

**GUVERNUL REPUBLICII MOLDOVA**

H O T Ă R Î R E

nr. \_\_\_\_\_ din \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017

**cu privire la aprobarea Conceptului tehnic al Sistemului informaţional automatizat naţional de informare și comunicare pentru supravegherea pieţei**

În temeiul prevederilor Legii nr. 7 din 26 februarie 2016 privind supravegherea pieței în ceea ce privește comercializarea produselor nealimentare (Monitorul Oficial al Republicii Moldova, 2016, nr.79-89, art.146), Guvernul

**HOTĂRĂŞTE**:

1. Se aprobă Conceptul tehnic al Sistemului informaţional automatizat naţional de informare și comunicare pentru supravegherea pieţei, se anexează.

2. Controlul asupra executării prezentei hotărîri se pune în sarcina Ministerului Economiei și Infrastructurii.

**Prim-ministru PAVEL FILIP**

Contrasemnează:

Viceprim-ministru,

ministrul economiei

și infrastructurii Octavian CALMÎC

Anexă

Hotărîrea Guvernului nr. \_\_\_ din\_\_\_\_\_\_\_\_\_ 2017

**CONCEPTUL TEHNIC**

**al Sistemului informaţional automatizat**

**naţional de informare și comunicare pentru supravegherea pieţei**

**INTRODUCERE**

Conceptul tehnic al Sistemului informaţional automatizat naţional de informare și comunicare pentru supravegherea pieţei (în continuare – Concept) specifică cerințele de bază privind Sistemul informaţional automatizat naţional de informare și comunicare pentru supravegherea pieţei (în continuare –*SIA NICSP*), precum destinația și scopul creării acestuia, funcţiile de bazăa sistemului, obiectele sistemului, structura resurselor informaţionale, infrastructura informaţională a sistemului, cerinţele de bază privind furnizarea informațiilor și preluarea acestora între autoritățile de supraveghere a pieței și organul vamal în cadrul activităților de supravegherea pieței privind comercializare produselor nealimentare,cerinţele cu privire la securitatea şi protecţia informaţiilor și este elaborat în conformitate cu Reglementarea tehnică RT 38370656-002:2006 „Procesele ciclului de viaţă al software-ului”, aprobată prin ordinul Ministerului Tehnologiei Informaţiei şi Comunicaţiilor nr.78 din 1 iunie 2006.

**Capitolul I**

**INFORMAŢII GENERALE**

**1. Dispoziţii generale**

Registrul de stat format de *SIA**NICSP*, cuprinde date sistematizate referitoare la: înregistrarea, păstrarea, prelucrarea şi utilizarearegistrelor de informaţii cu privire la agenții economici, autoritățile de supraveghere a pieței privind comercializarea produselor nealimentare, documente aferente controalelor, prescripții și notificări de interzicerea punerii la dispoziție pe piață, retragerea de pe piață și rechemare de la consumatori a produselor nealimentare care:

1. nu corespund cerințelor esențiale;
2. prezintă un risc grav;
3. nu corespund cerinţelor esenţiale şi, în acelaşi timp, prezintă un risc grav.

**2. Definiții**

În sensul prezentului Concept, noţiunile și termenii utilizați semnifică următoarele:

*concept*– document tehnic, reglementat de Regulamentul tehnic RT 38370656-002:2006 „Procesele ciclului de viaţă al software-ul”, care descrie ideologia creării și funcționării sistemului informaţional automatizat;

*eveniment*– scenariu de comportament al obiectului informaţional luat în evidență în Sistemul informaţional automatizat. Lista evenimentelor cuprinde întreg ciclul de viaţă al obiectului informațional, începînd cu înregistrarea iniţială şi finalizînd cu scoaterea din evidenţă și arhivarea corespunzătoare;

S*istemul informaţional automatizat naţional de informare și comunicare pentru supravegherea pieţei*– totalitate a mijloacelor software şi hardware, a echipamentelor şi reţelelor de comunicaţii electronice care asigură funcţionarea *SIA**NICSP*;

*produs periculos, risc grav* – în sensul Legii nr. 422-XVI din 22 decembrie 2006 privind securitatea generală a produselor;

*distribuitor, agent economic, cerințe esențiale,introducere pe piaţă, importator, legislație comunitară de armonizare, marcaj CE, producător, punere la dispoziţie pe piaţă, reprezentant autorizat*– în sensul Legii nr. 235 din 1 decembrie 2011 privind activităţile de acreditare şi de evaluare a conformităţii;

*colaborator vamal, punerea în liberă circulaţie, regim vamal* – în sensul Codului vamal al Republicii Moldova nr. 1149-XIV din 20 iulie 2000;

*sistem informational* – în sensul Legii nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat;

*autorităţi de supraveghere a pieţei,controlul caracteristicilor produselor (controlul produselor)*, *examinarea mostrelor de produse, inspector, identificarea produselor, monitorizarea pieţei, prescripţie, produs, program sectorial, rechemare, retragere, supraveghere a pieţei,*în sensul Legii nr. 7 din 26.02.2016 privind supravegherea pieței în ceea ce privește comercializarea produselor nealimentare;

*documente aferente controalelor–* toate documentele ce ţin de realizarea controlului, inclusiv: graficul controalelor planificate, decizia de control, decizia de prelungire a termenului de control, delegaţia de control, mandatul de control, prescripţia privind înlăturarea încălcărilor, prescripţia repetată, decizia de aplicare a sancţiunii, actele de control, procesele-verbale întocmite în cadrul controlului, explicaţiile persoanelor supuse controlului, contestaţiile acestor persoane, deciziile instanţelor de judecată în privinţa controalelor*.*

*grafic al controalelor planificate–* lista persoanelor fizice şi/sau juridice care practică activitate de întreprinzător şi al căror control a fost programat pe parcursul unui trimestru*.*

**3. Destinaţia Sistemului informaţional automatizat**

SIANICSP este destinat pentru a sprijini, în regim automatizat, măsurile de supraveghere a pieţeiîn ceea ce priveștecomercializarea produselor nealimentare, acesta fiind compatibil cu Sistemul informaţional automatizat „Registrul de stat al controalelor”. SIANICSP va asigura autoritatea de coordonare a activităţilor de supraveghere a pieţeicu un instrument eficient și centralizat pentru monitorizarea activităţilor desfăşurate şi măsurilor aplicate de autorităţile de supraveghere a pieţei în cooperare cu organului vamal pentru a asigura că produsele sînt conforme cu cerinţele esenţiale aplicabile sau că nu pun în pericol sănătatea, siguranţa ori alte aspecte ce țin de protecţia intereselor publice.

**4. Scopurile şi sarcinile SIA NICSP**

1. Scopurile SIA NICSP
2. Scopul primordial este asigurareacu o soluţie informatică performantă utilizată ca suport pentru automatizarea activităţii în vederea implementării prevederilor cadrului legal privind supravegherea pieţei în ceea ce priveștecomercializarea produselor nealimentare;
3. sprijinirea, în regim automatizat a măsurilor corective de supraveghere a piețeiîn ceea ce priveștecomercializarea produselor nealimentare;
4. organizarea interacţiunii eficiente şi a schimbului de informaţii prin utilizarea sistemelor informaționale dintre autoritățile de supraveghere a pieței și organul vamal;
5. colectarea şi prelucrarea operativă a informaţiilor privind trasabilitatea produselor nealimentare, suspendarea temporară, interzicerea punerii la dispoziție pe piață a produselor, retragerea produselor de pe piață și rechemare produselor de la consumatori;
6. evidența statistică şi analitică privind activităţile desfăşurate şi măsurile aplicate de autorităţile de supraveghere a pieţei;
7. SIA“N”ICSPare următoarele sarcini:
8. asigurarea înregistrării şi prelucrării tuturor informaţiilor  privind activităţile desfăşurate şi măsurile aplicate de autorităţile de supraveghere a pieţei;
9. transmiterea notificărilor de suspendare a punerii în liberă circulație și a datelor asociate de către organul vamal şi evidenţa informaţiilor cu privire la rezultatele și timpii de reacție a intervenţiei autorităților de supraveghere a pieței pentru fiecare eveniment;
10. asigurarea interacţiunii informaţionale cu sistemele informaţionale de stat, departamentale, teritoriale, în special cu Registrul de stat al populaţiei, Registrul de stat al unităţilor de drept, Sistemul informațional automatizat “Registrul de Stat a Controalelor”, Sistem Informațional Integrat Vamal ASYCUDA World;
11. controlul accesului la date și asigurarea securităţii informaţionale la formarea şi exploatarea resursei informaţionale SIA NICSP.

**5. Principiile de creare a SIA NICSP**

SIA NICSP este creat în baza următoarelor principii:

1. **de consecutivitate**– elaborarea şi realizarea proiectului pe etape;
2. **de expansibilitate şi scalabilitate**– posibilitatea extinderii şi modernizării în rezultatul creşterii numărului de servicii prestate și activități desfașurate;
3. **de productivitate**– asigurarea nivelului necesar de productivitate şi eficacitate pentru soluţionarea sarcinilor de diferite categorii;
4. **de fiabilitate şi toleranţă la erori**– sistemul trebuie să asigure prestarea garantată a serviciilor;
5. **de deschidere a arhitecturii**– realizarea cu uşurinţă a integrării nu numai la nivel național, dar şi la nivel internaţional;
6. **principiul transparenţei** -presupune proiectarea şi realizarea, conform principiului modular, cu utilizarea standardelor transparente în domeniul tehnologiilor informatice şi de telecomunicaţii;
7. **de gestionare centralizată**– gestionarea şi controlul trebuie realizate dintr-un centru unic;
8. **de legalitate**– crearea şi exploatarea SIA NICSP în corespundere cu legislaţia în vigoare a Republicii Moldova;
9. **de protecție a datelor cu caracter personal**– datele cu caracter personal vor fi prelucrate în conformitate cu cerințele actelor normative în vigoare;
10. **de identificare de stat a obiectelor destinate înregistrării**– utilizarea numărului de identificare al SIA NICSP, atribuit fiecărui obiect informaţional;
11. **de securitate a datelor** asigurarea integrității şi confidenţialităţii informaţiei, disponibilităţii resurselor şi serviciilor informaţionale;
12. **de utilizare**a produselor program şi a mijloacelor tehnice certificate și licenţiate.

**Capitolul II
CADRUL DE REGLEMENTARE A SIA NICSP**

**6. Actele normative de reglementare a creării și funcționării SIA NICSP:**

1. Constituția Republicii Moldova din 29.07.1994;
2. Hotărîrea Parlamentului nr. 153 din 15 iulie 2011 „Pentru aprobarea Strategiei securității naționale a Republicii Moldova”;
3. Legea nr. 422-XVI din 22 decembrie 2006 privind securitatea generală a produselor;
4. Legea nr. 235 din 1 decembrie 2011 privind activităţile de acreditare şi de evaluare a conformităţii;
5. Legea nr. 105-XV din 13 martie 2003 privind protecţia consumatorilor;
6. Legea nr. 793-XIV din 10 februarie 2000 contenciosului administrative;
7. Legea nr. 171-XIII din 6 iulie 1994 cu privire la secretul comercial (Monitorul Oficial al Republicii Moldova, 1994, nr. 13, art.126);
8. Legea nr. 245-XVI din 27 noiembrie 2008 cu privire la secretul de stat (Monitorul Oficial al Republicii Moldova, 2009, nr. 45-46, art.123);
9. Legea nr. 133 din 8 iulie 2011 privind protecţia datelor cu caracter personal (Monitorul Oficial al Republicii Moldova, 2011, nr. 170-175, art.492);
10. Legea nr. 7 din 26 februarie 2016 cu privire privind supravegherea pieţei în ceea ce priveștecomercializarea produselor nealimentare;
11. Legea nr. 172 din 25iulie 2014 privind aprobarea Nomenclaturii combinate a mărfurilor;
12. Codul vamal al Republicii Moldova nr. 1149-XIV din 20 iulie 2000;
13. Hotărîrea Guvernului nr.1076 din 23 septembrie 2016 pentru aprobarea Regulamentului privind procedurile de conlucrareîntre autorităţile de supraveghere a pieţei şi Serviciul Vamal;
14. Hotărîrea Guvernului nr.1212 din 04 noiembrie 2016 „Cu privire la aprobarea Metodologiei privind evaluarea riscurilor în cazul produselor nealimentare destinate consumatorilor şi selectarea măsurilor corective”.

**7. Actele normative de bază în domeniul informatizării**

1. Legea nr. 982-XIV din 11 mai 2000 privind accesul la informaţie (Monitorul Oficial al Republicii Moldova, 2000, nr.88, art.664);
2. Legea nr. 467-XV din 21 noiembrie 2003 cu privire la informatizare şi la resursele informaţionale de stat (Monitorul Oficial al Republicii Moldova,  2004, nr. 6-12, art.44);
3. Legea nr.241-XVI din 15 noiembrie 2007comunicațiilor electronice (Monitorul Oficial al Republicii Moldova, 2008, nr. 51-54, art.155);
4. Legea nr. 71-XVI din 22 martie 2007 cu privire la registre (Monitorul Oficial al Republicii Moldova, 2007, nr.70-73, art.314);
5. Legea nr. 1069-XIV din 22 iunie 2000 cu privire la informatică (Monitorul Oficial al Republicii Moldova, 2001, nr.73-74, art.547);
6. Legea nr. 264-XV din 15 iulie 2004 cu privire la documentul electronic şi semnătura digitală (Monitorul Oficial al Republicii Moldova, 2004, nr. 132-137, art.710);
7. Hotărîrea Guvernului nr. 128 din 20 februarie 2014 privind platforma tehnologică guvernamentală comună (MCloud)
8. Hotărîrea Guvernului nr. 717 din 29 august 2014 privind platforma guvernamentală de registre și acte permissive (PGRAP);
9. Hotărîrea Guvernului nr. 735 din 11 iunie 2002 „Cu privire la sistemele speciale de telecomunicații ale Republicii Moldova”;
10. Hotărîrea Guvernului nr.1123 din 14 decembrie 2010 „Privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal”;
11. Hotărîrea Guvernului nr.710 din 20septembrie2011 „Cu privire la aprobarea Programului strategic de modernizare tehnologică a guvernării (e-Transformare)”;
12. Hotărîrea Guvernului nr.857 din 31 octombrie 2013 „Cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”;
13. Hotărîrea Guvernului nr.1090 din 31decembrie 2013 privind serviciul electronic guvernamental de autentificareşi control al accesului (MPass);
14. Hotărîrea Guvernului nr.405 din 02 iunie 2014 privind serviciul electronic guvernamental integratde semnătură electronica (MSign);
15. Hotărîrea Guvernului nr.656 din 05 septembrie 2012 cu privire la aprobarea Programului privindCadrul de Interoperabilitate;
16. Hotărîrea Guvernului nr.404 din 02 iunie 2014 cu privire la pilotarea platformei de interoperabilitate;
17. Hotărîrea Guvernului nr.708 din 28 februarie 2014 privind serviciul electronic guvernamentalde jurnalizare (MLog).

**8. Regulamentele tehnice și standardele în domeniul tehnologiei informației și comunicațiilor electronice**

1) Reglementarea tehnică RT 38370656-002:2006 „Procesele ciclului de viaţă al software-ului”, aprobată prin ordinul Ministerului Tehnologiei Informaţiei şi Comunicaţiilor nr.78 din 1 iunie 2006 (Monitorul Oficial al Republicii Moldova, 2006, nr. 95-97, art.335);

2) SM ISO/CEI 15288:2015 „Ingineria sistemelor şi software-ului. Procesele ciclului de viaţă al sistemului”;

3) SM ISO/CEI 12207:2014 „Ingineria sistemelor şi software-ului. Procesele ciclului de viaţă al software-ului”;

4) SM ISO/CEI 27002:2014 „Tehnologia informaţiei. Tehnici de securitate. Cod de bună practică pentru managementul securităţii informaţiei”;

5) SM ISO/CEI 15408-1:2014 „Tehnologia informaţiei. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informaţiei. Partea 1: Introducere şi model general”;

6) SM ISO/CEI 15408-2:2014 „Tehnologia informaţiei. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informaţiei. Partea 2: Cerinţe funcţionale de securitate”;

7) SM ISO/CEI 15408-3:2014 „Tehnologia informaţiei. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informaţiei. Partea 3: Cerinţe de asigurare a securităţii”.

**Capitolul III**

**FUNCȚIILE SIA NICSP**

**9. SIA NICSP** asigură executarea atît a funcțiilor de bază ale sistemului informațional, cît și a funcțiilor specifice, determinate de destinaţia acestuia, care sînt grupate în contururile funcționale specializate.

**10. Funcțiile de bază ale SIA NICSP**

1. Formarea resursei informaționale. Funcțiile de bază în procesul de formare a bazei de date a **SIA NICSP** sunt funcțiile de înregistrare, actualizarea datelor și scoaterea din evidenţă a obiectelor informaționale (schimbarea statutului obiectului – de ex. arhivare). Aceste funcții se execută în funcţie de îndeplinirea unor sau altor scenarii de bază:

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

b) actualizarea datelor **SIA NICSP** constă în reînnoirea sistematică a bazei de date a acestuia în cazul schimbării sau completării atributelor obiectelor de evidență;

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

d) informația se șterge fizic numai după expirarea termenului de păstrare a informației în arhiva electronică (7 ani).

Informația se introduce în **SIA NICSP** doar în baza deciziei registratorului. Toate schimbările în sistem se păstrează în ordine cronologică.

1. Organizarea suportului informațional. Informațiile din baza de date a **SIA NICSP** sunt oferite în funcție de nivelul de acces stabilit. Beneficiarii datelor din sistem sînt obligați să le folosească doar în scopuri legale.
2. Nivelul accesului utilizatorului datelor **SIA NICSP** la informația solicitată este stabilit de legislație, în funcţie de statutul său juridic și regimul juridic al informației. În cazul depistării neconcordanțelor dintre datele care se conțin în documentele emise în cadrul funcţionării **SIA NICSP** și datele din baza de date a **SIA NICSP**, informația din baza de date a **SIA NICSP** se consideră de bază.
3. Asigurarea securităţii și protecției informațiilor. Asigurarea securităţii şi protecţiei informaţiilor la toate etapele de colectare, stocare şi utilizare a resurselor informaţionale de stat care se referă la domeniul de competență al **SIA NICSP**.
4. Asigurarea calităţii informaţiei. Calitatea informaţiei se asigură prin crearea şi susţinerea componentelor sistemului de calitate, bazate pe abordarea procesuală.
5. Asigurarea multilaterală a funcţionării **SIA NICSP**.

**11. Spaţiul funcţional al SIA NICSP**

Spaţiul funcţional al **SIA NICSP** reprezintă un set de funcţii realizate de subsistemele informaționale automatizate, separate din cadrul **SIA NICSP**, care interacționează reciproc.

În cadrul funcţionării **SIA NICSP** sunt realizate următoarele funcţii specifice, grupate în contururi funcţionale:

1. Conturul funcţional privind interacţiunea informaţională a tuturor componentelor **SIA NICSP** „Administrarea şi monitorizarea acţiunilor participanților la **SIA NICSP**” reprezintă un sistem integrat de control şi monitorizare privind formarea şi utilizarea resursei informaţionale a **SIA NICSP** în domeniul supravegherii pieței privind comercializarea produselor nealimentare, precum şi a rezultatelor privind reacţionarea(notificarea) și intervențiile autorităților de supraveghere a pieței în colaborare cu organul vamal.

Acest contur include următoarele funcţii:

1) asigurarea integrităţii logice a **SIA NICSP**;

2) administrarea bazelor de date ale **SIA NICSP**;

3) delimitarea drepturilor de acces pentru utilizatori, introducerea sistemului de parole;

4) asigurarea securităţii, protecţiei şi păstrării informaţiei în sistem conform standardelor internaţionale SM ISO/CEI 27002 „Tehnologii informaţionale. Cod de bună practică pentru managementul securităţii informaţionale” şi SM ISO/CEI 15408 „Tehnologii Informaţionale. Tehnici de securitate. Criterii de evaluare pentru securitatea tehnologiei informaţiei”;

5) asigurarea respectării cerinţelor **SIA NICSP** privind protecţia datelor cu caracter personal.

1. Conturul funcţional „Autoritatea de supraveghere a pieței” include următoarele funcţii:
2. se conectează în sistem;
3. primește de la organul vamal și vizualizează notificările privind suspendarea punerii în liberă circulație(anexa nr.1 Hotărîrea Guvernului nr.1076 din 23 septembrie 2016);
4. completează formularulstandard de notificarea organului vamal:
5. privind aplicarea măsurilor corective produselor care prezintă un risc grav sau nu corespund cerințelor esențiale(anexa nr.2Hotărîrea Guvernului nr.1076 din 23 septembrie 2016);
6. reacție la notificarea de suspendare a punerii în liberă circulație în cazul produselor conforme(anexa nr.3 Hotărîrea Guvernului nr.1076 din 23 septembrie 2016);
7. reacție la notificarea de suspendare a punerii în liberă circulație în cazul produselor nesigure sau neconforme (anexa nr.4 Hotărîrea Guvernului nr.1076 din 23 septembrie 2016).
8. anexează actele necesare confirmative - importă din SIA „Registrul de stat al Controalelor” conform metalinkului documentele aferente controalelor(prescripţia (după caz) privind suspendarea temporară a punerii la dispoziţie pe piaţă / interzicerea introducerii pe piaţă a produsului/retragerea din circulaţie / rechemarea de la consumatori (utilizatori)/distrugerea produselor care prezintă un risc,procesul-verbal de control, procesele-verbale întocmite în cadrul controlului, etc);
9. anexează (importă) documente scanate în format PDF, JPG;
10. semnează notificarea și documentele anexate cu semnătura digitală și transmite notificarea prin utilizarea sistemului informațional către organul vamal;
11. primeșteînștiințare despre evenimentele notificării – expediat/livrat/acceptat/refuzat;
12. generează rapoarte statistice în conformitate cu criteriile de selectare(agent economic, grup de produse/poziția tarifară, autoritatea notificantă(postul vamal), marca comercială, țara de origine, start data/end data, motivul notificării, etc) cu delimitarea accesului la informații strict conform competențelor atribuite fiecărei autorități de supraveghere a pieței;
13. Conturul funcţional „Autoritatea de coordonare” include următoarele funcţii:
14. se conectează în sistem;
15. vizualizează notificările și documentele anexate;
16. verifică comunicările între autoritățile de supraveghere a pieței și notificările către și de la organul vamal;
17. generează rapoarte statistice în conformitate cu criteriile de selectare(autoritate de supraveghere a pieței, agent economic, grup de produse/poziția tarifară, autoritatea notificantă (postul vamal), marca comercială, țara de origine, start data/end data, motivul notificării, etc);
18. Conturul funcţional „Serviciul Vamal” include funcţiile:
19. historizarea notificărilor expediate către/de la autoritățile de supraveghere a pieței;
20. se conectează în sistem;
21. emite înștiințare de recepționare/acceptare/refuz a notificărilorde la autoritățile de supraveghere a pieței (conform anexa nr.2, nr.3 nr.4 Hotărîrea Guvernului nr.1076 din 23 septembrie 2016);
22. completează formularul standard de notificare privind suspendarea punerii în liberă circulațiea autorităților de supraveghere a pieței (anexa nr.1 Hotărîrea Guvernului nr.1076 din 23 septembrie 2016);
23. semnează notificarea și documentele anexate cu semnătura digitală și transmite notificarea prin utilizarea sistemului informațional;
24. primește și vizualizează notificările de la autoritățile de supraveghere a pieței:
25. privind aplicarea măsurilor corrective produselor care prezintă un risc grav sau nu corespunde cerințelor esențiale(anexa nr.2 Hotărîrea Guvernului nr.1076 din 23 septembrie 2016);
26. reacție la notificarea de suspendare a punerii în liberă circulație în cazul produselor conforme(anexa nr.3 Hotărîrea Guvernului nr.1076 din 23 septembrie 2016);
27. reacție la notificarea de suspendare a punerii în liberă circulație în cazul produselor nesigure sau neconforme (anexa nr.4 Hotărîrea Guvernului nr.1076 din 23 septembrie 2016)
28. generează rapoarte statistice în conformitate cu criteriile de selectare (autoritate de supraveghere a pieței, agent economic, grup de produse/poziția tarifară, autoritatea notificantă(postul vamal), marca comercială, țara de origine, start data/end data, motivul notificării, etc);

**Capitolul IV**

**STRUCTURA ORGANIZATORICĂ**

**A SIA NICSP**

**12.Posesorul SIA NICSP**

Posesorul **SIA NICSP** este Ministerul Economiei și Infrastructurii (MEC).

**13. Deţinătorul SIA NICSP**

Deţinătorul **SIA NICSP** este Ministerul Economiei și Infrastructurii.

Rolul de deţinător al sistemului reflectă aspectul administrativ şi cel tehnologic ce ţine de competenţa MEC. MEC este responsabil de buna funcţionare a Sistemului informaţional automatizat naţional de informare și comunicare pentru supraveghere a pieţei.

**14. Administratorul sistemului**

1) **SIA NICSP** va fi găzduit pe platforma tehnologică guvernamentală comună (MCloud), MEC va încheia acorduri sau contracte, după caz, cu Centrul de Guvernare Electronică (E-Government) privind prestarea serviciilor platformei tehnologice guvernamentale comune (MCloud), în baza modelelor aprobate de Cancelaria de Stat, iar administrarea sistemului va fi împărţită între Administratorul M-Cloud şi MEC. Responsabilităţile Administratorului M-Cloud vor fi reglementate de un contract SLA (Service Level Agreement) - Întreprinderea de Stat „Centrul de telecomunicaţii speciale” în calitate de operator tehnico-tehnologic al platformei tehnologice guvernamentale comune (MCloud) conform HG 128 din 20.02.2014.

2) Administratorul sistemului are acces deplin la toate funcţionalităţile sistemului, fişierele şi bazele de date aferente sistemului, încăperile în care se află echipamentul şi utilajul pe care rulează aplicaţiile software sau care asigură securitatea datelor.

3) Responsabilităţile Administratorului sînt:

a) asigurarea funcţionării normale a sistemului informatic, garantînd accesibilitatea, securitatea şi integritatea datelor;

b) gestiunea certificatelor digitale de acces a utilizatorilor (aprobare, respingere etc.);

c) monitorizează activitatea utilizatorilor în sistem;

d) la cererea în scris a proprietarului sistemului, Administratorul face modificări în funcţionalităţile sistemului (în limitele posibilităţilor admise de sistem) etc.;

e) efectuează administrarea tehnică a infrastructurii sistemului informatic care prevede:
- administrarea şi asigurarea funcţionalităţii echipamentelor tehnice pe care rulează aplicaţiile software, inclusiv cel de securizare a perimetrului reţelei şi accesului la date;

- dispunerea sau închirierea canalelor de acces în bandă largă la Internet şi reţeaua guvernamentală;

- administrarea serverului WEB de aplicaţii prin intermediul căruia se prestează serviciile incluse în sistem.

**15. Registratorii SIA NICSP**:

1. Autoritățile de supraveghere a pieței conform Anexei la Legea nr.7 din 26 februarie 2016 privind supravegherea pieţei în ceea ce priveşte comercializarea produselor nealimentare;
2. Autoritatea de coordonare (Ministerul Economiei și Infrastructurii) a activităților de supraveghere a pieței;
3. Serviciul Vamal.

**16. Furnizorii de informaţii în SIA NICSP**

Furnizorii de informaţii în **SIA NICSP**, care oferă informația ce se referă la supraveghere a pieței în ceea ce privește comercializarea produselor nealimentare, sunt:

1. Agenţia pentru Protecţia Consumatorilor și Supravegherea Pieței;
2. Agenţia pentru Supravegherea Tehnică;
3. Agenţia Navală Republicii Moldova;
4. Autoritatea din subordinea MEI responsabilă de supravegherea în domeniul transportului feroviar;
5. Serviciul Vamal;
6. Agenţia Naţională pentru Sănătate Publică;
7. Agenția Națională pentruReglementare în Comunicații Electronice și Tehnologia Informației;
8. Inspectoratul pentru Protecția Mediului.

**Capitolul V
DOCUMENTELE SIA NICSP**

**17. Documentele utilizate** în cadrul **SIA NICSP** se divizează în următoarele categorii:

*Documentele tehnologice de intrare* sunt următoarele:

1. formulare standard de notificare privind suspendarea punerii în liberă circulație;
2. actele ce confirmă necesitatea notificării;
3. formulare standard de notificare privind aplicarea măsurilor corrective produselor care prezintă un risc grav sau nu corespund cerințelor esențiale;
4. formulare standard de reacții:
5. la notificarea de suspendare a punerii în liberă circulație în cazul produselor conforme;
6. la notificarea de suspendare a punerii în liberă circulație în cazul produselor nesigure sau neconforme;
7. cererile de modificare a informaţiei;
8. actele ce confirmă necesitatea efectuării modificărilor.
9. documente scanate in format PDF, JPG.

*Documentele tehnologice de ieșire* sunt următoarele:

1. înștiințarea recepționării notificării;
2. înștiințarea recepționării reacției;
3. formulare standard de notificare a suspendării punerii la dispoziție pe piață;
4. formulare standard de notificare a interzicerii punerii la dispoziție pe piață;
5. formulare standard de notificare a retragerii de pe piață;
6. formulare standard de notificare a returnării de la consumator;
7. rapoartele statistice în format electronic;
8. notificarea (de admitere, de refuz).

*Documentele tehnologice ale sistemului*:

Din categoria documentelor tehnologice stocate în **SIA NICSP** fac parte:

1. confirmările din partea sistemelor informatice ale altor autorităţi publice sau angajaţilor acestora privind veridicitatea documentelor prezentate;
2. înregistrările fişierelor log privind interacţiunea utilizatorilor cu **SIA NICSP**;
3. certificatele digitale ale utilizatorilor care se autentifică în sistem.

**SIA NICSP** va împrumuta și utiliza informații privind documente aferente controalelor (toate documentele ce ţin de realizarea controlului, inclusiv: graficul controalelor planificate, decizia de control, decizia de prelungire a termenului de control, delegaţia de control, mandatul de control, prescripţia privind înlăturarea încălcărilor, prescripţia repetată, decizia de aplicare a sancţiunii, actele de control, procesele-verbale întocmite în cadrul controlului, explicaţiile persoanelor supuse controlului, contestaţiile acestor persoane, deciziile instanţelor de judecată în privinţa controalelor) din SIA “Registrul de stat al Controalelor”.

**Capitolul VI
RESURSA INFORMAŢIONALĂ**

**18. Obiectele informaţionale**

Resursa informaţională a **SIA NICSP** cuprinde următoarele obiecte informaţionale:

1. notificare privind aplicarea măsurilor corective produselor care prezintă un risc grav sau nu corespund cerinţelor esenţiale prin:
* interzicerea punerii la dispoziție sau a introducerii pe piață a produsului; sau
* retragereadin circulație;sau
* rechemarea produsului și avertizarea publicului în legătură cu riscul prezentat; sau
* distrugerea produselor care prezintă un risc grav, interzise definitiv pentru comercializare.
1. notificare privind suspendarea punerii în liberă circulaţie completată;
2. înștiințare de recepționare notificare/reacție;
3. înștiințare de acceptare;
4. înștiințare de refuz;
5. reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor conforme;
6. reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor nesigure sau neconforme.
7. subiecții supuși supravegherii de piață sunt persoanele juridice(obiect împrumutat din Registrul de stat al unităţilor de drept);
8. evenimentul (obiect informaţional intrasistemic).

**19. Identificarea obiectelor informaţionale**

Identificarea obiectelor informaționale se efectuează prin utilizarea numărului de identificare unic pentru fiecare obiect al **SIA NICSP** în parte:

1. identificator al obiectului informaţional *„notificare privind suspendarea punerii în liberă circulaţie completată”* este numărul de identificare care are următoarea structură:

YY NNNNNN, unde:

YY – ultimele două cifre ale anului în care a fost înregistrată notificarea;

NNNNNNN – numărul de ordine al înregistrării în **SIA NICSP** în anul respectiv.

Numărul în cauză este generat în mod automat în **SIA NICSP** şi este atribuit fiecărei notificări privind suspendarea punerii în liberă circulaţie completată;

1. identificator al obiectului informaţional *„notificare privind aplicarea măsurilor corective produselor care prezintă un risc grav sau nu corespunde cerinţelor esenţiale”*este numărul de identificare care are următoarea structură:

YY NNNNNN, unde:

YY – ultimele două cifre ale anului în care a fost înregistrată notificarea;

NNNNNNN – numărul de ordine al înregistrării în **SIA NICSP** în anul respectiv.

Numărul în cauză este generat în mod automat în **SIA NICSP** şi este atribuit fiecărei notificări privind suspendarea punerii în liberă circulaţie completată;

1. identificator al obiectului informaţional *„înștiințare de recepționare notificare/reacție*” este numărul de identificare care are următoarea structură:

YY NNNNNN, unde:

YY – ultimele două cifre ale anului în care a fost înregistrată înștiințarea;

NNNNNNN – numărul de ordine al înregistrării în **SIA NICSP** în anul respectiv.

Numărul în cauză este generat în mod automat în **SIA NICSP** şi este atribuit fiecărei notificări privind suspendarea punerii în liberă circulaţie completată;

1. identificator al obiectului informaţional *„înștiințare de acceptare”* este numărul de identificare care are următoarea structură:

YY NNNNNN, unde:

YY – ultimele două cifre ale anului în care a fost înregistrată înștiințarea;

NNNNNNN – numărul de ordine al înregistrării în **SIA NICSP** în anul respectiv.

Numărul în cauză este generat în mod automat în **SIA NICSP** şi este atribuit fiecărei notificări privind suspendarea punerii în liberă circulaţie completată

1. identificator al obiectului informaţional *„înștiințare de refuz”* este numărul de identificare care are următoarea structură:

YY NNNNNN, unde:

YY – ultimele două cifre ale anului în care a fost înregistrată înștiințarea;

NNNNNNN – numărul de ordine al înregistrării în **SIA NICSP** în anul respectiv.

Numărul în cauză este generat în mod automat în **SIA NICSP** şi este atribuit fiecărei notificări privind suspendarea punerii în liberă circulaţie completată;

1. identificator al obiectului informaţional *„reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor conforme”* este numărul de identificare care are următoarea structură:

YY NNNNNN, unde:

YY – ultimele două cifre ale anului în care a fost înregistrată reacție;

NNNNNNN – numărul de ordine al înregistrării în **SIA NICSP** în anul respectiv.

Numărul în cauză este generat în mod automat în **SIA NICSP** şi este atribuit fiecărei notificări privind suspendarea punerii în liberă circulaţie completată;

1. identificator al obiectului informaţional *„reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor nesigure sau neconforme”* este numărul de identificare care are următoarea structură:

YY NNNNNN, unde:

YY – ultimele două cifre ale anului în care a fost înregistrată reacție;

NNNNNNN – numărul de ordine al înregistrării în **SIA NICSP** în anul respectiv.

Numărul în cauză este generat în mod automat în **SIA NICSP** şi este atribuit fiecărei notificări privind suspendarea punerii în liberă circulaţie completată;

1. identificator al obiectului informaţional *„persoană fizică”* este numărul de identificare de stat al persoanei fizice din Registrul de stat al populaţiei (IDNP);
2. identificator al obiectului informaţional *„persoană juridică”* este numărul de identificare de stat al unităţii de drept din Registrul de stat al unităţilor de drept (IDNO);
3. identificator al obiectului informaţional *„eveniment”,* format din:„data” + „numărul de ordine”.

**20. Scenariile de bază**

Scenariile de bază reprezintă o listă de evenimente ce se produc cu obiectul informaţional şi se ţin în evidenţă în **SIA NICSP**. Acestea se divizează în două grupe: prima – introducerea, actualizarea şi scoaterea obiectelor informaţionale din evidenţă, a doua – furnizarea informaţiei:

1. la obiectul informațional „*notificare privind aplicarea măsurilor corective produselor care prezintă un risc grav sau nu corespunde cerinţelor esenţiale*”:
2. inspectorul autorității de supraveghere a pieței se autentifică în **SIA NICSP** prin nume de utilizator și parolă și/sau utilizează serviciul MPass pentru autentificare şi acces în sistem;
3. completează formularul standard „*notificare privind aplicarea măsurilor corective produselor care prezintă un risc grav sau nu corespunde cerinţelor esenţiale*”, conform anexei nr.2 la Hotărîrea Guvernului nr.1076 din 23 septembrie 2016;
4. anexează documente privind măsurile aplicate și motivul notificării;
5. semnează notificarea și documentele anexate cu semnătura digitală și transmite notificarea prin utilizarea sistemului informațional;
6. **SIA NICSP** va genera automat un număr unic al notificării și va înregistra data creării evenimentului;
7. organul vamal va primi, prin sistem înștiințarea privind notificarea nouă înregistrată în sistem.
8. la obiectul informațional *„notificare privind suspendarea punerii în liberă circulaţie completată”:*
9. colaboratorulorganului vamal se autentifică în **SIA NICSP** prin nume de utilizator și parolă și/sau utilizează serviciul MPass pentru autentificare şi acces în sistem;
10. completează formularul standard „*notificarea privind suspendarea punerii în liberă circulaţie*”, conform anexei nr.1 la Hotărîrea Guvernului nr.1076 din 23 septembrie 2016
11. anexează documente privind motivul notificării;
12. semnează notificarea și documentele anexate cu semnătura digitală și transmite notificarea prin utilizarea sistemului informațional;
13. **SIA NICSP** va genera automat un număr unic al notificării și va înregistra data creării evenimentului;
14. autoritatea de supraveghere a pieței va primi, prin sistem înștiințarea privind notificarea nouă înregistrată în sistem.
15. la obiectul informațional „*înștiințare de recepționare notificare/reacție*”:

**SIA NICSP** în baza soluțiilor de notificare interne și prin intermediul platformei de interoperabilitate MConect va asigura înregistrarea în baza de date a evenimentelor și transmiterea înștiințarilor de recepționare notificare/reacție de către și către utilizatorii sistemului din cadrul autorităților de supraveghere a pieței și a organului vamal;

1. la obiectul informațional „*înștiințare de acceptare*”:
2. colaboratorulorganului vamal se autentifică în **SIA NICSP** prin nume de utilizator și parolă și/sau utilizează serviciul MPass pentru autentificare şi acces în sistem;
3. colaboratorul organului vamal va verifica plenitudinea datelor și va întreprinde acțiuni de acceptanță a notificarării de la autoritățile de supraveghere a pieței;
4. sistemul va transmite cu aplicarea semnăturii digitale a colaboratoruluiorganului vamalînștiintarea despre acceptare către autoritatea de supraveghere a pieței notificantă;
5. autoritatea de supraveghere a pieței va primi, prin soluțiile de notificare a sistemuluiînștiințarea de acceptare înregistrată în sistem.
6. la obiectul informațional „*înștiințare de refuz*”:
7. colaboratorul organului vamal se autentifică în **SIA NICSP** prin nume de utilizator și parolă și/sau utilizează serviciul MPass pentru autentificare şi acces în sistem;
8. în cazul în care colaboratorul organului vamal va stabili lipsa de informații cu privire la produs/lotul de produse sau dacă notificarea nu este îndeplinită corect, va întreprinde acțiuni de înștiințare a autorității de supraveghere despre aceasta și despre faptul că notificarea a fost respinsă;
9. sistemul va transmite înștiintarea cu aplicarea semnăturii digitale a colaboratorului organului vamal despre refuz către autoritatea de supraveghere a pieței notificantă;
10. autoritatea de supraveghere a pieței va primi, prin soluțiile de notificare a sistemului înștiințarea de refuz înregistrată în sistem.
11. la obiectul informațional „*reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor conforme*”:
12. inspectorul autorității de supraveghere a pieței se autentifică în **SIA NICSP** prin nume de utilizator și parolă și/sau utilizează serviciul MPass pentru autentificare şi acces în sistem;
13. completează formularul standard „*reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor conforme*”, conform anexei nr.3 la Hotărîrea Guvernului nr.1076 din 23 septembrie 2016;
14. anexează documente privind motivul notificării;
15. semnează reacția la notificare și documentele anexate cu semnătura digitală și transmite formularul de reacție la notificare prin utilizarea sistemului informațional;
16. **SIA NICSP** va genera automat un număr unic al reacției și va înregistra data creării evenimentului;
17. organul vamal va primi, prin sistem înștiințarea privind *„reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor conforme” nouă* înregistrată în sistem.
18. la obiectul informațional *„reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor nesigure sau neconforme”:*
19. inspectorul autorității de supraveghere a pieței se autentifică în **SIA NICSP** prin nume de utilizator și parolă și/sau utilizează serviciul MPass pentru autentificare şi acces în sistem;
20. completează formularul standard *„reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor nesigure sau neconforme”*,conform anexei nr.4 la Hotărîrea Guvernului nr.1076 din 23 septembrie 2016;
21. anexează documente privind măsurile aplicate pentru interzicerea întroducerii pe piață și indică rezoluția “Produs periculos – nu se autorizează punerea în liberă circulație”/”Produs neconform - nu se autorizează punerea în liberă circulație” în cazul în care produsele sînt plasate într-un regim vamal diferit de cel care prevede punerea lor în liberă circulație;
22. semnează reacția la notificare și documentele anexate cu semnătura digitală și transmite formularul de reacție la notificare prin utilizarea sistemului informațional;
23. **SIA NICSP** va genera automat un număr unic al reacției și va înregistra data creării evenimentului;
24. organul vamal va primi, prin sistem înștiințarea privind *„reacție la notificarea de suspendare a punerii în liberă circulaţie în cazul produselor nesigure sau neconforme”* nouă înregistrată în sistem.

**21. Clasificatoarele**

În vederea asigurării veridicităţii şi reducerii volumului informaţiei păstrate în **SIA NICSP**, precum şi pentru o clasificare corectă a obiectelor în acesta, se utilizează sistemul de clasificatoare elaborate în baza clasificatoarelor naţionale ale Republicii Moldova şi a directivelor europene:

a) clasificatoarele internaţionale;

b) clasificatoarele naţionale ale Republicii Moldova;

c) clasificatoarele intrasistemice, elaborate în baza clasificatoarelor internaţionale, a clasificatoarelor naţionale ale Republicii Moldova şi a directivelor europene.

Astfel, se vor folosi cel puţin următoarele clasificatoare naţionale:

CUATM – clasificatorul unităţilor administrativ-teritoriale;

CTP – clasificatorul tipurilor de proprietate;

CFOJ – clasificatorul formelor organizaţional-juridice ale agenţilor economici;

CAEM-2 – clasificatorul activităţilor economice;

Clasificatoarele intrasistemice se elaborează şi se utilizează în cadrul **SIA NICSP** doar în cazurile absenţei clasificatoarelor naţionale şi internaţionale aprobate.

**22. Interacţiunea cu alte sisteme informaţionale**

Pentru asigurarea formării corecte a resursei informaţionale **SIA NICSP** va fi necesară organizarea accesului la resursele informaţionale a următoarelor sisteme informaţionale automatizate:

1. Serviciile guvernamentale de platformă:
2. Serviciul electronic de autentificare şi control al accesului MPass – în vederea autentificării utilizatorilor în sistem;
3. Semnătura digitală MSign;
4. Serviciul de jurnalizare MLog.
5. Sistemul informaţional automatizat „Registrul de stat al unităţilor de drept”, care conţine date despre toate categoriile de unităţi de drept, constituite în bază legală – în scopul preluării şi validării datelor despre persoanele juridice privind corectitudinea combinaţiilor de IDNO, denumire, cod CUATM, cod CAEM etc. necesară înregistrărilor, modificărilor sau radierilor (care conţin date despre persoane juridice);
6. Sistemul informaţional automatizat „Registrul de stat al populaţiei”, care include date despre persoanele fizice – în vederea preluării şi validării înregistrărilor, modificărilor sau radierilor (care conţin date despre persoane fizice) şi a verificării acestora privind corectitudinea combinaţiilor de IDNP, nume, prenume, act de identitate;
7. Sistemul informaţional automatizat „Registrul de stat al unităţilor administrativ-teritoriale şi al străzilor din localităţile Moldovei”, care cuprinde date cu privire unităţile teritorial-administrative, străzi, clădiri, amplasarea obiectivului turistic, a structurilor de primire turistică şi a localităţilor turistice etc.);
8. Sistemul informaţional automatizat “Registrul de stat al controalelor”– registru public consolidat de evidenţă a controalelor, completat de organele de control și ţinut în mod obligatoriu de către autoritatea administrației publice centrale de supraveghere a controalelor;
9. Sistemul Informaţional Integrat Vamal ASYCUDA World - totalitatea mijloacelor informaţional-tehnice şi a produselor de program utilizate în procesul tehnologic al organelor vamale(ASYCUDA: Automated SYstem for CUstoms DAta) - produsul de program elaborat de către Conferinţa Naţiunilor Unite pentru Comerţ şi Dezvoltare în scopul susţinerii reformelor în organele vamale, precum şi acordarea suportului la facilitarea comerţului şi controlului vamal;

Interoperabilitatea dintre sistemele informaţionale se vaasigura prin intermediul platformei guvernamentale de interoperabilitate „MConnect”, utilizînd web-servicii şi standarde/protocoale securizate precum SOAP, HTTPS etc.

Datele recepționate din celelalte resurse informaționale sînt utilizate în scopul asigurării supravegherii pieței în ceea ce privește comercializarea produselor nealimentare.

**Capitolul VII**

**INFRASTRUCTURA INFORMAŢIONALĂ**

**DE COMINICAȚII ELECTRONICE**

**23. Nivelurile de infrastructură**

**SIA NICSP** se va realiza prin implementarea unui sistem informaţional creat în baza platformei tehnologice guvernamentale comune MCloud. Componentele de bază ale arhitecturii **SIA NICSP** sunt:

1. Cloud guvernamental (MCloud);
2. Platforma Guvernamentală de Registre şi Acte Permisive (PGRAP);
3. staţiile de lucru, unităţile computerizate (PC, Laptop, tablete) ale autorităților de supraveghere a pieței, autorității de coordonare și organul vamal implicați în procesul de de supraveghere a pieței în ceia ce privește comercializarea produselor nealimentare;

Infrastructura tehnică a **SIA NICSP** va fi plasată pe platforma tehnologică guvernamentală MCloud. Spaţiul funcţional al **SIA NICSP** va cuprinde toate serviciile şi infrastructura hard oferită de proprietarul platformei MCloud, aşa ca PaaS şi IaaS.

Arhitectura **SIA NICSP** va fi SOA (service-oriented architecture), ceea ce va permite ca **SIA NICSP** să fie integrat cu toate serviciile MCloud şi cu serviciile electronice oferite de Centrul de Guvernare Electronică precum Msign, Mpass, MLog, Mnotify şi integrarea cu alte sisteme informaţionale ale altor autorităţi publice prin MConect.

Datorită faptului că interfaţa de client a **SIA NICSP** va servi browser-ul web, nu vor fi necesare resurse hard şi soft adăugătoare semnificative.

Accesul la **SIA NICSP** va fi asigurat prin orice aparat conectat la Internet cu utilizarea certificatelor de autentificare și semnătură digitală.



Fig. 1. Structura generală conceptuală a sistemului informațional automatizat național de informare și comunicare privind supravegherea pieței

**24. Complexul hardware şi software**

Lista produselor hardware şi software utilizate la crearea infrastructurii informaţionale și de comunicații electronice a **SIA NICSP** este determinată de către Ministerul Economiei și Infrastructurii, de comun acord cu furnizorul soluției de implementare a sistemului informaţional automatizat, furnizorul naţional de transmitere a datelor guvernamentale și cu operatorul tehnologic a platformei guvernamentale MCloud.

**Capitolul VIII**

**SECURITATEA ŞI PROTECŢIA SIA NICSP ICSP**

**25. Definiţie**

Securitatea **SIA NICSP** presupune starea de protecţie a resurselor şi infrastructurii informaţionale, prin care se asigură veridicitatea, integritatea, confidenţialitatea, disponibilitatea şi autenticitatea resurselor informaționale.   Sistemul securităţii informaţionale reprezintă totalitate a acțiunilor juridice, organizatorice, economice şi tehnologice orientate spre prevenirea pericolelor asociate resurselor şi infrastructurii informaţionale.

**26. Pericole asociate securităţii informaţionale**

Prin pericol pentru securitatea informaţională se înţelege un eveniment sau o acţiune potenţial posibilă, orientată spre cauzarea unui prejudiciu resurselor sau infrastructurii informaţionale.

Principalele pericole pentru securitatea informaţională a **SIA NICSP** sunt:

1) colectarea şi/sau utilizarea ilegală a informaţiei;

2) încălcarea tehnologiei de prelucrare a informaţiei;

3) încălcareaconfidenţialităţii informaţiei;

4) încălcarea integrităţii logice şi a integrităţii fizice a informaţiei;

5) încălcarea funcţionării infrastructurii informaţionale;

6) acţiunea fizică asupra componentelor infrastructurii informaţionale;

7) inserarea în produsele software şi hardware a componentelor care realizează funcţii neprevăzute în documentaţia cu privire la aceste produse;

8) elaborarea şi răspîndirea programelor care afectează funcţionarea normală a sistemelor informaţionale şi de telecomunicaţii, precum şi a sistemelor securităţii informaţionale;

9) nimicirea, deteriorarea şi suprimarea radioelectronică sau distrugerea mijloacelor şi sistemelor de prelucrare a informaţiei, de telecomunicaţii şi comunicaţii;

10) influenţa asupra sistemelor cu parolă-cheie de protecţie a sistemelor automatizate de prelucrare şi transmitere a informaţiei;

11) compromiterea cheilor şi mijloacelor de protecţie criptografică a informaţiei;

12) scurgerea informaţiei prin canale tehnice;

13) implementarea dispozitivelor electronice pentru interceptarea informaţiei în mijloacele tehnice de prelucrare, păstrare şi transmitere a informaţiei prin canalele de comunicaţii, precum şi în încăperile de serviciu ale autorităţilor;

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

15) interceptarea informaţiei în reţelele de transmitere a datelor şi în liniile de comunicaţii, decodificarea acestei informaţii şi/sau răspîndirea informaţiei false;

16) utilizarea tehnologiilor informaţionale necertificate, a mijloacelor de protecţie a informaţiei, a mijloacelor de informatizare, de telecomunicaţii şi comunicaţii necertificate în procesul creării şi dezvoltării infrastructurii informaţionale;

17) accesul neautorizat la resursele informaţionale;

18) încălcarea restricţiilor legale privind accesul și divulgarea informaţiei.

Surse ale pericolelor pot fi infractorii, personalul instituțiilor şi utilizatorii de rea-credinţă.

**27. Scopurile şi sarcinile de asigurare a securităţii informaţionale**

Pentru asigurarea edificării sistemului eficient de asigurare a securităţii informaționale ale obiectelor **SIA NICSP** sunt necesare:

1) identificarea cerinţelor securităţii informaţiei specifice pentru fiecare obiect al protecţiei în cauză;

2) respectarea cerinţelor actelor normative naţionale şi internaţionale;

3) utilizarea celor mai bune practici (standarde, metodologii) pentru asigurarea securităţii informaţionale;

4) determinarea subdiviziunilor responsabile pentru asigurarea securităţii informaţionale;

5) distribuirea între subdiviziuni a sferelor de responsabilitate în asigurarea securităţii informaţionale;

6) în baza gestionării riscurilor de securitate a informaţiei, determinarea cerințelor tehnice și organizatorice, care constituie politica de securitate informaţională a obiectului protecţiei;

7) realizarea cerinţelor politicii desecuritateinformaţională prin implementarea metodelor software şi hardware şi a mijloacelor de protecţie a informaţiei corespunzătoare;

8) realizarea sistemului de management al securităţii informaţionale.

*Sarcinile de bază ale asigurării securităţii informaţionale sînt:*

1) asigurarea confidenţialităţii informaţiei, prevenirea accesului la informaţie fără drepturi şi împuterniciri corespunzătoare;

2) asigurarea integrităţii logice a informaţiei, prevenirea introducerii, actualizării şi nimicirii neautorizate a informaţiei;

3) asigurarea integrităţii fizice a informaţiei;

4) asigurarea protecţiei infrastructurii informaţionale împotriva deteriorării şi tentativelor de modificare a funcţionării.

*Mecanismele de bază ale asigurării securităţii informaţionale sunt:*

1) autentificarea şi autorizarea;

2) controlul accesului;

3) înregistrarea acţiunilor şi auditul;

4) criptarea informaţiei;

5) analizarea și modelarea fluxurilor informaționale (sistemele CASE);

6) monitorizarea reţelelor;

7) detectarea şi prevenirea intruziunilor (IDS/IPS);

8) prevenirea scurgerii informaţiei confidenţiale (sistemului DLP);

9) analizatori de protocoale;

10) mijloacele de programare antivirus;

11) ecrane între reţele (firewall);

12)sistemele copierii de rezervă;

13) sistemele de alimentare fără întrerupere cu energie electrică;

14) organizarea pazei, securității;

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

16) mijloacele de analiză a sistemelor de protecţie;

17) alte mecanisme.

Utilizarea mecanismelor de asigurare a securităţii informaţionale se planifică la etapa de proiectare a sistemelor şi infrastructurii informaţionale.

Una dintre cele mai vulnerabile verigi ale sistemului securităţii informaţionale constituie factorul uman și respectarea procedurilor stabilite. De aceea, un element important al securităţii informaţionale se consideră instruirea personalului privind metodele şi procedeele de asigurare a securității informaționale.

**28. Sistemul de protecţie a datelor cu caracter personal**

Organizarea sistemului de protecție a datelor cu caracter personal constituie o parte componentă a mecanismului de asigurare a securităţii informaționale a **SIA NICSP**.

Sistemul de protecţie a datelor cu caracter personal se constituie în baza:

1) raportului privind rezultatele efectuării auditului intern;

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

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

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

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

6) documentelor de reglementare şi politicilor de securitate elaborate.

Accesarea datelor cu caracter personal ale persoanei fizice din resursele și sistemele informaționale de stat, precum și păstrarea și actualizarea acestora în baza de date a **SIA NICSP** este posibilă doar în cazurile desfășurării activităților de supraveghere a pieței în ceia ce privește comercializarea produselor nealimentare de către reprezentanții (inspectorii) autorităților de supraveghere a pieței, autorității de coordonare și a organului vamal.