, chat, alte canale electronice);

d) Studierea proiectului de raport analitic, ajustarea lui, pregătirea versiunii sale finale;

3) analiza conținutului referinței analitice - se analizează cazurile suspecte separate în sensul spălării banilor și finanțării terorismului;

4) monitorizarea financiară:

a) obținerea de informații suplimentare din baza de date SIA ICCSB;

b) informațiile primite de la registrele şi sistemele informaționale naționale, departamentale și teritoriale;

c) studierea schemelor de tranzacții;

d) arhivarea;

e) întocmirea raportului final;

5) crearea unui raport privind investigația financiară (RIF) și efectuarea unei investigații financiare:

a) obținerea informațiilor suplimentare din baza de date SIA ICCSB;

b) solicitări de la entitățile raportoare;

c) răspunsurile din partea entităților raportoare;

d) informațiile primite de la registrele şi sistemele informaționale naționale, departamentale și teritoriale;

e) cererile și răspunsurile adresate autorităților competente, organizațiilor naționale și persoanelor fizice;

f) solicitări către organizațiile internaționale (Solicitare EGMONT);

g) răspunsurile de la organizațiile internaționale;

h) adoptarea deciziei cu privire la sistarea activității financiare (Decizie de sistare);

i) adoptarea deciziei cu privire la anulare a sistării activității financiare (Decizie de anulare a sistării);

j) solicitarea permisiunii de divulgare și de transfer de informații;

k) obținerea permisiunii de divulgare și de transfer de informații;

l) studierea schemelor de tranzacții;

m) pregătirea raportului final.

Scenariu F - procesele de analiză strategică:

1) crearea unui raport privind inițierea analizei strategice (Raport de inițierea analizei strategice);

2) analiza informațiilor primite și acumulate:

a) obținerea de informații din baza de date SIA ICCSB;
b) solicitări de la entitățile raportoare;
c) răspunsuri de la entități raportoare;
d) obținerea informațiilor de la registrele și sistemele informaționale naționale, departamentale și teritoriale ;
e) efectuarea analizelor strategice, pe baza unei evaluări a imaginii globale a tendințelor pe termen mediu și lung;
f) îndeplinirea previziunilor și efectuarea evaluărilor, destinate fundamentării obiectivelor strategice și a deciziilor manageriale privind prevenirea și combaterea spălării banilor și finanțării terorismului;
g) efectuarea unei evaluări a riscurilor de spălare a banilor și finanțare a terorismului;
h) efectuarea analizei a materialul statistic;
i) efectuarea unei evaluări a eficienței sistemului de prevenire și combatere a spălării banilor și finanțării terorismului;

3) pregătirea documentelor și rapoartelor analitice și statistice.

Scenariu G - procesul de supraveghere:

1) primirea și analizarea informațiilor din baza de date, precum și alte documente a SIA ICCSB;
2) pregătirea în sistem a raportului cu privire la rezultatele supravegherii;
3) luarea deciziei de sancționare, pregătirea în sistem a deciziei de sancționare;
4) informarea autorităților de supraveghere.

Scenariu H - pregătirea și furnizarea de informații;

1) pregătirea și transmiterea informațiilor în regim automatizat:
   a) pregătirea și transmiterea materialelor către autoritățile competente a informațiilor prezentate de către entitățile raportoare despre activitățile și tranzacţiile, suspicioase în sensul spălării banilor, legate de infracțiuni și finanțarea terorismului, precum și alte informații relevante, colectate în conformitate cu Legea nr. 308 din 22 decembrie 2017 cu privire la prevenirea și combaterea spălării banilor și finanțării terorismului;
   b) pregătirea și transmiterea informațiilor către autoritățile competente privind apariția unor suspiciuni justificate de spălare a banilor și/sau finanțarea terorismului;
   c) pregătirea documentelor și notificarea entităților raportoare, organelor cu funcții de supraveghere a entităților raportoare și alte autorități competente în problemele ce țin de prevenirea și combaterea spălării banilor și/sau finanțării terorismului;

d) pregătirea documentelor și transmiterea informațiilor autorităților competente din țară, precum și autorităților competente din alte țări (jurisdicții), precum și organizații internaționale, în domeniul prevenirii și combaterii spălării banilor și/sau finanțării terorismului;

2) pregătirea și transmiterea informațiilor în regim automat:

a) conectarea la sistemele informaționale ale entităților raportoare, organele de drept și alte autorități competente, organizațiile naționale, furnizarea unui API specializat (interfața software a unei aplicații de integrare specializată sau a subsistemului SIA) și transmiterea on-line printr-un protocol convenit, imediat după apariția unor suspiciuni justificate de spălare a banilor, finanțarea terorismului, care necesită primirea și reacționarea imediată;

b) furnizarea informațiilor în regim automat (inclusiv pregătirea și transmiterea informațiilor prin e-mail) aparținând altor țări (jurisdicțiilor) organelor de drept și autorităților competente, precum și organizațiilor internaționale, în domeniul prevenirii și combaterii spălării banilor și finanțării terorismului.

Capitolul VII

INFRASTRUCTURA INFORMAȚIONAL- TEHNOLOGICĂ

21. Nivelurile infrastructurii

SIA ICCSB va fi realizată prin implementarea unui sistem informatic care va fi găzduit pe platforma tehnologică a Serviciului Prevenirea și Combaterea Spălării Banilor, cu păstrarea copiilor de rezervă pe platforma guvernamentală tehnologică comună MCloud.

Componentele principale ale infrastructurii SIA ICCSB sunt:

1) Cloud-ul guvernamental (MCloud);
2) platforma automatizată de informare și comunicare a Serviciului Prevenirea și Combaterea Spălării Banilor;
3) infrastructura bazei de date a resurselor informaționale de stat care acoperă datele sistematice privind activitățile și tranzacțiile, suspecte în sensul spălării banilor, a infracțiunilor conexe și finanțării terorismului, precum și alte informații relevante colectate în conformitate cu prevederile Legii nr. 308 din 22 decembrie 2017 privind prevenirea și combaterea spălării banilor și finanțarea terorismului;
4) rețeaua locală, stațiile de lucru, unitățile computerizate (calculatoare, laptopuri, tablete) ale Serviciului prevenirea și combaterea spălării banilor;
5) sistemele automatizate de informare și comunicare ale unităților raportoare.

Dezvoltarea SIA ICCSB presupune consolidarea și dezvoltarea unei platforme automatizate de informare și comunicare, a unei rețele locale, a stațiilor de lucru, a unităților computerizate (PC-uri, laptop-uri, tablete) ale Serviciului Prevenirea și Combaterea Spălării Banilor.

Accesul la SIA ICCSB se va face conform listei dedicate de adrese IP, folosind certificate electronice de autentificare. Totodată acțiunilor din sistem vor fi confirmate și semnate electronic de către angajații autorizați.

22. Integrarea SIA ICCSB cu alte sisteme informaționale

Infrastructura tehnologică a SIA ICCSB va fi SOA (arhitectură orientată spre servicii), care va permite integrarea SIA cu toate serviciile MCloud și serviciile electronice oferite, cum ar fiMsign, Mpass, MLog și alte servicii electronice cu sistemele informatice ale altor agenții guvernamentale și unitățile de raportare prin intermediul platformei de integrare MConect.

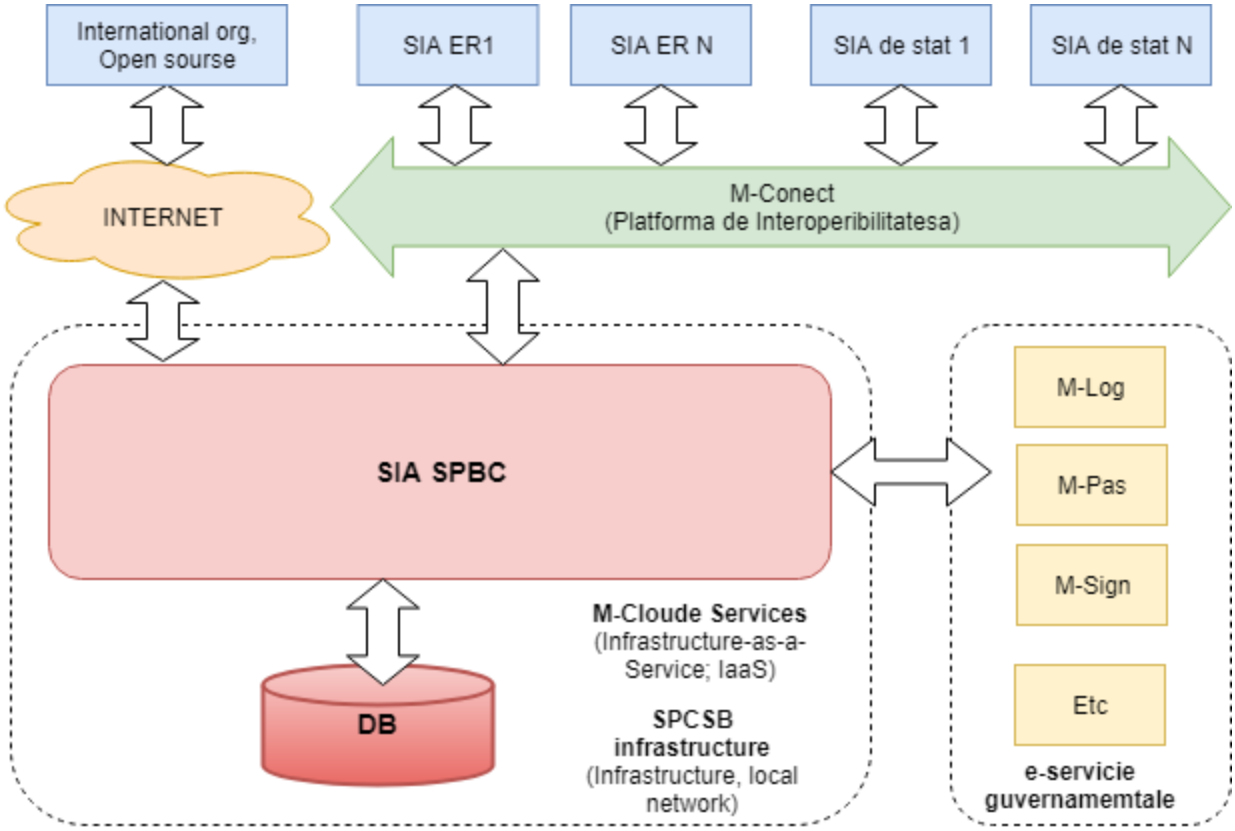

Fig. 1. Principalele componente ale infrastructurii tehnologice a SIA ICCSB și interacțiunea acestora

23. Arhitectura SIA ICCSB

Arhitectura SIA ICCSB are următoarele componente arhitecturale:

1) subsistemul de interacțiune informațională și de informare.

Subsistemul este conceput pentru a interacționa cu sistemele de informare și telecomunicații ale unităților de raportare și a altor organizații, de a primi și a trimite informații, precum și de a oferi acces la informații și de a primi informații din sistemele și registrele cu informații de stat. Subsistemul interacționează cu platforma guvernamentală M-connect. Pentru a obține informații în moduri speciale de evenimente asincrone, subsistemul are propriile contururi de interacțiune și integrare a informației.

2) Subsistemul de acumulare de informații.

Subsistemul asigură acumularea, stocarea, actualizarea și prelucrarea informațiilor primite.

3) Subsistemul de circulație a documentelor și gestiunea proceselor de lucru.

Subsistemul oferă activități de informare a Serviciului prevenirea și combaterea spălării banilor, principalele sale procese de afaceri, lucrul cu documente, obiecte de informare și date. Subsistemul oferă acces și posibilitatea angajaților Serviciului de a lucra în SIA ICCSB, inclusiv rețeaua locală și alte metode.

4) Subsistemul procesării intelectuale și analizei operaționale.

Subsistemul este conceput pentru a detecta cazuri și tranzacții potențial suspecte în ceea ce privește spălarea banilor și finanțarea terorismului. Generarea automată a documentelor analitice pentru a expedia notificare către angajații Serviciului prevenirea și combaterea spălării banilor referitor la tranzacțiile identificate, pentru a furniza informațiile și documentele necesare.

5) Subsistemul analitic.

Subsistemul analitic - un subsistem pentru analiza complexă, cuprinde o multitudine de diferite instrumente analitice pentru a efectua prelucrarea statistică, pentru a efectua diverse analize, pentru a pregăti documentele analitice și rapoarte.

24. Complexul de software și hardware

O listă de software și hardware utilizate în crearea de informații electronice și a infrastructurii de telecomunicații a SIA ICCSB, se vor determina de Serviciul Prevenirea și Combaterea Spălării Banilor și finanțării terorismului cu furnizorii de diferite decizii privind punerea în aplicare a componentei tehnologice individuale a sistemului informațional automatizat și, dacă este necesar, cu operatorul de tehnologii al platformei guvernamentale MCloud.

Capitolul VIII

SECURITATEA ȘI PROTECȚIA SIA ICCSB

25. Definiție

Securitatea SIA ICCSB presupune starea de securitate a resurselor informaționale și a infrastructurii informaționale, ceea ce asigură fiabilitatea, integritatea, confidențialitatea, disponibilitatea și autenticitatea resurselor informaționale. Sistemul de securitate a informațiilor este un set de măsuri juridice, organizaționale, economice și tehnologice menite să prevină amenințările la adresa resurselor informaționale și a infrastructurii informaționale.

26. Amenințările la adresa securității informațiilor

Prin amenințarea la securitatea informațiilor se înțelege un eveniment sau o acțiune potențială care are ca scop provocarea pagubelor la resursele informaționale sau la infrastructura informațională.

Principalele amenințări la adresa securității informaționale a SIA ICCSB sunt:

1) colectarea ilegală și / sau utilizarea informațiilor;
2) încălcarea tehnologiei de procesare a informațiilor;
3) încălcarea confidențialității informațiilor;
4) încălcarea integrității logistice și a securității fizice a informațiilor;
5) perturbarea infrastructurii informaționale;
6) impact fizic asupra componentelor infrastructurii informaționale;
7) introducerea în produsele hardware și software a componentelor care implementează funcții care nu sunt prevăzute în documentația pentru aceste produse;
8) dezvoltarea și distribuirea programelor care perturbă funcționarea normală a sistemelor de informare - comunicare și telecomunicații, inclusiv a sistemelor de protecție a informațiilor;
9) distrugerea, deteriorarea, suprimarea electronică sau distrugerea mijloacelor și sistemelor de prelucrare a informațiilor, telecomunicațiilor și comunicațiilor;
10) impactul sistemelor automate de procesare și transmitere a informațiilor asupra sistemelor de protecție a parolei;
11) compromiterea cheilor și mijloacelor de protecție criptografică a informațiilor;
12) scurgerea de informații prin canale tehnice;
13) introducerea de dispozitive electronice pentru interceptarea informațiilor în mijloacele tehnice de procesare, stocare și transmitere a informațiilor prin intermediul canalelor de comunicare, precum și în birourile autorităților publice;
14) distrugerea, deteriorarea, și furtul echipamentelor și al altor echipamente de stocare;

15) interceptarea informațiilor în rețelele de transmitere a datelor și pe liniile de comunicații, decriptarea acestor informații și / sau impunerea de informații false;
16) utilizarea tehnologiilor informaționale interne și externe necertificate, a mijloacelor de protecție a informațiilor, a telecomunicațiilor și a mijloacelor de comunicare în crearea și dezvoltarea infrastructurii informaționale;
17) accesul neautorizat la resursele informaționale;
18) încălcarea restricțiilor legale privind accesul și distribuirea informațiilor;
19) transferul şi divulgarea neautorizată a datelor cu caracter personal".

27. Scopurile și obiectivele pentru asigurarea securității informațiilor

Pentru a asigura construirea unui sistem eficient de securitate a informațiilor obiectelor SIA ICCSB, este necesar:

1) definirea cerințelor de protecție a informațiilor specifice fiecărui obiect protejat;
2) luarea în considerare a cerințelor actelor normative naționale și internaționale;
3) utilizarea celor mai bune practici (standarde, metodologii) pentru a asigura securitatea informațiilor;
4) identificarea unităților responsabile de implementarea și susținerea sistemului de securitate a informațiilor;
5) repartizarea responsabilității între departamente în implementarea cerințelor sistemului de securitate a informațiilor;
6) definirea, bazată pe managementul riscului de securitate a informațiilor, dispoziții generale, cerințe tehnice și organizatorice care constituie politica de securitate a informațiilor obiectului protejat;
7) respectarea cerințelor politicii de securitate a informațiilor prin introducerea de software și metode tehnice adecvate și instrumente de protecție a informațiilor;
8) implementarea sistemului de management al securității informațiilor.

Principalele sarcini pentru asigurarea securității informațiilor sunt:

1) asigurarea confidențialității informațiilor, prevenirea primirii informațiilor de către persoanele care nu au drepturile și competențele corespunzătoare;
2) asigurarea integrității logice a informațiilor, prevenirea intrării neautorizate, actualizării și distrugerii neautorizate a informațiilor;
3) asigurarea securității fizice a informațiilor;
4) asigurarea protecției infrastructurii informațiilor împotriva daunelor și încercărilor de a schimba funcționarea.

Principalele mecanisme de asigurare a securității informațiilor sunt:

1) autentificarea și autorizarea;
2) control acces;
3) înregistrarea acțiunilor și auditul;
4) criptarea informațiilor;
5) analiza și modelarea fluxurilor de informații (sistemul CASE)
6) monitorizarea rețelei;
7) detectarea și prevenirea intruziunii (IDS / IPS);
8) prevenirea scurgerilor de informații confidențiale (sistemul DLP);
9) analizoare de protocol;
10) mijloace antiviruși;
11) firewall-uri (firewall);
12) sisteme de rezervă;
13) sisteme de alimentare neîntreruptibile;
14) organizația de securitate; regim de securitate
15) mijloace de prevenire a accesului neautorizat în clădiri și spații;
16) instrumente de analiză a securității.

Utilizarea mecanismelor de securitate a informațiilor ar trebui planificată în faza de proiectare a sistemelor de informare și a infrastructurii informatice.

Cea mai vulnerabilă legătură în sistemul de securitate a informațiilor este factorul uman și nerespectarea procedurilor stabilite. În acest sens, un element important al securității informațiilor este antrenarea personalului în metodele și modurile de asigurare a securității informațiilor.

28. Sistemul de protecție a datelor cu caracter personal

Organizarea sistemului de protecție a datelor cu caracter personal este parte integrantă a sistemului general de securitate a informațiilor al SIA ICCSB.

Sistemul de protecție a datelor cu caracter personal este elaborat în baza:

1) rapoartelor cu rezultatele auditului intern;
2) categoriile de date cu caracter personal;
3) actul de clasificare a sistemului informatic de prelucrare a datelor cu caracter personal;
4) modele de amenințări la adresa securității datelor cu caracter personal;
5) dispozițiile privind delimitarea drepturilor de acces la datele cu caracter personal prelucrate;
6) documentele de orientare și politicile de securitate elaborate.

29. Organizarea procedurilor interne ale sistemului de prelucrare a datelor cu caracter personal:

Pentru a asigura permanent un nivel ridicat de protecţie a datelor cu caracter personal SIA privind prelucrarea spălării banilor implică în special:

1) luarea în considerare a protecţiei datelor cu caracter personal încă la momentul conceperii sistemului în special prin minimizarea colectării datelor în funcţie de scop, stabilirea perioada de stocare precum şi garantarea rolului şi responsabilităţii părţilor în efectuarea prelucrării datelor;
2) aplicarea de măsuri tehnice şi organizatorice adecvate pentru a asigura că în mod implicit, sînt prelucrate numai date cu caracter personal care sunt necesare pentru fiecare scop specific al prelucrării;
3) anticiparea unei posibile încălcări a securităţii datelor;
4) asigurarea confidenţialităţii şi securităţii prelucrării prin adoptarea de măsuri tehnice şi organizatorice adecvate.”.