Anexa nr.3
la Hotărîrea Guvernului
nr._____ din _____2019

CONCEPTUL TEHNIC
al Sistemului informațional „Registrul cererilor de intervenție”

INTRODUCERE

Asigurarea respectării drepturilor de proprietate intelectuală în Republica Moldova reprezintă o condiție necesară pentru crearea, protecția, gestionarea și valorificarea plenară a potențialului proprietății intelectuale care să contribuie la dezvoltarea unei economii naționale competitive, bazate pe cunoaștere și inovare.

Produsele intelectuale, informația și cunoștințele, potențialul spiritual, ştiinţific şi cultural al societății contemporane sînt forța motrice a dezvoltării durabile şi determină competitivitatea economică. Toate acestea demonstrează creșterea rolului proprietății intelectuale în societatea modernă, iar eforturile guvernelor de a investi în consolidarea regimurilor de proprietate intelectuală sunt considerate ca investiții generatoare de valoare adăugată şi creștere economică, care implică, totodată, asumarea eforturilor financiare pentru utilizarea tehnologiilor informaționale moderne, inclusiv prin crearea unui sistem informațional pentru asigurarea activității tuturor autorităților cu atribuții în domeniul respectării drepturilor de proprietate intelectuală în Republica Moldova.

Activitatea organelor vamale în domeniul protecției drepturilor asupra obiectelor de proprietate intelectuală, constă în aplicarea măsurilor la frontieră conform procedurii stabilite la Capitolul XII din Codul Vamal. Acest domeniu de activitate vamală se realizează în colaborare cu autorităţile şi organizațiile implicate în asigurarea protecției proprietății intelectuale și titularii drepturilor și are drept obiectiv principal contracararea traficului internațional cu produse contrafăcute și opere-pirat.

Activitatea Serviciului Vamal în acest domeniu este orientată spre asigurarea aplicării eficiente a măsurilor de protecție la frontieră în scopul protejării pieței interne de importul mărfurilor contrafăcute și operelor-pirat, comercializarea cărora cauzează prejudicii titularilor de drepturi, generează acte de concurența neloială, reprezintă un pericol pentru securitatea economică a țării și sănătatea consumatorului autohton.

În scopul eficientizării activității de aplicare a măsurilor legale în vederea protecției la frontieră a drepturilor de proprietate intelectuală și asigurării unui management calitativ și transparent al proceselor relaționale în acest sens (gestionarea cererilor de intervenție), dar și oferirea unui mecanism titularilor de drepturi de proprietate intelectuală pentru depunerea în regim on-line a cererilor de intervenție, monitorizarea statutului acestora și o comunicare mai strînsă, optimă între Serviciul Vamal și titularii de drepturi, se impune necesitatea creării și instituirii Sistemului informațional „Registrul cererilor de intervenție” (*în continuare* - SI e-RCI), ca parte componentă a platformei informaționale în domeniul protecției drepturilor de proprietate intelectuală.

Prezentul Concept tehnic reprezintă o viziune generală asupra creării şi funcționării SI e-RCI, care va conduce la sporirea capacității de gestionare a sistemului de proprietate intelectuală de către principalii actori implicați în asigurarea respectării drepturilor de proprietate intelectuală. Conceptul tehnic stabilește obiectivele, scopul, principiile, cadrul normativ-juridic, caracteristicile funcționale de bază și arhitectura conceptuală a SI e-RCI, precum şi descrie succint obiectele informaționale şi funcționalitățile sistemului.

Capitolul I
DISPOZIŢII GENERALE

1. Definiția Sistemului informațional

Sistemul informațional „Registrul cererilor de intervenție” este un sistem informațional automatizat, parte a platformei informaționale în domeniul protecției drepturilor de proprietate intelectuală, constituit dintr-un ansamblu de resurse și tehnologii informaționale, mijloace tehnice de program și metodologii, aflate în interconexiune care permite titularilor de drepturi de proprietate intelectuală depunerea în regim on-line a cererilor de intervenție pentru aplicarea, la frontieră a măsurilor de protecție a proprietății intelectuale, iar Serviciului Vamal oferă un mecanism de gestionare/management a cererilor de intervenție depuse.

Denumirea prescurtată a Sistemului informațional „Registrul cererilor de intervenție” este SI e-RCI.

În rezultatul funcționării SI e-RCI se formează resursa informațională reprezentată de Registrul Cererilor de Intervenție

2. Destinația sistemului informațional

SI e-RCI este destinat spre a fi utilizat de titularii de drepturi de proprietate intelectuală pentru depunerea în adresa Serviciului Vamal a cererilor de intervenție, în conformitate cu Capitolul XII al Codului Vamal, precum și utilizarea de către Serviciul Vamal pentru organizarea procesului de management și gestionare a cererilor de intervenție, începând de la recepționarea electronică a acestora și pînă la reflectarea deciziei luate prin completarea Registrului cererilor de intervenție.

3. Obiectivul sistemului informațional

Obiectivul principal al SI e-RCI este de a asigura aplicarea eficientă și operativă a măsurilor de protecție la frontieră a drepturilor de proprietate intelectuală și oferirea pentru titularii de drepturi de proprietate intelectuală a unor mecanisme eficiente de interacțiune cu organele de specialitate, prin:

1) oferirea interfeței pentru depunerea de către titularii de drepturi a cererilor de intervenție și monitorizarea statutului cererilor depuse, recepționarea notificărilor;

2) expunerea unificată a informației privind cererile de intervenție acceptate prin Registrul cererilor de intervenție;

3) expunerea unificată a informației privind măsurile de protecție aplicate, acțiunile întreprinse de Serviciul Vamal, prin Registrul cererilor de intervenţie;

4) oferirea spațiului de lucru necesar Serviciului Vamal pentru gestionarea cererilor de intervenție, monitorizarea și raportarea proceselor aferente și a măsurilor aplicate;

5) crearea mecanismului statistic pentru monitorizarea eficienței activităților întreprinse de Serviciul Vamal în domeniul asigurării protecției drepturilor de proprietate intelectuală.

4. Noțiuni

În sensul prezentului Concept tehnic, următoarele noțiuni semnifică:

ansamblu de mijloace software şi hardware – totalitate a programelor şi mijloacelor tehnice care asigură realizarea proceselor informaționale;

bază de date – colecție de date organizată conform unei structuri conceptuale, care descrie caracteristicile acestor date şi relațiile dintre entitățile lor componente, destinată unuia sau mai multor domenii de aplicație;

identificator de obiect informațional – unul dinte atributele obiectului informațional, care este unic şi rămîne invariabil pe parcursul întregii perioade de existență a obiectului în SI e-RCI;

clasificator – totalitate a semnificațiilor anumitor caracteristici ale obiectului şi codurilor digitale sau literale ce corespund acestora;

obiect informațional – reflectare virtuală a obiectului înregistrării în cadrul resursei informaționale;

resursă informațională – totalitate de informații conținute în SI e-RCI, organizată în conformitate cu cerințele stabilite şi cu legislația;

obiecte de proprietate intelectuală (în continuare - OPI) – orice rezultat al activității intelectuale, confirmat şi protejat prin drepturile corespunzătoare privind utilizarea acestuia, care se divizează în obiecte de proprietate industrială (invenții, soiuri de plante, topografii de circuite integrate, mărci, desene şi modele industriale, indicații geografice, denumiri de origine şi specialități tradiționale garantate) și obiecte ale dreptului de autor (opere literare, artistice şi științifice exprimate în diferite forme, prevăzute prin lege) şi ale drepturilor conexe (interpretări, fonograme, videograme şi emisiuni ale organizațiilor de difuziune);

cerere de intervenție – solicitare prezentată Serviciului Vamal pentru a interveni în cazul mărfurilor susceptibile de a aduce atingere unui drept de proprietate intelectuală;

date privind încălcările drepturilor de proprietate intelectuală – cereri de intervenție referitoare la obiectele de proprietate intelectuală depuse la Serviciul vamal, OPI ce beneficiază de protecţie la frontieră, reţineri înregistrate şi rezultatul reţinerilor; cereri (sesizări) referitoare la obiectele de proprietate intelectuală depuse la Inspectoratul General al Poliției, procedura de control efectuată, actul de constatare, procedura de ridicare a produselor şi dosare înregistrate (contravenționale şi penale); cereri (sesizări) referitoare la obiectele de proprietate intelectuală depuse la Procuratura Generală, procedura de control efectuată, actul de constatare, procedura de ridicare a produselor, dosare înregistrate şi hotărâri judecătorești.

5. Principiile de bază ale sistemului

Principiile de bază ale creării SI e-RCI sunt:

1) *principiul legalității*, care presupune crearea şi exploatarea sistemului informațional în conformitate cu legislația națională, a normelor şi standardelor internaționale recunoscute în domeniu;

2) *principiul respectării drepturilor omului*, care prevede utilizarea sistemului în strictă conformitate cu actele normative naționale și în limitele prevederilor tratatelor și convențiilor în domeniul asigurării drepturilor omului, la care Republica Moldova este parte;

3) *principiul integrității datelor*, care presupune păstrarea conținutului şi interpretarea univocă a datelor în condițiile unor acțiuni accidentale. Integritatea datelor se consideră a fi păstrată dacă datele nu au fost denaturate, modificate sau distruse;

4) *principiul plenitudinii datelor*, prin care se are în vedere asigurarea volumului complet al informației colectate în conformitate cu actele normative;

5) *principiul veridicității datelor*, care presupune introducerea datelor în SI e-RCI în baza documentelor autentice, precum şi asigurarea unui grad înalt de corespundere a datelor stocate în Sistem cu starea reală a obiectelor reprezentate de acestea într-un domeniu concret;

6) *principiul datelor sigure*, care presupune introducerea datelor în sistem doar prin canale autorizate, autentificate și criptate;

7) *principiul securității informaționale*, care presupune asigurarea unui nivel adecvat de integritate, selectivitate, accesibilitate şi eficiență pentru protecția datelor de pierderi, alterări, deteriorări şi de acces nesancționat;

8) *principiul accesibilității informației cu caracter public*, care presupune implementarea procedurilor de asigurare a accesului solicitanților la informația cu caracter public furnizată de soluția informatică;

9) *principiul transparenței*, care presupune proiectarea şi implementarea sistemului conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informaționale şi de telecomunicații;

10) *principiul scalabilității*, care semnifică posibilitatea extinderii şi completării sistemului informațional cu noi funcţii sau îmbunătăţirea celor existente;

11) *principiul integrării cu produsele de program existente*, care presupune posibilitatea soluției informatice de a se integra și interacționa cu aplicațiile, serviciile și bazele de date implementate în cadrul autorităților publice și instituțiilor din Republica Moldova;

12) *principiul simplității şi comodității utilizării*, care presupune proiectarea şi realizarea tuturor aplicaţiilor, mijloacelor tehnice și de program accesibile utilizatorilor sistemului, bazate pe principii exclusiv vizuale, ergonomice şi logice de concepţie;

13) *principiul independenței și neutralității tehnologice*, care presupune că sistemul trebuie să se orienteze pe cerințele funcționale, asigurând accesul la serviciul informatic public independent de tehnologii sau produse specifice;

14) *principiul îmbinării publicității şi confidenţialităţii*, care prevede publicarea informaţiei general accesibile, cu excepţia informaţiei recunoscute ca fiind confidenţială, în modul stabilit de legislaţia naţională;

15) *principiul unității spațiului informațional*, care prevede utilizarea unui sistem unic de clasificatoare, formate de date, protocoale de interacţiune informaţională, standarde, documente normative şi metodice interdependente, condiţie care este necesară pentru formarea spaţiului informaţional unic al sistemului de prestare a serviciilor publice;

16) *principiul protecţiei datelor cu caracter personal*, prevede crearea şi exploatarea sistemului în conformitate cu acordurile şi convenţiile internaţionale, precum şi cu legislaţia naţională în domeniul protecţiei datelor cu caracter personal;

17) *principiul conectivității*, care presupune că sistemul trebuie să poată crea și expune servicii informaționale de consum și de furnizare a datelor;

18) *principiul controlului*, care prevede controlul măsurilor ce asigură calitatea, fiabilitatea resurselor şi sistemelor informaţionale de stat, precum şi păstrarea şi utilizarea raţională a acestora;

19) *principiul utilizării produselor de program licențiate* și a mijloacelor tehnice certificate;

20) *principiul neexcesivităţii şi pertinenţei*, care relevă necesitatea limitării volumului de informaţii cu accesibilitate limitată prelucrate, în aşa fel încît să fie prelucrate doar informaţiile relevante şi necesare în contextul realizării sarcinilor SI e-RCI.

6. Sarcinile principale ale sistemului:

Sarcinile de bază ce urmează a fi realizate la exploatarea SI e-RCI sunt:

1) Eficientizarea procesului de implementare a mecanismelor de protecție a drepturilor de proprietate intelectuală;

2) Standardizarea procedurilor, formularelor, nomenclatoarelor, seturilor de date, la nivelul întregului sistem;

3) Optimizarea comunicării și coordonării interinstituționale prin automatizarea procesului de colectare și transmitere a datelor relevante procesului de aplicare a mecanismelor de protecție a drepturilor de proprietate intelectuală de către autoritățile implicate în implementarea legilor și actelor normative guvernamentale privind drepturile de proprietate intelectuală din Republica Moldova;

4) Creșterea gradului de transparență și accesibilitate a informațiilor prin asigurarea mijloacelor de acces unificat la baza de date privind cererile de intervenție acceptate, dar și la măsurile de protecție aplicate pentru protejarea obiectelor de proprietate intelectuală;

5) Securizarea informațiilor cu accesibilitate limitată, prin implementarea unei politici de acces în sistem pentru fiecare utilizator în funcție de competențe și atribuții specifice;

6) Asigurarea mecanismelor corespunzătoare de monitorizare și audit prin implementarea instrumentelor terțe, externe de asigurare a redundanței informațiilor și evenimentelor jurnalizate;

7) Asigurarea interoperabilității cu alte sisteme informaționale pentru a prelua și a transmite informații.

Capitolul II
CADRUL NORMATIV-JURIDIC AL SI e-RCI

7. Cadrul juridico-normativ al SI e-RCI este format din legislaţia naţională, acordurile şi convenţiile internaţionale la care Republica Moldova este parte, precum şi actele normative care reglementează domeniul proprietăţii intelectuale.

8. Crearea şi funcţionarea SI e-RCI este reglementată, în particular, de următoarele acte normative:

Constituţia Republicii Moldova din 29 iulie 1994;

Codul civil al Republicii Moldova nr.1107/2002 (Monitorul Oficial al Republicii Moldova, 2002, nr.82–86, art.661);

Codul de procedură civilă al Republicii Moldova nr.225/2003 (republicat în Monitorul Oficial al Republicii Moldova, 2018, nr.285–294, art.436);

Codul contravenţional al Republicii Moldova nr.218/2008 (republicat în Monitorul Oficial al Republicii Moldova, 2017, nr.78-84, art.100);

Codul penal al Republicii Moldova nr. 985/2002 (publicat în Monitorul Oficial al Republicii Moldova, 2009, nr. 72-74, art. nr. 195);

Codul de procedură penală al Republicii Moldova nr.122/2003 (republicat în Monitorul Oficial al Republicii Moldova, 2013, nr.248–251, art.699);

Codul vamal al Republicii Moldova nr.1149/2000 (republicat în Monitorul Oficial al Republicii Moldova, ediţie specială din 01.01.2007);

Codul de executare al Republicii Moldova nr.443/2004 (republicat în Monitorul Oficial al Republicii Moldova, 2010, nr.214–220, art.704);

Legea nr.114/2014 cu privire la Agenţia de Stat pentru Proprietatea Intelectuală (Monitorul Oficial al Republicii Moldova, 2014, nr.282-289, art.600);

Legea nr. 161/2007 privind protecția desenelor și modelelor industriale (Monitorul Oficial al Republicii Moldova, 2007, nr.136-140, art.577);

Legea nr. 38/2008 privind protecția mărcilor (Monitorul Oficial al Republicii Moldova, 2008, nr.99-101, art.362);

Legea nr. 50/2008 privind protecția invențiilor (Monitorul Oficial al Republicii Moldova, 2008, nr.117-119, art.455);

Legea nr. 39/2008 privind protecția soiurilor de plante (Monitorul Oficial al Republicii Moldova, 2008, nr.99-101, art.364);

Legea nr.66/2008 privind protecția indicațiilor geografice, denumirilor de origine și specialităților tradiționale garantate (Monitorul Oficial al Republicii Moldova, 2008, nr.134-137, art.527);

Legea nr. 139/2010 privind dreptul de autor și drepturile conexe (Monitorul Oficial al Republicii Moldova, 2010, nr.191-193, art.630);

Legea nr. 320/2012 cu privire la activitatea Poliţiei şi statutul poliţistului (Monitorul Oficial al Republicii Moldova, 2013, nr.42-47, art.145);

Legea nr. 3/2016 cu privire la Procuratură (Monitorul Oficial al Republicii Moldova, 2016, nr.69-77, art.113);

Legea nr.982/2000 privind accesul la informaţie (Monitorul Oficial al Republicii Moldova, 2000, nr.88-90, art.664);

Legea nr.1069/2000 cu privire la informatică (Monitorul Oficial al Republicii Moldova, 2001, nr.73-74, art.547);

Legea nr.467/2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova, 2004, nr.6-12, art.44);

Legea nr.142/2018 cu privire la schimbul de date și interoperabiliate (Monitorul Oficial al Republicii Moldova, 2018, nr. 295-308, art. 452);

Legea nr.71/2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314);

Legea nr.133/2011 privind protecţia datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2011, nr.170-175, art.492);

Legea nr.91/2014 privind semnătura electronică şi documentul electronic (Monitorul Oficial al Republicii Moldova, 2014, nr.174-177, art.397);

Hotărîrea Guvernului nr. 1496/2008 pentru aprobarea Regulamentului privind procedura de depunere, examinare şi înregistrare a desenelor şi modelelor industriale (Monitorul Oficial al Republicii Moldova, 2009, nr.3-6, art.10) ;

Hotărîrea Guvernului nr. 488/2009 pentru aprobarea Regulamentului privind procedura de depunere, examinare şi înregistrare a mărcilor (Monitorul Oficial al Republicii Moldova, 2009, nr.127-130, art.550);

Hotărîrea Guvernului nr. 528/2009 pentru aprobarea Regulamentului privind procedura de depunere şi examinare a cererii de brevet de invenţie şi de eliberare a brevetului (Monitorul Oficial al Republicii Moldova, 2009, nr.138-139, art.593);

Hotărîrea Guvernului nr. 295/2009 pentru aprobarea Regulamentului privind procedurile de depunere şi examinare a cererii, de acordare şi de menţinere în vigoare a brevetului pentru soi de plantă (Monitorul Oficial al Republicii Moldova, 2009, nr.80-81, art.346);

Hotărîrea Guvernului nr. 610/2010 pentru aprobarea Regulamentului privind procedura de depunere, examinare şi înregistrare a indicaţiilor geografice, a denumirilor de origine şi a specialităţilor tradiţionale garantate (Monitorul Oficial al Republicii Moldova, 2010, nr.119-120, art.691);

Hotărîrea Guvernului nr. 89/2012 pentru aprobarea Regulamentului cu privire la înregistrarea obiectelor dreptului de autor şi drepturilor conexe (Monitorul Oficial al Republicii Moldova, 2012, nr.34-37, art.114);

Hotărîrea Guvernului nr. 915/2016 pentru aprobarea Regulamentului privind asigurarea respectării drepturilor de proprietate intelectuală de către organele vamale (Monitorul Oficial al Republicii Moldova, 2016, nr.247-255, art.999);

Hotărârea Guvernului nr. 1123/2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal (Monitorul Oficial al Republicii Moldova, 2010, nr. 254-256, art. 1282);

Hotărârea Guvernului nr.1090/2013 privind serviciul electronic guvernamental de autentificare și control al accesului (MPass) (Monitorul Oficial al Republicii Moldova, 2014, nr.4-8, art.2);

Hotărârea Guvernului nr.128/2014 privind platforma tehnologică guvernamentală comună (MCloud) (Monitorul Oficial al Republicii Moldova, 2014, nr.47-48, art.145);

Hotărârea Guvernului nr.405/2014 privind serviciul electronic guvernamental integrat de semnătură electronică (MSign) (Monitorul Oficial al Republicii Moldova, 2014, nr.147-151, art.445);

Hotărârea Guvernului nr.708/2014 „Privind serviciul electronic guvernamental de jurnalizare (MLog)" (Monitorul Oficial al Republicii Moldova, 2014, nr.261-267, art.756);

Hotărîrea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat (Monitorul Oficial al Republicii Moldova, 2018, nr.157-166, art.474).

Capitolul III
SPAŢIUL FUNCŢIONAL AL SI e-RCI

9. Sistemul trebuie să asigure realizarea funcțiilor de bază ale sistemului informațional, conform legislației, precum și a funcțiilor specifice ce reies din destinația sistemului, după cum urmează:

1) *inițierea procedurii de protecție* – crearea interfeței pentru depunerea de către titularul de drepturi la Serviciul Vamal a cererii de intervenție, monitorizarea statutului cererilor depuse;

2) *managementul cererilor de intervenție* – oferirea spațiului tehnologic pentru Serviciul Vamal, în scopul organizării procesului de examinare și acceptare a cererilor de intervenție, stabilire a perioadei de intervenție;

3) *formarea resursei informaționale unice în domeniul cererilor de intervenție acceptate* și obiectelor de proprietate intelectuală ce beneficiază de această măsură de protecție;

4) *formarea resursei informaționale unice privind măsurile de protecție prin reținerea mărfurilor* susceptibile a aduce atingere dreptului de proprietate intelectuală, precum și privind aplicarea măsurilor asupra mărfurilor în privința cărora s-a dovedit că aduc atingere unui drept de proprietate intelectuală;

5) *asigurarea accesului la informație*. Informația din SI e-RCI este pusă la dispoziția autorităților implicate şi titularilor de drepturi. Nivelul de acces al beneficiarilor la informația din

SI e-RCI este stabilit de legislație, în dependență de statutul juridic și regimul juridic al informației. Fiecare beneficiar este obligat să utilizeze informația strict în scopurile legale;

6) *asigurarea securității și protecției informației*. Asigurarea securității și protecției informației, la toate etapele de prelucrare a resurselor informaționale se efectuează în conformitate cu prevederile legislației și standardelor de securitate, bunelor practici în domeniul dat, cu utilizarea metodelor avansate de autentificare și de autorizare a utilizatorilor, conform rolului atribuit în SI e-RCI, precum şi cu utilizarea mecanismelor de protecție a datelor şi a canalelor de conexiune, de monitorizare și jurnalizare a evenimentelor produse în cadrul sistemului;

7) *administrarea sistemului*, care include următoarele acțiuni de administrare a rolurilor și drepturilor utilizatorilor, administrarea nomenclatoarelor, alte activități de administrare şi acces la funcționalitățile SI e-RCI;

8) *asigurarea calității informațiilor* utilizînd componentele sistemului de management al calității.

10. În cadrul funcționării SI e-RCI vor fi realizate funcții specifice, grupate în module și contururi funcționale, după cum urmează:

1) **Modulul funcțional al titularului de drepturi de proprietate intelectuală**. În cadrul acestui modul sunt operaționale următoarele contururi funcționale:

a) conturul „CERERI DE INTERVENȚIE”;

b) conturul „REGISTRUL CERERILOR DE INTERVENȚIE”;

c) conturul „NOTIFICĂRI”;

d) conturul „INCIDENTE”.

2) **Modulul funcțional al Serviciului Vamal.** Acest modul reprezintă spațiul de lucru destinat reprezentanților Serviciului Vamal pentru organizarea procesului de examinare, acceptare a cererilor de intervenție, gestionarea Registrului cererilor de intervenție și măsurilor de reținere aplicate. În cadrul acestui modul sunt operaționale următoarele contururi funcționale:

a) conturul „CERERI DE INTERVENȚIE”;

b) conturul „REGISTRUL CERERILOR DE INTERVENȚIE”;

c) conturul „REȚINERI”;

d) conturul „NOTIFICĂRI”;

e) conturul „INCIDENTE”.

3) **Modulul funcțional de administrare și monitorizare** asigură interacțiunea informațională a tuturor participanților sistemului și reprezintă un subsistem integrat de control și monitorizare a formării și utilizării resursei informaționale.

Conturul respectiv include următoarele funcții:

a) asigurarea integrității logice a SI e-RCI;

b) administrarea bazelor de date ale SI e-RCI;

c) elaborarea și mentenanța ghidurilor de sistem și a clasificatoarelor;

d) delimitarea drepturilor de acces pentru utilizatori;

e) monitorizarea respectării regulilor de autentificare și autorizare, management al utilizatorilor;

f) asigurarea securității, protecției și integrității informației în sistem conform cerințelor standardelor naționale SM EN ISO/IEC 27001:2017 „Tehnologia informației. Tehnici de securitate. Sisteme de management al securității informației. Cerințe”;

g) asigurarea respectării cerințelor sistemului de protecție a datelor cu caracter personal.

11. Modul funcțional al titularului de drepturi de proprietate intelectuală, reprezintă interfața destinată titularilor de drepturi pentru depunerea cererilor de intervenție, monitorizarea statutului acestor cereri, consultarea Registrului cererilor de intervenție, recepționarea notificărilor, raportarea incidentelor, informarea privind drepturile de proprietate intelectuală.

11.1. Conturul „**CERERI DE INTERVENȚIE**” (titular), oferă următoarele funcționalități:

- căutarea unei cereri de intervenție după: numărul cererii, titularul de drepturi, numărul de înregistrare al OPI;

- vizualizarea rezultatului căutării reprezintă informații despre cererile de intervenție inițiate de titularul de drepturi;

- adăugarea unei înregistrări – funcționalitate care permitea inițierea, completarea unei cereri de intervenție, atașarea documentelor conform prevederilor legale, semnarea electronică a cererii și remiterea în adresa Serviciului Vamal. Informația despre obiectele de proprietate intelectuală sunt preluate în mod automatizat, prin servicii informaționale, din Sistemul informațional în domeniul obiectelor de proprietate intelectuală, gestionat de AGEPI;

- organizarea cererilor de intervenție ale titularului în:

- Cereri în lucru – reflectă cererile inițiate, cererile completate ce pot fi semnate electronic, cererile semnate electronic de titular;
- Cereri transmise – reflectă cererile transmise către Serviciul Vamal și permite vizualizarea în timp real a statutului cererii transmise (Figura. 1);
- Cereri incomplete – reflectă cererile transmise către Serviciul Vamal și returnate de către acesta pentru corectări, completări;
- Cereri acceptate – reflectă cererile care au fost aprobate de către Serviciul Vamal;
- Cereri respinse – reflectă cererile ce au fost respinse de către Serviciul Vamal;
- Cereri anulate – reflectă cererile anulate în conformitate cu prevederile legale;
- Cereri suspendate - reflectă cererile suspendate în conformitate cu prevederile legale;
- Cereri în curs de expirare - reflectă cererile în curs de expirare;
- Cereri expirate – reflectă cererile care deja au expirat.

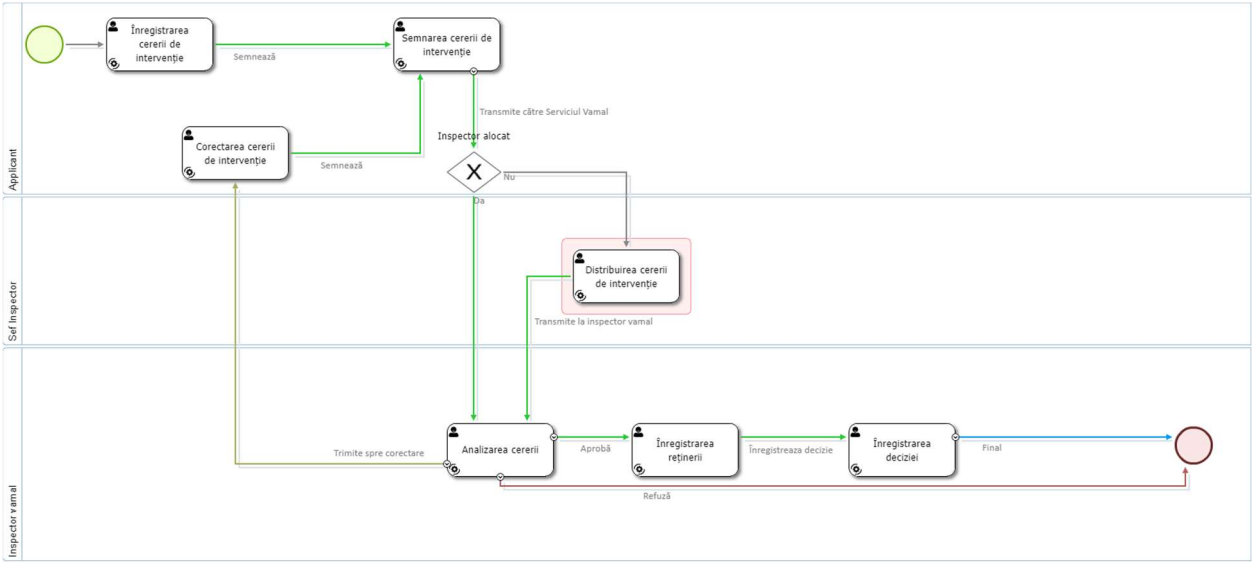

Figura 1. Exemplu privind rezultatul operațiunii de monitorizare a statutului cererii de intervenție transmise de titular.

În cadrul conturului informațional „**CERERE de INTERVENȚIE**” sunt configurate date despre următoarele obiecte informaționale:

a) obiectul informațional „Intervenție”, care conține următoarele date:

- numărul cererii;
- data depunerii cererii;
- data transmiterii;
- numărul de intrare al cererii;
- statutul solicitantului;
- mențiunea privind solicitarea utilizării procedurii de la art. 305^1 Cod Vamal;
- inspectorul vamal responsabil/alocat;
- data deciziei;
- perioada de valabilitate a protecției;
- informații privind decizia de refuzare;

- documente generate (Declarația titularului, în sensul art. 302[1] Cod Vamal și Cererea de intervenție, în sensul art. 303 Cod Vamal).

b) obiectul informațional „Solicitant”, care conține următoarele date:
- jurisdicția persoanei;
- statutul persoanei;
- calitatea persoanei;
- funcția;
- IDNO/IDNP;
- denumirea persoanei juridice/Nume, prenumele persoanei fizice;
- date de contact (localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

c) obiectul informațional „Persoane de contact”, care conține următoarele date:
- jurisdicția persoanei;
- statutul persoanei;
- calitatea persoanei;
- responsabilitatea persoanei (probleme administrative/tehnice);
- IDNP;
- nume, prenumele persoanei fizice;
- date de contact (localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

d) obiectul informațional „Obiectul de proprietate intelectuală”, preluat din Sistemul informaţional privind protecţia obiectelor de proprietate intelectuală (în continuare – SI e-OPI), și conține următoarele date:
- numărul cererii de intervenție;
- numărul înregistrării OPI;
- data înregistrării OPI;
- termenul de valabilitate al înregistrării OPI;
- statutul OPI;
- originea cererii;
- denumirea OPI;
- tipul OPI;
- clasele de protecție/clasificare;
- imaginea grafică;
- datele titularului OPI/reprezentantului (Jurisdicția persoanei; Statutul persoanei; Calitatea persoanei; Funcția; IDNO; Denumirea persoanei juridice; Date de contact: localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

e) obiectul informațional „Documente atașate”, care conține următoarele date:
- numărul documentului;
- tipul documentului;
- numele fișierului;
- autorul documentului;
- data creării documentului;
- mărimea fișierului.

f) obiectul informațional „Reținere”, care va conține următoarele date:
- numărul cererii de intervenție;
- subdiviziunea organului vamal;
- data reținerii/suspendării;
- procedura aplicată (cerere de intervenție/ex officio);
- tipul produsului;
- starea bunului;
- OPI;
- proprietarul bunurilor;
- titularul de drepturi;
- țara de origine;
- țara de destinație;

- tipul de transport;
- acțiunea întreprinsă (tipul acțiunii, data dispunerii acțiunii, data aplicării acțiunii).

g) obiectul informațional „Contestații”, care conține următoarele date:
- numărul cererii de intervenție;
- tipul/obiectul contestației;
- rezultatul contestației.

11.2. Conturul „**REGISTRUL CERERILOR DE INTERVENȚIE**” oferă titularului de drepturi funcționalități de:

- Căutare avansată în Registrul cererilor de intervenție;
- Consultare, vizualizare a datelor din Registrul cererilor de intervenție și acces direct către detaliile cererii de intervenție;
- Căutare punctuală în Registrul cererilor de intervenție;
- Exportarea informațiilor din Registrul cererilor de intervenție (format Word, Excel, PowerPoint, PDF, TIFF file, MHTML, CSV, XML file, Data feed);
- Imprimarea informațiilor din Registrul cererilor de intervenție.

În cadrul conturului informațional „**REGISTRUL CERERILOR DE INTERVENȚIE**”, sunt configurate următoarele date:

- numărul cererii de intervenție;
- data depunerii cererii;
- statut solicitant;
- persoană fizică/persoană juridică;
- național/străin;
- numele persoanei responsabile de examinare din cadrul Serviciului Vamal;
- statutul cererii;
- informația despre OPI relaționat cererii de intervenție (tipul OPI, numărul înregistrării, nume titular de drepturi, clasele de protecție/clasificare, imaginea grafică).

11.3. Conturul funcțional „**NOTIFICĂRI**”, oferă titularului de drepturi recepționarea notificărilor privind acțiunile întreprinse în contextul inițierii, depunerii unei cereri de intervenție, acțiunile întreprinse de Serviciul Vamal în legătura cu cererea titularului și statutul de examinare a acesteia.

Conturul conține următoarele tipuri de notificări:

- notificare privind inițierea cererii de intervenție;
- notificare privind cererea de intervenție pregătită pentru a fi semnată electronic;
- notificare privind semnarea electronică de către titular a cererii de intervenție;
- notificare privind transmiterea cererii de intervenție către Serviciul Vamal;
- notificare privind expedierea/returnarea cererii de intervenție pentru modificări, corectări, completări;
- notificare privind inspectorul vamal asignat;
- notificare privind acceptarea cererii de intervenție;
- notificare privind refuzarea cererii de intervenție;
- notificare privind anularea cererii de intervenție;
- notificare privind suspendarea cererii de intervenție;
- notificare privind expirarea cererii de intervenție.

11.4. Conturul funcțional „**INCIDENTE**”, permite titularului de drepturi raportarea unor incidente, probleme apărute în procesul de utilizare a sistemului informațional.

Incidentele raportate sunt clasificate în următoarele tipuri:

- Cerință tehnică anterior nedefinită;
- Cerință tehnică neimplementată (eroare logică);
- Îmbunătățire minoră de utilizare;
- Eroare de soft ce determină funcționarea inadecvată a sistemului (bug);
- Solicitare de clarificare;
- Solicitare de suport tehnic;
- Solicitare de training.

La fel, în cadrul conturului funcțional titularul are posibilitatea de a căuta un anumit incident, în baza unor parametri dinamici, precum și de a monitoriza statutul incidentului raportat:

- Depus;
- În progres;
- În proces de testare;
- Suspendat;
- Anulat;
- Soluționat.

12. **Modulul funcțional al Serviciului Vamal**, reprezintă spațiul de lucru destinat reprezentanților Serviciului Vamal pentru organizarea procesului de examinare, acceptare a cererilor de intervenție, gestionarea Registrului cererilor de intervenție și măsurilor de reținere aplicate. În cadrul acestui modul sunt operaționale următoarele contururi funcționale:

12.1. Conturul „**CERERI DE INTERVENȚIE**" (Serviciul Vamal), oferă următoarele funcționalități:

Pentru inspectorul vamal șef:

- căutarea unei cereri de intervenție după: numărul cererii, titularul de drepturi, numărul de înregistrare al OPI;
- vizualizarea rezultatului căutării, care reprezintă informații despre cererile de intervenție inițiate de titularul de drepturi;
- recepționarea și vizualizarea cererilor de intervenție depuse de titulari;
- alocarea unui inspector vamal și transmiterea spre examinare de către acesta a cererii de intervenție;
- gestionarea cererilor de intervenție aflate în examinare la inspectorii vamali și funcționalitatea de realocare a inspectorului;
- gestionarea cererilor de intervenție pe suport de hîrtie, examinate de inspectorii vamali;
- gestionarea cererilor de intervenție acceptate, funcționalitatea de realocare a inspectorului vamal;
- gestionarea cererilor de intervenție respinse, suspendate și anulate.

Pentru inspectorul vamal:

- căutarea unei cereri de intervenție după: numărul cererii, titularul de drepturi, numărul de înregistrare al OPI;
- vizualizarea rezultatului căutării, care reprezintă informații despre cererile de intervenție inițiate de titularul de drepturi;
- recepționarea și vizualizarea cererilor de intervenție depuse de titulari și repartizate de inspectorul vamal șef;
- gestionarea cererilor de intervenție electronice și pe hîrtie, repartizate spre examinare de inspectorul vamal șef prin funcționalitatea de „Aprobarea cererii", „Refuzarea cereri";
- gestionarea cererilor de intervenție acceptate prin funcționalitatea de „Anularea cererii" și „Suspendarea cererii";
- gestionarea cererilor de intervenție respinse, suspendate și anulate.

În cadrul conturului informațional „**CERERI DE INTERVENȚIE**" (Serviciul Vamal), sunt configurate date despre următoarele obiecte informaționale:

a) obiectul informațional „Intervenție", care conține următoarele date:

- numărul cererii;
- data depunerii cererii;
- data transmiterii;
- numărul de intrare al cererii;
- statutul solicitantului;
- mențiunea privind solicitarea utilizării procedurii de la art. 305^1 Cod Vamal;
- inspectorul vamal responsabil/alocat;
- data deciziei;

- perioada de valabilitate a protecției;
- informații privind decizia de refuzare;
- documente generate (Declarația titularului, în sensul art. 302[1] Cod Vamal și Cererea de intervenție, în sensul art. 303 Cod Vamal).

b) obiectul informațional „Solicitant”, care conține următoarele date:
- jurisdicția persoanei;
- statutul persoanei;
- calitatea persoanei;
- funcția;
- IDNO/IDNP;
- denumirea persoanei juridice/Nume, prenumele persoanei fizice;
- date de contact (localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

c) obiectul informațional „Persoane de contact”, care conține următoarele date:
- jurisdicția persoanei;
- statutul persoanei;
- calitatea persoanei;
- responsabilitatea persoanei (probleme administrative/tehnice);
- IDNP;
- nume, prenumele persoanei fizice;
- date de contact (localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

d) obiectul informațional „Obiectul de proprietate intelectuală”, preluat din SI e-OPI, și conține următoarele date:
- numărul cererii de intervenție;
- numărul înregistrării OPI;
- data înregistrării OPI;
- termenul de valabilitate al înregistrării OPI;
- statutul OPI;
- originea cererii;
- denumirea OPI;
- tipul OPI;
- clasele de protecție/clasificare;
- imaginea grafică;
- datele titularului OPI/reprezentantului (Jurisdicția persoanei; Statutul persoanei; Calitatea persoanei; Funcția; IDNO; Denumirea persoanei juridice; Date de contact: localitate, oraș, cod poștal, strada, apartament, telefon fix/mobil, email, fax).

e) obiectul informațional „Documente atașate”, care conține următoarele date:
- numărul documentului;
- tipul documentului;
- numele fișierului;
- autorul documentului;
- data creării documentului;
- mărimea fișierului.

f) obiectul informațional „Rețineri”, care va conține următoarele date:
- numărul cererii de intervenție;
- subdiviziunea organului vamal;
- data reținerii/suspendării;
- procedura aplicată (cerere de intervenție/ex officio);
- tipul produsului;
- starea bunului;
- OPI;
- proprietarul bunurilor;
- titularul de drepturi;
- țara de origine;

- țara de destinație;
- tipul de transport;
- acțiunea întreprinsă (tipul acțiunii, data dispunerii acțiunii, data aplicării acțiunii).

g) obiectul informațional „Contestații”, care conține următoarele date:
- numărul cererii de intervenție;
- tipul/obiectul contestației;
- rezultatul contestației.

12.2. Conturul „**REGISTRUL CERERILOR DE INTERVENȚIE**” (Serviciul Vamal) oferă reprezentatului Serviciul Vamal funcționalități de:

- Căutare avansată în Registrul cererilor de intervenție;
- Consultare, vizualizare a datelor din Registrul cererilor de intervenție și acces direct către detaliile cererii de intervenție;
- Căutare punctuală în Registrul cererilor de intervenție;
- Exportarea informațiilor din Registrul cererilor de intervenție (format Word, Excel, PowerPoint, PDF, TIFF file, MHTML, CSV, XML file, Data feed);
- Imprimarea informațiilor din Registrul cererilor de intervenție.

În cadrul conturului informațional „**REGISTRUL CERERILOR DE INTERVENȚIE**” (Serviciul Vamal), sunt configurate următoarele date:
- numărul cererii de intervenție;
- data depunerii cererii;
- statut solicitant;
- persoană fizică/persoană juridică;
- național/străin;
- numele persoanei responsabile de examinare din cadrul Serviciului Vamal;
- statutul cererii;
- informația despre OPI relaționat cererii de intervenție (tipul OPI, numărul înregistrării, nume titular de drepturi, clasele de protecție/clasificare, imaginea grafică).

12.3. Conturul funcțional „**REȚINERI**” (Serviciul Vamal), reprezintă instrumentarul necesar reprezentanților Serviciului Vamal pentru gestionarea și monitorizarea procedurilor de reținere a bunurilor în privința cărora există suspecții că aduc atingere drepturilor de proprietate intelectuală.

Conturul pune la dispoziție reprezentantului Serviciului Vamal funcționalități de:

1) inițiere a procedurii ex officio. Astfel, la inițierea unei noi înregistrări privind procedura ex officio, sunt configurate următoarele cîmpuri de date:
- numărul cererii de intervenție;
- subdiviziunea organului vamal;
- data reținerii/suspendării;
- procedura aplicată;
- tipul produsului;
- starea bunului (contrafăcut, falsificat, original);
- țara de origine;
- țara de destinație;
- tipul transportului (aerian, maritim, rutier, poștal, cale ferată).

2) vizualizare, consultare a reținerilor dispuse de Serviciul Vamal, unde sunt disponibile următoarele date:
- numărul cererii de intervenție;
- subdiviziunea organului vamal;
- data reținerii/suspendării;
- procedura aplicată;
- tipul produsului;
- starea bunului (contrafăcut, falsificat, original);
- obiectul de proprietate intelectuală;

- proprietarul bunurilor;
- titularul de drepturi;
- țara de origine;
- țara de destinație;
- tipul transportului (aerian, maritim, rutier, poștal, cale ferată);
- acțiuni dispuse, cu posibilitatea de redactare, adăugare a unei noi acțiuni.

12.4. Conturul funcțional „**NOTIFICĂRI**" (Serviciul Vamal), oferă reprezentantului Serviciului Vamal recepționarea notificărilor privind acțiunile întreprinse în contextul inițierii, depunerii unei cereri de intervenție, acțiunile întreprinse de Serviciul Vamal în legătura cu cererea titularului și statutul de examinare a acesteia.

Conturul conține următoarele tipuri de notificări:
- notificare privind cererea de intervenție pregătită pentru a fi semnată electronic;
- notificare privind semnarea electronică de către titular a cererii de intervenție;
- notificare privind transmiterea cererii de intervenție către Serviciul Vamal;
- notificare privind expedierea/returnarea cererii de intervenție pentru modificări, corectări, completări;
- notificare privind inspectorul vamal asignat;
- notificare privind acceptarea cererii de intervenție;
- notificare privind refuzarea cererii de intervenție;
- notificare privind anularea cererii de intervenție;
- notificare privind suspendarea cererii de intervenție;
- notificare privind expirarea cererii de intervenție.

12.5. Conturul funcțional „**INCIDENTE**", permite reprezentantului Serviciului Vamal raportarea unor incidente, probleme apărute în procesul de utilizare a sistemului informațional.

Incidentele raportate sunt clasificate în următoarele tipuri:
- Cerință tehnică anterior nedefinită;
- Cerință tehnică neimplementată (eroare logică);
- Îmbunătățire minoră de utilizare;
- Eroare de soft ce determină funcționarea inadecvată a sistemului (bug);
- Solicitare de clarificare;
- Solicitare de suport tehnic;
- Solicitare de training.

La fel, în cadrul conturului funcțional titularul are posibilitatea de a căuta un anumit incident, în baza unor parametri dinamici, precum și de a monitoriza statutul incidentului raportat:
- Depus;
- În progres;
- În proces de testare;
- Suspendat;
- Anulat;
- Soluționat.

Capitolul IV
SPAȚIUL ORGANIZAȚIONAL AL SI e-RCI

13. Funcțiile de bază privind formarea și exploatarea SI e-RCI sunt divizate între:
1) Posesorul sistemului;
2) Deținătorul sistemului;
3) Operatorul tehnico-tehnologic;
4) Utilizatorii sistemului.

14. Posesorul și **Deținătorul** SI e-RCI este Serviciul Vamal, cu drept de gestionare şi de utilizare a datelor şi a resurselor conținute de acesta, precum și cu responsabilitățile de asigurare a creării și exploatării eficiente a acestui sistem.

15. Operatorul tehnico-tehnologic al SI e-RCI este IP „Serviciul Tehnologia Informației și Securitate Cibernetică”, care asigură mentenanța și administrarea tehnică a sistemului conform legislaţiei.

16. Utilizatori ai SI e-RCI sunt titularii de drepturi și Serviciul Vamal.

Capitolul V
SPAŢIUL TEHNOLOGIC AL SI e-RCI

17. Arhitectura SI e-RCI este proiectată a fi una deschisă, modulară și bazată pe componente integrate, care asigură posibilitatea dezvoltării sale fără a afecta continuitatea funcționării. Aceste principii sunt aplicabile și se regăsesc la toate nivelele arhitecturii sistemului.

18. Arhitectura SI e-RCI este orientată spre servicii (SOA, Service Oriented Architecture) și este constituită din 3 nivele:

1) *Nivelul de prezentare*, nivel superior care reprezintă interfața grafică de prezentare pentru utilizator (GUI, Graphical User Interface). Rolul interfeței de prezentare este de a transpune sarcinile și rezultatele într-o formă inteligibilă utilizatorului;

2) *Nivelul de business-logică*, nivel de mijloc care este responsabil pentru accesarea, procesarea și transformarea datelor, gestionează Business-regulile și asigură coerența și precizia datelor. Nivelul de Business-Logică este accesat din nivelul de prezentare pentru a face ca funcționalitățile să fie disponibile utilizatorilor și poate oferi funcționalitățile sistemelor informatice externe prin intermediul interfețelor de schimb de date;

3) *Nivelul de date*, nivel inferior, unde toate informațiile stocate sunt preluate dintr-o bază de date sau un sistem de fișiere. Informația este ulterior transmisă către nivelul logic pentru procesare și ulterior, eventual înapoi către utilizator. Baza de date și datele sunt implementate utilizând sistemul de gestionare a bazelor de date relaționale (DBMS).

19. Caracteristici ale nivelului de prezentare:

a) Utilizatorul va folosi un browser web pentru a accesa toate funcționalitățile și datele SI e-RCI pentru care este autorizat. Sistemul este compatibil cu cel puțin 2 versiuni recente ale următoarelor browser-e web: Microsoft Internet Explorer, Microsoft Edge, Mozila Firefox, Google Chrome, Safari;

b) Sistemul implementează interfața web HTML5 și utilizează doar browser-ul web;

c) Nivelul de prezentare nu implementează reguli de business-logică, cu excepția validării intrărilor de date.

20. Caracteristici ale nivelului de business-logică:

a) Nivelul de business-logică este complet independent de nivelul de prezentare și de aplicațiile externe care utilizează interfețe de schimb de date;

b) Are o arhitectură complet modulară bazată pe componente reutilizabile și interfețe abstracte. Nu trebuie să existe funcții identice realizate de diferite componente;

c) Conține și delimitează expres componentele de „business workflow" și „business entity".

d) Accesul la componentele de „business entity" se va realiza prin intermediul componentelor de „business workflow”. Componentele de „business entities” trebuie să fie definite în mod clar la nivelul de business-logică;

e) Componentele de „business entity" conțin toate datele și business-logica legată de „business entity", pentru desfășurarea business-operațiunilor, punerea în aplicare a business-normelor relevante și pentru menținerea integrității și acurateței datelor conținute;

f) Componentele legate de nivelul de business-logică comunică prin interfețe dedicate/funcții interne (cuplaj strâns);

g) Componentele nivelul de business-logică sunt accesibile pentru aplicații externe numai prin intermediul interfețelor de schimb de date;

h) Arhitectura nivelulului de business-logică permite accesul simultan la funcționalitățile sistemului.

21. Caracteristici ale nivelului de date:

a) Modelul de date implementat la nivelul de date al sistemului se raportează la cel puțin forma a treia-normală pentru proiectarea bazei de date, pentru a reduce duplicarea datelor și asigurarea integrității referențiale;

b) Modelul de date al sistemului urmează modelul comun de modelare a datelor (Common Data Modeling) cu ajutorul a unui Model de date comun care constă din tipuri generice de entități cum ar fi clasa, relațiile și altele;

c) Datele din nivelul de date sunt accesate numai prin intermediul nivelului de Business-Logic și independent de nivelul de Business-Logic;

d) Modelul de date implementat la nivelul de date este corect documentat. Documentația trebuie să conțină atât descrierea tehnică a datelor (de exemplu, diagrame de relații ale entităților, structuri de baze de date, obiecte din baze de date etc.) și descrierea semantică (asocierea structurilor de date cu business-entitățile și proprietățile acestora). Descrierea semantică trebuie să fie disponibilă pentru utilizatori, unde este posibil (de exemplu, personalizarea rapoartelor);

e) Nivelul de date asigură integritatea și precizia datelor (integritatea tranzacției).

22. Platforma tehnologică a SI e-RCI este alcătuită din totalitatea de componente software necesare pentru a asigura mediul de funcționare a sistemului, care vor include: platforme de dezvoltare software, sistem de gestionare a bazelor de date, sisteme de operare.

Sistemul e-RCI va fi găzduit în Platforma tehnologică guvernamentală comună MCloud.

23. Implementarea sistemului trebuie să respecte standarde deschise și să utilizeze tehnologii bine-cunoscute și general acceptate. Astfel, trebuie îndeplinite următoarele cerințe:

a) Sistemul în întregime urmează să fie bazat pe tehnologii web, standarde și tehnologii cum ar fi arhitectura software bazată pe servicii (Service Oriented Architecture - SOA), protocoale de comunicare bazate pe XML (SOAP și XML-RPC), TLSSSL etc.;

b) Interfețele de aplicații trebuie să se bazeze pe standarde deschise (REST, HTML,SOAP). Interfețele aplicației vor permite o cuplare slabă cu sisteme informatice externe (de exemplu, comunicarea bazată pe mesaje);

c) Toate interfețele aplicației implementate în Sistemul e-RCI trebuie să fie documentate corespunzător (de exemplu, utilizând limbajul de descriere a serviciilor web - WSDL);

d) Platforma tehnologică pentru software va fi independentă de platforma tehnologică hardware (adică trebuie să funcționeze pe cel puțin două tipuri de procesoare de la diferiți producători);

e) Platforma tehnologică pentru software va fi maxim omogenă (adică trebuie să conțină un număr minim de tehnologii diferite, de exemplu aceleași sisteme de operare pentru middleware și baze de date);

f) Platforma tehnologică pentru software va sprijini crearea, modificarea, prelucrarea, stocarea și accesarea datelor textuale în formatul Unicode;

g) Toate componentele sistemului (de exemplu, middleware, baze de date) trebuie să funcționeze pe o platformă cu sisteme de operare Windows Server sau Linux care sunt sprijinite în MCloud. Versiunile acceptate ale sistemelor de operare trebuie să fie menținute de producători și trebuie să aparțină ultimelor 2 versiuni majore.

24. SI e-RCI va integrat cu următoarele servicii electronice guvernamentale:

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

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

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

25. Interacțiunea SI e-RCI cu resursele informaționale externe este realizată prin intermediul platformei de interoperabilitate (**MConnect**).

CAPITOLUL VI
ASIGURAREA SECURITĂŢII INFORMAŢIONALE A SISTEMULUI

26. Prin securitatea informațională se subînțelege starea de protecție a sistemului la etapele procesului de creare, procesare, stocare și transmitere a datelor de la acțiuni accidentale sau intenționate cu caracter natural sau artificial, care au drept scop crearea prejudiciului participanților în procesul de schimb informațional.

27. Sistemul complex al securității informatice reprezintă totalitatea mijloacelor legislative, organizatorice și economice precum și a mijloacelor tehnologice și metodelor de protecție software-hardware și criptografică a informației, orientate spre asigurarea unui nivel necesar de integritate, confidențialitate și accesibilitate a resurselor informaționale.

28. Principalele sarcini ale asigurării securității informaționale sunt:

a) asigurarea integrității informației – menținerea și asigurarea exactității și integrității datelor pe parcursul întregului ciclu de viață, protecția împotriva modificării sau ștergerii datelor;

b) asigurarea confidențialității – protecția împotriva accesului neautorizat la date;

c) asigurarea disponibilității accesibilității – protecția împotriva blocării accesului utilizatorilor autorizați la resursele informaționale.

29. În scopul asigurării securității informaționale SI e-RCI, va sprijini următoarele mecanisme:

a) *Autentificare*: Garantează faptul că zonele restricționate ale serviciului sunt accesibile numai utilizatorilor cu identitatea verificată prin MPass;

b) *Autorizare*: Garantează că utilizatorii autentificați pot accesa numai serviciile și datele care corespund rolurilor și drepturilor de acces ale acestora;

c) *Confidențialitate*: Garantează că datele schimbate între persoana care o solicită și furnizorul nu pot fi interceptate sau accesate de o terță parte neautorizată și că datele nu pot fi accesate într-un moment necorespunzător;

d) *Integritate*: Garantează că fluxul de date realizat între solicitant și furnizor nu a fost modificat sau manipulat de o terță parte neautorizată sau datele nu au fost accesate înainte de un termen anumit sau un timp anumit;

e) *Non-repudiere*: Măsură prin care se asigură faptul că, după emiterea/recepționarea unei informații, expeditorul/destinatarul nu poate nega, în mod fals, că a expediat/primit informații;

f) *Înregistrarea și monitorizarea acțiunilor utilizatorilor sistemului*: pentru a detecta într-o etapă incipientă încercarea de a accesa date confidențiale sau de a afecta intenționat sau accidental integritatea informației prin MLog;

g) Auditul IT;

h) Criptarea informațiilor;

i) *Continuarea activității și recuperarea în caz de dezastru*;

j) *Mentenanță*: Sistemul trebuie asigurat în permanență cu suportul și mentenanța necesară conform nivelului agreat de servicii (SLA).

30. Pentru a atinge aceste obiective de asigurare a securității informaționale, SI e-RCI va oferi câteva mecanisme de securitate:

a) *Firewall-uri*: Firewall-urile fac parte din arhitectura tehnică a sistemului pentru a oferi o linie de apărare atunci când utilizatorii externi încearcă să se conecteze la sistem de pe Internet sau dintr-o altă rețea. Firewall-urile trebuie să fie configurate astfel încât să permită numai serviciile de rețea absolut necesare și protocoalele pentru operarea sistemului. Nu pot fi activate servicii și/sau protocoale adiționale (principiul privilegiilor minime). De asemenea, acestea trebuie să sprijine reluarea în caz de nereușită (failover) pentru asigurarea unui nivel de disponibilitate ridicată. Acest mecanism se va asigura prin utilizarea platformei MCloud;

b) *Antivirus / Anti-spam*: Soluțiile hardware și / sau software / hardware trebuie să asigure protecție antivirus și anti-spam pentru toate serverele. Fișierele vor fi scanate în timp ce se încarcă în sistem. În cazul în care un fișier infectat este depistat, procedura de încărcare va fi stopată, iar fișierul va fi respins. Sistemul trebuie să fie configurat să actualizeze zilnic automat definițiile în timpul orelor nelucrătoare. Acest mecanism se va asigura prin utilizarea platformei MCloud;

c) *Sistem de detectare a intruziunilor*: Sistemul de detectare a intruziunilor va include toți agenții necesari pentru toate serverele. Acest mecanism se va asigura prin utilizarea platformei MCloud;

d) *Comunicații securizate (transfer de date) între serverele web și utilizatori*: Schimbul de informații sensibile urmează a fi securizat în mod corespunzător. În acest context, urmează a fi utilizat un protocol securizat, cum ar fi HTTPS, pentru a evita accesul neautorizat la datele transmise. Acest protocol securizat trebuie să fie utilizat în mod consistent pe toate site-urile sistemului, excluzând posibilitatea transmiterii necriptate a informației. În caz contrar, utilizatorii ar putea fi expuși la mai multe tipuri de atacuri. În mod ideal, site-ul Web ar trebui să posede proprietatea de "securitate perfectă" („forward secrecy");

e) *Copierea de rezervă sistematică a datelor stocate*: Permite recuperarea rapidă și fiabilă a datelor în cazul unor incidente care are ca rezultat pierderea sau deteriorarea datelor. Acest mecanism se va asigura prin utilizarea platformei MCloud;

f) *Criptarea datelor*: Toate datele stocate în diferitele componente ale sistemului (i.e. servere, stocare de date, LDAP) vor fi criptate;

g) *Certificate digitale*: Sistemul va utiliza certificatele digitale pentru a asigura principiile integrității și non-repudiere. Acest mecanism este asigurat prin integrarea cu MSign și MPass;

h) *Abilitatea de auditare a acțiunilor realizate*: Toate activitățile efectuate de utilizatori, fie cu succes sau nu (cum ar fi încercările de logare nereușită), vor fi monitorizate și înregistrate în jurnalele cu acces limitat a sistemului. Acest mecanism este asigurat prin integrarea cu MLog.

31. Adițional, sistemul va include și alte instrumente conceptuale de securitate, în special:

a) Arhitectura tehnică securizată: Sistemul va implementa cel puțin o arhitectură pe trei niveluri (bază de date, aplicații și nivelul de prezentare), fiind împărțită în diferite zone de securitate și va conține cel puțin un DMZ și o zonă internă;

b) Controalele de securitate încorporate în sistem: De exemplu, rolurile utilizatorilor cu drepturi de acces predefinite, principiul "patru ochi" pentru luarea deciziilor cheie, validarea datelor la introducere, etc.;

c) Mecanismul de marcare temporală: Asigură înregistrarea timpului tuturor tranzacțiilor din cadrul sistemului;

d) Respectarea Cerințelor minime obligatorii de securitate cibernetică, aprobate prin Hotărârea Guvernului nr.201/2017.

32. Organizarea sistemului de protecție a datelor cu caracter personal constituie o parte componentă a mecanismului de asigurare a securității informaționale a SI e-RCI. Sistemul de protecție a datelor cu caracter personal se constituie în baza:

a) raportului privind rezultatele efectuării auditului intern;

b) listei datelor cu caracter personal care trebuie să fie protejate;

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

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

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

f) documentelor de reglementare şi politicilor de securitate elaborate.

CAPITOLUL VII
CONCLUZII

33. Implementarea SI e-RCI va conduce la îmbunătățirea procesului de comunicare dintre titularul de drepturi și Serviciul Vamal, va optimiza și transparentiza procesul și acțiunile de asigurare a nivelului adecvat de protecție pentru obiectele de proprietate intelectuală, va permite recunoașterea încălcărilor şi încurajarea titularilor drepturilor de proprietate intelectuală să-şi apere drepturile, astfel oferind un mecanism statistic pentru monitorizarea eficienței activităților de aplicare în domeniu protecției drepturilor de proprietate intelectuală. Efectul elaborării şi implementării SI e-RCI va putea fi observat începînd cu etapa introducerii în exploatare experimentală, deși impactul complet se va manifesta în întregime pe parcurs.

Neimplementarea SI e-RCI poate avea un impact negativ substanțial în domeniul asigurării implementării adecvate a mecanismelor de protecție a drepturilor de proprietate intelectuală, determinat de calitatea insuficientă a intervențiilor și acțiunilor întreprinse de Serviciul Vamal în acest sens.