Republica Moldova

MINISTERUL DEZVOLTĂRII INFORMAȚIONALE

ORDIN Nr. 94
din 17.09.2009

cu privire la aprobarea unor reglementări tehnice

Publicat : 23.04.2010 în Monitorul Oficial Nr. 58-60 art Nr : 232

În temeiul Legii privind activitatea de reglementare tehnică nr. 420-XVI din 22.12.2006 şi întru executarea Hotărîrii Guvernului "Cu privire la unele acțiuni de implementare a Strategiei Naționale de edificare a societății informaționale – "Moldova electronică" în anul 2007" nr. 606 din 1.06.2007, precum şi a Hotărîrii Guvernului "Cu privire la aprobarea repartizării mijloacelor Fondului pentru realizarea Programului național de elaborare a reglementărilor tehnice" nr. 564 din 21.05.2007,

ORDON:

1. A aproba reglementările tehnice:

a) modul de evidență a serviciilor publice electronice, conform anexei nr. 1;

b) prestarea serviciilor publice electronice. Cerințe tehnice, conform anexei nr. 2;

c) asigurarea securității informaționale la prestarea serviciilor publice electronice. Cerințe tehnice, conform anexei nr. 3;

d) determinarea costului de elaborare şi implementare a sistemelor informaționale automatizate. Normativele şi estimarea cheltuielilor de lucru, conform anexei nr. 4.

2. Reglementările tehnice menționate în punctul 1 vor intra în vigoare în termen de trei luni de la data publicării în Monitorul Oficial al Republicii Moldova.

3. Controlul asupra executării prezentului ordin se pune în sarcina dlui Pavel Şincariuc, director al Direcției generale dezvoltarea societății informaționale.

VICEMINISTRUL DEZVOLTĂRII
INFORMAȚIONALE Oleg ROTARU

Nr. 94. Chişinău, 17 septembrie 2009.

Anexa nr. 1
la Ordinul nr. 94
din 17.09.2009

Reglementare tehnică
Modul de evidență a serviciilor publice electronice

1. Domeniu de aplicare

Prezenta reglementare stabileşte destinația, obiectivele, principiile şi modul de realizare a evidenței şi înregistrării serviciilor publice electronice.

Serviciile publice electronice (în continuare – servicii publice), reprezintă o parte integrantă a activității oricăror autorități ale administrației publice, organizații şi întreprinderi de stat.

O parte însemnată a serviciilor publice conțin masive şi produse informaționale, acordate prin intermediul mijloacelor electronice, ce reflectă rezultatele activității acestor întreprinderi într-o sferă sau alta. Gestionarea serviciilor publice trebuie să fie realizată nemijlocit în procesul activității autorităților administrației publice.

În procesul gestionării serviciilor publice trebuie să fie asigurată realizarea următoarelor sarcini:

- completitudinea creării masivelor şi produselor informaționale primare şi derivate, care constituie serviciile publice;
- păstrarea şi protecția sigură a serviciilor publice;
- accesul liber al cetățenilor şi organizațiilor la serviciile publice, care nu conțin informații ce constituie secret de stat, comercial, de serviciu sau personal;
- crearea condițiilor pentru utilizarea eficientă a serviciilor publice în activitatea autorităților administrației publice.

Pentru a asigura realizarea sarcinilor fixate, este necesar de a introduce reguli şi proceduri unice de evidență.

Prestarea serviciilor publice are drept scop asigurarea accesului la informația oficială pentru populație şi mediul de afaceri, ridicarea nivelului calității serviciilor publice, sporirea gradului de participare a cetățenilor în procesul de prestare a serviciilor.

În acest sens, participanți la procesul de prestare a serviciilor publice sînt:

- instituțiile publice de nivel local şi central;
- cetățenii;
- sectorul de afaceri.

Furnizorii de servicii publice sînt autoritățile administrației publice, instituțiile sau organizațiile de stat care execută comanda de stat pentru prestarea unui anumit tip de servicii în limitele competenței şi obligațiilor funcționale ale acestora.

Consumatori de servicii publice sînt cetățenii sau organizațiile care au apelat direct sau prin intermediul reprezentantului lor la furnizorul de servicii publice pentru realizarea drepturilor sau intereselor legitime, sau executarea obligațiilor stabilite prin acte normative.

2. Baza juridico-normativă

Prezenta reglementare este elaborată în baza următoarelor acte legislative ale Republicii Moldova:

- Legea Republicii Moldova „Privind dreptul de autor şi drepturile conexe” nr. 293-XIII din 23.11.1994;
- Legea Republicii Moldova „Privind accesul la informație” nr. 982-XIV din 11.05.2000;
- Legea Republicii Moldova „Cu privire la informatizare şi la resursele informaționale de stat” nr. 467-XV din 21.11.2003;
- Legea Republicii Moldova „Cu privire la documentul electronic şi semnătura digitală” nr. 264-XV din 15.07.2004;
- Legea Republicii Moldova „Privind comerțul electronic” nr. 284-XV din 22.07.2004;

- Legea Republicii Moldova „Privind activitatea de reglementare tehnică” nr. 420-XVI din 22.12.2006;
- Legea Republicii Moldova „Cu privire la protecția datelor cu caracter personal” nr. 17-XVI din 15.02.2007;
- Legea Republicii Moldova „Cu privire la registre” nr. 71-XVI din 22.03.2007;
- Legea Republicii Moldova „Cu privire la secretul de stat” nr. 245 din 27.11.2008.

3. Terminologie

În prezenta reglementare sînt utilizați următorii termeni:

Date de evidență – datele de o anumită componență despre persoanele, obiectele şi/sau fenomenele de orice natură identificate, care constituie obiectul evidenței.

Evidența de stat – evidență, a cărei organizare este realizată de către autoritățile administrației publice.

Evidența electronică – evidența, partea sau totalitatea datelor care pot exista sau pot fi utilizate (inclusiv pentru stabilirea drepturilor şi obligațiilor persoanelor şi a altor consecințe de drept) exclusiv în formă electronică.

Organizatorul evidenței – persoana care duce evidența serviciilor publice de sine stătător, sau prin împuternicirea sau obligarea cuiva la realizarea acestei activități total sau parțial în interesele sale.

Posesor al informației - subiectul care exercită dreptul de posesiune şi folosință asupra resurselor şi sistemelor informaționale, al tehnologiilor şi mijloacelor de asigurare a acestora şi realizează împuternicirile de dispoziție în limitele stabilite de legislația în vigoare.

Registrator – persoană, ce duce evidența serviciilor publice total sau parțial în interesul organizatorului evidenței, în baza împuternicirilor primite de la acesta sau în baza obligației.

Resursă informațională cu acces limitat – resursa informațională, ce conține informație despre secretele de stat şi informație confidențială sau informație, accesul la care este limitat de proprietarii resurselor informaționale.

Sistem de evidență – totalitatea mijloacelor ce asigură ținerea evidenței serviciilor publice, inclusiv mijloacele pentru lucrările de secretariat, utilajul tehnico-ingineresc şi aplicațiile computerizate informațional-comunicaționale, ce realizează logica evidenței, precum şi textele originale, documentația de sistem şi de utilizare a acestor aplicații computerizate.

4. Obiective şi sarcini

Obiectivul prezentei reglementării constă în descrierea modului şi principiilor de evidență a serviciilor publice în spațiul informațional național.

Serviciile publice includ totalitatea resurselor informaționale şi a serviciilor autorităților administrației publice. Prestarea serviciilor publice este susținută de infrastructura informațional-comunicațională de stat prin intermediul rețelei centrelor de solicitare şi centrelor de acces public, precum şi prin intermediul Internet-ului, televiziunii digitale şi al telefoanelor mobile.

În scopul realizării unei utilizări eficiente a serviciilor publice este prevăzută distribuirea resurselor informaționale şi a controlului asupra utilizării acestora. Evidența tuturor serviciilor publice serveşte drept instrument pentru organizarea eficientă a lucrărilor orientate spre satisfacerea la timp a necesităților noi ale autorităților administrației publice, precum şi spre reacționarea rapidă şi la timp la posibilitățile emergente.

Scopul organizării evidenței serviciilor publice în spațiul informațional național este şi sporirea eficienței, capacității de gestionare, coordonării activității tuturor subdiviziunilor structurale ale autorităților administrației publice.

Evidența serviciilor publice se efectuează în următoarele scopuri:

- colectarea, clasificarea şi utilizarea informațiilor complete, actuale şi veridice despre serviciile

publice create, curente şi lichidate;
- monitorizarea situaţiei sistemului de prestare a serviciilor publice;
- evaluarea eficienţei creării şi utilizării serviciilor publice;
- relevarea solicitărilor de servicii publice din partea utilizatorilor;
- asigurarea caracterului deschis şi transparent al informaţiilor privind activitatea autorităţilor administraţiei publice, legată de formarea şi utilizarea informaţiei cuprinse în serviciile publice;
- determinarea tendinţelor şi direcţiilor de dezvoltare a serviciilor publice.

Prezenta reglementare stabileşte modul de evidenţă a serviciilor publice din punctul de vedere al înregistrării şi actualizării datelor.

Evidenţei obligatorii sînt supuse serviciile publice ale autorităţilor administraţiei publice, alte servicii publice nou- elaborate, create, achiziţionate şi (sau) care funcţionează în baza mijloacelor proprii sau cu atragerea mijloacelor din bugetul de stat, precum şi bazele (băncile) de date separate ce sînt achiziţionate sau transmise spre a fi utilizate de către autorităţile administraţiei publice.

5. Prestarea serviciilor publice

5.1. Clasificarea serviciilor publice

Caracteristicile serviciilor publice sînt:
- prestarea serviciilor publice în sfera activităţii de semnificaţie generală;
- existenţa unui cerc nelimitat de subiecţi ce utilizează serviciile menţionate;
- desfăşurarea activităţii de prestare a serviciilor publice nemijlocit autorităţilor administraţiei publice sau indirect altor subiecţi (în baza unui acord formalizat privind atragerea unei organizaţii terţe la executarea anumitor acţiuni legate de prestarea serviciilor publice prin mijloace electronice);
- baza juridică a prestării serviciilor publice o poate constitui atît proprietatea publică cît şi cea privată.

Serviciile publice se prestează prin mijloace electronice în baza interacţiunii dintre trei categorii de participanţi de bază:
- „Guvern - Cetăţean” – prestarea serviciilor publice se bazează pe interacţiunea dintre cetăţean şi guvern, o mare parte a căreia se realizează în regim on-line. Serviciile publice principale de care beneficiază cetăţenii sînt următoarele:

1) achitarea impozitelor;
2) serviciul de căutare a unui loc de muncă prin intermediul agenţiei de ocupare a forţei de muncă;
3) obţinerea asistenţei sociale;
4) perfectarea actelor personale;
5) înregistrarea mijloacelor de transport;
6) înregistrarea bunurilor imobile;
7) depunerea cererilor şi primirea autorizaţiilor pentru construcţie;
8) depunerea reclamaţiilor la poliţie;
9) serviciile bibliotecilor publice;
10) înregistrarea actelor de stare civilă (certificate de naştere, de înregistrare a căsătoriei, notificarea despre schimbarea domiciliului etc.);
11) înmatricularea în instituţiile superioare de învăţămînt;
12) contribuirea la securitatea publică;
13) serviciile medicale;

- „Guvern - Business” – prestarea serviciilor publice se bazează pe interacţiunea dintre administraţia publică şi mediul de afaceri. Serviciile publice principale din această categorie sînt următoarele:

1) contribuţiile sociale şi de pensii ale angajaţilor şi angajatorilor;

2) achitarea impozitelor de către organizații;
3) înregistrarea societăților noi;
4) transferul de date către organele statistice;
5) completarea şi depunerea declarațiilor vamale;
6) primirea autorizațiilor legate de protecția mediului;
7) depunerea cererilor şi primirea autorizațiilor pentru construcție;
8) efectuarea achizițiilor publice.

- „Guvern - Guvern" – prestarea serviciilor publice se bazează pe interacțiunea dintre autoritățile administrației publice şi instituțiile de stat prin intermediul mijloacelor electronice de comunicație.

Din punct de vedere funcțional, serviciile publice se împart în următoarele clase de servicii:
- prestarea serviciilor publice de semnificație generală;
- prestarea serviciilor în domeniul informației de afaceri şi comerciale;
- prestarea serviciilor în domeniul înregistrării relațiilor funciare şi cadastrale;
- prestarea serviciilor în domeniul sistemului financiar-bancar;
- prestarea serviciilor informaționale în domeniul învățămîntului – implementarea şi utilizarea noilor tehnologii de comunicație şi informaționale în procesul educațional;
- prestarea serviciilor informaționale în domeniul ştiinței;
- prestarea serviciilor informaționale în domeniul ocrotirii sănătății;
- prestarea serviciilor informaționale în domeniul informației juridice;
- prestarea serviciilor informaționale în domeniul asigurărilor sociale;
- prestarea serviciilor informaționale privind securitatea;
- prestarea serviciilor informaționale în domeniul patrimoniului cultural;
- prestarea serviciilor informaționale în domeniul drepturilor omului;
- prestarea serviciilor informaționale în domeniul turismului.

În funcție de direcția de activitate, serviciile publice se clasifică în:
- servicii publice externe:
1) dezvoltarea social-economică;
2) ştiința şi cunoştințele;
3) protecția mediului ambiant;
4) ocrotirea sănătății;
5) protecția drepturilor, drepturile democratice şi drepturile omului;
6) politica socială;
7) cultura;
8) învățămîntul;
9) securitatea publică;
10) sistemul judiciar;
11) securitatea şi apărarea națională;
12) resursele naturale:
- servicii publice interne:
1) reglementarea socială, planificarea şi administrarea serviciilor;
2) gestionarea resurselor umane;
3) gestionarea resurselor financiare;
4) gestionarea informației şi tehnologiilor;
5) gestionarea fondurilor, resurselor;
6) gestionarea comunicațiilor;
7) gestionarea furnizărilor;
8) administrarea;

9) servicii profesionale.

În funcție de metoda de acces, serviciile publice se împart în următoarele tipuri:

- informație deschisă şi accesibilă tuturor;
- informație cu acces limitat: secret de stat, secret comercial, date cu caracter personal.

În funcție de criteriul de efectuare a plății, serviciile publice se clasifică după cum urmează:

- servicii publice cu plată;
- servicii publice gratuite.

În funcție de gradul de personificare, serviciile publice se împart în:

- individuale;
- colective.

Este posibilă prestarea serviciilor publice conform diferitor nivele de complexitate:

Nivelul 1 – Informarea.

Acest nivel include furnizarea informației privind:

- serviciile publice;
- activitatea autorităților administrației publice;
- serviciile de deservire informațională;
- căutarea informației;
- procesarea informației;
- eliberarea datelor (documentelor);
- păstrarea informației.

Nivelul 2 – Interacțiunea.

Acest nivel permite prestarea următoarelor servicii:

- copierea formularelor din rețeaua Internet;
- prelucrarea formularelor, inclusiv autentificarea acestora;
- implementarea sistemului de circulație electronică a documentelor;
- serviciile de utilizare a Internet-ului, sistemelor informaționale, bazelor de date, rețelelor;
- servicii consultative;
- servicii de transmitere a informației;
- servicii de acces la rețeaua Internet;
- servicii de utilizare a poştei electronice şi de creare a paginilor web.

Nivelul 3 – Tranzacții.

Acest nivel permite prestarea următoarelor servicii:

- transmiterea informației;
- luarea deciziilor şi furnizarea bunurilor şi/sau serviciilor (inclusiv efectuarea plăților prin mijloace electronice).

Nivelul 4 – Transformarea.

Acest nivel permite redefinirea actului de gestiune.

5.2. Procesul de prestare a serviciilor publice

Procesul de prestare a serviciilor publice este realizat prin mijloace electronice cu ajutorul unicului punct de acces - Portalul Guvernamental.

Prestarea serviciilor publice se efectuează în baza resurselor şi sistemelor informaționale (SI) existente sau create şi urmează să cuprindă următoarele procese ale ciclului de viață a SI ce funcționează în cadrul gestionării sistemelor şi tehnologiilor informaționale:

1) planificarea – lucrările anteproiect – se elaborează concepția sistemului şi propunerea-business privind prestarea serviciilor publice;

2) elaborarea – elaborarea sistemului informațional de prestare a serviciilor publice – se determină, analizează, elaborează, creează, testează şi, în caz de necesitate, evaluează mecanismele

de interacțiune a elementelor de program şi structurilor organizaționale, precum şi se stabilesc cerințele față de hardware, infrastructura utilizatorului, instruire şi mentenanță. Se elaborează sarcina tehnică, proiectul tehnic, versiunea sistemului software, documentația tehnică, procesul-verbal de testare de calificare, actul de predare în exploatare experimentală;

3) implementarea – implementarea sistemului informațional de prestare a serviciilor publice – se pregăteşte infrastructura utilizatorului şi utilajul din încăperile în care va funcționa produsul software, se testează capacitatea de lucru a produsului software în condiții reale de exploatare, precum şi se organizează instruirea personalului privind lucrul cu produsul software sau componentele acestuia;

4) exploatarea – exploatarea sistemului informațional de prestare a serviciilor publice – include procesele legate de utilizarea produselor software pentru prestarea serviciilor, precum şi controlul funcționării, depistării şi documentării problemelor survenite;

5) suportul şi mentenanța - mentenanța sistemului informațional de prestare a serviciilor publice – se controlează funcționarea produsului software, se înregistrează problemele pentru analiză, se întreprind acțiuni de prevenire şi corectare, precum şi acțiuni pentru adaptarea şi perfecționarea produsului software;

6) monitorizarea şi deciziile privind modernizarea sistemelor informaționale – utilizarea sistemului informațional de prestare a serviciilor publice – prevede retragerea din exploatare a produsului software şi a subsistemelor software şi proceselor software auxiliare legate de acesta.

În cadrul proceselor de gestionare a tehnologiilor informaționale sînt create sisteme informaționale şi resurse de prestare a serviciilor publice destinate să mențină funcționalitatea eficientă a autorităților administrației publice şi exercitarea obiectivelor strategice şi tactice de către acestea.

Sistemul de prestare a serviciilor publice trebuie să includă următoarele tipuri de resurse informaționale:

- resurse informaționale de stat – resurse informaționale aflate în proprietatea statului şi care se clasifică în teritoriale, instituționale şi de bază;
- sisteme informaționale care constituie subsistemele guvernării electronice;
- pagini web şi domenii ale autorităților administrației publice;
- clasificatoare, obiecte informaționale şi servicii informaționale;
- documentație tehnică, certificate de înregistrare a domenelor şi acte de certificare a sistemelor informaționale.

Aceste sisteme şi resurse informaționale urmează să fie atribuite la o clasă şi categorie concretă de servicii publice.

6. Evidența serviciilor publice

Evidența serviciilor publice reprezintă evidența componentelor resurselor informaționale în cadrul căreia urmează să fie reflectate funcțiile şi principiile evidenței, formarea serviciilor publice, precum şi regimul juridic al acestora.

Evidența serviciilor publice trebuie să cuprindă următoarele etape ale ciclului de viață la prestarea serviciilor publice:

- punerea inițială la evidență a serviciului public presupune înregistrarea acestuia în registru;
- actualizarea datelor despre serviciul public trebuie să fie efectuată în registru prin modificarea datelor de înregistrare în cazul, în care:

1) se schimbă organizația care prestează servicii;
2) se schimbă însuşi serviciul;
3) se schimbă condițiile de prestare a serviciului;
4) se schimbă documentația eliberată la prestarea serviciilor;

5) se schimbă SI de bază pentru prestarea serviciului.

La încetarea procesului de prestare a serviciului public toată informația despre serviciul respectiv trebuie să fie anulată.

Sistemul de ținere a evidenței serviciilor publice cuprinde:

-baza juridico-normativă;

-documentele de toate nivelurile, care reglementează evidența;

-organizațiile, ce realizează evidența;

- suporturile de hîrtie şi electronice şi sistemele informaționale folosite la ținerea evidenței serviciilor publice.

6.1. Funcțiile sistemului de evidență a serviciilor publice

Sistemul de evidență a serviciilor publice trebuie să îndeplinească următoarele funcții:

- colectarea, acumularea, prelucrarea, păstrarea şi actualizarea datelor serviciilor publice;
- asigurarea la nivel de stat a evidenței unice a serviciilor publice;
- asigurarea autorităților administrației publice cu informație operativă şi statistică;
- asigurarea schimbului de informație între autoritățile administrației publice, precum şi cu autoritățile analogice ale altor țări;
- controlul asupra respectării modului de evidență a serviciilor publice, elaborarea şi realizarea măsurilor de reacționare oportună la tendințele şi manifestările negative;
- asigurarea organizatorică, normativă şi metodică a activității autorităților administrației publice, ce exercită nemijlocit funcțiile de evidență a serviciilor publice;
- asigurarea funcționării complexului tehnic de program şi a rețelelor informaționale autorizate, utilizate în cadrul sistemului de evidență a serviciilor publice.

La dezvoltarea serviciilor publice este necesar de aplicat următoarele metode de realizare a funcțiilor de evidență:

- perfecționarea asigurării juridico-normative şi metodice a gestionării serviciilor publice;
- perfecționarea structurilor organizatorice privind formarea şi utilizarea serviciilor publice;
- organizarea evidenței serviciilor publice şi elaborarea criteriilor şi metodelor de evaluare a costului acestora;
- elaborarea principiilor şi crearea sistemului de asigurare financiar-economică a activității de formare şi utilizare a serviciilor publice;
- elaborarea şi implementarea tehnologiilor unificate de utilizare a rețelelor de telecomunicații pentru coordonarea gestionării serviciilor publice;
- organizarea şi realizarea controlului de stat al funcționării serviciilor publice.

6.2. Principiile de bază ale evidenței serviciilor publice

Evidența serviciilor publice trebuie să fie realizată în conformitate cu următoarele principii de bază:

- principiul legalității - prevede la crearea, procurarea, utilizarea şi administrarea serviciilor publice, conformitatea acestora cu legislația națională în vigoare;
- principiul îmbinării publicității şi confidențialității - prevede publicarea informației general accesibile, cu excepția informației recunoscute ca fiind confidențială, în modul stabilit de legislația națională în vigoare;
- principiul eficienței şi economicității - prevede faptul că procurarea resurselor informaționale utilizate pentru asigurarea continuității procesului de prestare a serviciilor publice este realizată reieşind din necesitatea de satisfacere a necesităților informaționale şi de reducere a cheltuielilor de buget;
- principiul îmbinării plății şi gratuității de prestare a informației - prevede că informația procurată din contul mijloacelor bugetului de stat se acordă gratuit autorităților administrației publice.

Transmiterea informației indicate mai sus altor utilizatori are loc contra unei anumite plăți, dacă legislația nu prevede altfel;

- principiul succesivității – prevede, că crearea, procurarea, utilizarea şi administrarea serviciilor publice se desfăşoară pe etape;
- principiul integrității - prevede, că sistemul de prestare a serviciilor publice trebuie să fie unul dintre subsistemele de bază ale sistemului informațional integrat de stat;
- principiul justificării - prevede utilizarea informației documentate în sistemul de prestare a serviciilor publice;
- principiul scalabilității - prevede posibilitatea de extindere şi dezvoltare a componentelor sistemului de evidență a serviciilor publice;
- principiul unității spațiului informațional - prevede utilizarea unui sistem unic de clasificatoare, formate de date, protocoale de interacțiune informațională, standarde, documente normative şi metodice interdependente, condiție care este necesară pentru formarea spațiului informațional unic al sistemului de prestare a serviciilor publice;
- principiul protecției datelor personale - prevede crearea şi exploatarea sistemului de evidență a serviciilor publice în conformitate cu acordurile şi convențiile internaționale, precum şi cu legislația națională în vigoare în domeniul protecției drepturilor omului;
- principiul identificării unice - prevede faptul, că toate obiectele informaționale de evidență trebuie să aibă un număr unic de identificare;
- principiul controlului - prevede controlul măsurilor ce asigură calitatea, fiabilitatea resurselor şi sistemelor informaționale de stat, precum şi păstrarea şi utilizarea rațională a acestora;
- principiul securității - prevede asigurarea protecției sistemului de prestare a serviciilor publice contra influențelor de orice natură ce afectează continuitatea procesului de prestare a serviciilor.

6.3. Organizarea evidenței serviciilor publice

Serviciile publice prestate sînt supuse evidenței obligatorii.

Evidența serviciilor publice se realizează în scopul:

- asigurării informaționale a autorităților administrației publice;
- informării cetățenilor şi organizațiilor despre serviciile publice, precum şi despre modul de acces la acestea.

Formarea datelor privind evidența serviciilor publice trebuie să fie efectuată de către autoritatea administrației publice în registru, care trebuie să includă informație despre serviciile publice, precum şi despre sistemele şi resursele informaționale de stat corespunzătoare, care constituie baza pentru prestarea serviciilor publice, în conformitate cu legislația națională în vigoare.

Formele de ținere a evidenței serviciilor publice sînt registrele, jurnalele, dosarele, cartelele, cărțile, conturile de evidență, înregistrările, iar în cazul utilizării tehnologiilor informaționale, formele de ținere a evidenței sînt fişierele tabelelor electronice, bazele de date, sistemele de fişiere textuale şi alte mijloace de organizare a datelor digitale.

Formele de furnizare a datelor de evidență trebuie să fie determinate de următorii factori:

- forma de ținere a evidenței;
- mijloacele tehnice ce asigură ținerea evidenței;
- organizarea datelor de evidență;
- metodele de furnizare a datelor de evidență persoanelor interesate.

Formele de furnizare a datelor de evidență sînt:

- eliberarea actelor, rapoartelor, extraselor, certificatelor, adeverințelor;
- înştiințarea vocală;
- publicațiile în mijloacele de informare în masă;
- revelarea prin rețele computerizate de uz comun.

6.4. Regimul juridic al serviciilor publice

Regimul juridic al serviciilor publice trebuie să includă:

- modul şi sursele de formare a serviciilor publice;
- modul de documentare a informației;
- dreptul de proprietate asupra anumitor documente şi masive de documente;
- procedura de apărare juridică şi de utilizare a serviciilor publice;
- modul de înregistrare a serviciilor publice şi de includere a serviciilor publice în circuitul economic;
- determinarea categoriei de acces la serviciile publice.

6.4.1. Modul şi sursele de formare a serviciilor publice

Serviciile publice trebuie să fie formate de către autoritățile administrației publice respective, responsabile de formarea serviciilor publice în conformitate cu împuternicirile oferite acestora.

Formarea serviciilor publice trebuie să fie realizată în cadrul registrului, incluzînd lista de date privind serviciile publice, sistemele, precum şi paginile web şi domenele autorităților administrației publice, în conformitate cu legislația națională în vigoare.

Serviciile publice trebuie să includă informația furnizată de către autoritățile administrației publice, cetățeni, organizații şi asociații obşteşti ce îşi desfăşoară activitatea pe teritoriul Republicii Moldova în odinea stabilită de legislația în vigoare.

Responsabilitate pentru autenticitatea informației privind serviciile publice o poartă proprietarii de servicii publice.

Modul, condițiile de prezentare şi conținutul informației documentate pentru formarea serviciilor publice se stabilesc în conformitate cu Legile Republicii Moldova „Cu privire la registre" nr. 71-XVI din 22.03.2007 şi „Privind accesul la informație" nr. 982-XIV din 11.05.2000.

În rezultatul formării serviciilor publice trebuie determinată următoarea informație:

– descrierea detaliată a serviciilor publice şi a componentelor necesare;
– metodele de implementare şi prestare a serviciilor publice;
– procedurile de control al nivelului necesar de calitate a serviciilor publice.

6.4.2. Modul de documentare a informației

Serviciile publice trebuie să fie formate pe baza informației documentate. Informația documentată constituie obiectul dreptului de proprietate şi este expusă sub formă de document separat sau totalitate de documente, fixate pe un purtător de informație cu rechizitele corespunzătoare, inclusiv sub formă de document electronic.

Indiferent de categoria serviciilor publice, conținutul informației, furnizate utilizatorilor potențiali de servicii publice, include:

– informații privind lista serviciilor publice;
– informații despre furnizorul abilitat să presteze un anumit tip de servicii publice;
– informații despre persoanele cu funcții de răspundere care prestează în mod nemijlocit servicii publice utilizatorilor;
– descrierea serviciilor publice prestate în conformitate cu lista serviciilor publice prestate.

Descrierea serviciilor publice prestate reprezintă un document destinat utilizatorilor de servicii publice în care este explicat modul de obținere a unui anumit serviciu public.

Descrierea serviciilor publice prestate include următoarea informație:

– destinația serviciului public;
– termenul de obținere a serviciului;
– documentele necesare pentru obținerea serviciului;
– datele de contact ale lucrătorilor din cadrul autorităților administrației publice la care se poate de adresat pentru obținerea serviciului respectiv;

– informații privind condițiile şi cerințele înaintate față de utilizatorii de servicii;
– modul de obținere a serviciului în formă electronică;
– informația privind achitarea serviciului, în cazul în care este prevăzut că serviciul este cu plată;
– servicii suplimentare, aferente obținerii serviciului;
– indicatorii cheie ai calității serviciilor: oportunitatea, accesibilitatea, continuitatea şi procesul de prezentare a reclamațiilor.

Pentru anumite tipuri de servicii publice pot fi stabilite particularități specifice ale regimului juridic al acestora, în special, rezultante din destinația funcțională a acelor servicii publice sau în urma clasării serviciilor publice la o anumită categorie de acces la acestea.

Documentarea informației constituie o condiție obligatorie pentru includerea informației în serviciile publice. Informația documentată din serviciile publice trebuie să fie sistematizată, clasificată şi asigurată cu rechizitele corespunzătoare.

Rechizitele de bază ale informației documentate sînt:
- denumirea documentului;
- proprietarul informației;
- sursa de informație;
- data şi ora apariției şi documentării;
- modul de utilizare;
- alte rechizite, necesare pentru sistematizare şi clasificare.

La includerea informației în componența serviciilor publice trebuie să fie asigurată posibilitatea de căutare a acesteia, în funcție de clasificare şi conform rechizitelor stabilite. Datele, conținute în banca centrală a registrului, includ rechizitele şi informația în conformitate cu legislația în vigoare.

Informația în serviciile publice poate fi prezentată în formă textuală, grafică, audio, video şi multimedia (combinația formatelor textual, grafic, audio şi video).

Documentul, obținut din sistemul informațional automatizat, precum şi păstrat, procesat şi transmis cu ajutorul sistemelor informaționale şi telecomunicaționale obțin forță juridică în modul stabilit de legislația în vigoare.

6.4.3. Dreptul de proprietate asupra anumitor documente şi masive de documente

Dreptul de proprietate asupra anumitor documente şi masive de documente este stabilit de Legea Republicii Moldova „Privind dreptul de autor şi drepturile conexe” nr. 293-XIII din 23.11.1994. În conformitate cu prevederile acestui act normativ, dreptul de proprietate asupra resurselor informaționale de stat aparțin statului.

Responsabilitatea pentru încălcarea drepturilor de proprietate este reglementată de legea menționată şi de alte acte normative în vigoare.

6.4.4. Procedura de apărare juridică şi de utilizare a serviciilor publice

Serviciile publice sînt prestate utilizatorilor în conformitate cu:
- legislația Republicii Moldova;
- Acordul cu privire la nivelul de deservire;
- în baza solicitării;
- conform altor temeiuri.

Raporturile juridice privind prestarea serviciilor publice sînt reglementate de legislația națională în vigoare şi acordurile încheiate cu utilizatorii serviciilor menționate. În caz de nerespectare a înțelegerilor de către oricare dintre părți, partea care a comis încălcarea poartă răspundere în conformitate cu prevederile Acordului cu privire la nivelul de deservire, precum şi în conformitate cu legislația în vigoare.

Acordul cu privire la nivelul de deservire reprezintă un acord încheiat între furnizorul şi utilizatorul de servicii publice, în care sînt descrise în mod detaliat serviciile prestate, în limba care

este înțeleasă de utilizatori şi comodă pentru aceştia, drepturile şi obligațiile ambelor părți cu privire la prestarea serviciilor publice, precum şi responsabilitățile părților în caz de neexecutare a obligațiunilor ce le revin.

Persoanele vinovate de divulgarea, modificarea sau distrugerea informației privind serviciile publice poartă răspundere disciplinară, civilă, administrativă sau penală în conformitate cu legislația în vigoare.

6.4.5. Modul de înregistrare şi includere a serviciilor publice în circuitul economic

Serviciile publice sînt considerate disponibile pentru a fi înregistrate doar după darea în exploatare a sistemului informațional şi efectuarea auditului independent după implementare, în limitele cerințelor interne şi prevederilor legislației.

Proprietarul informației trebuie să pregătească toată documentația necesară în conformitate cu modul de documentare, după care în registru sînt introduse datele necesare.

Pentru a înregistra fiecare serviciu public este necesar de introdus următoarea informație în registru:

- codul serviciului public;
- tipul serviciului public;
- funcționalitatea serviciului public;
- orientarea specială;
- data începerii şi termenul de prestare a serviciului;
- numărul de obiecte ale resurselor informaționale, incluse în serviciu;
- lista resurselor informaționale, incluse în serviciu;
- tipul confidențialității resurselor informaționale, incluse în serviciu;
- versiunile software-ului utilizat în procesul de prestare a serviciului;
- autoritatea administrației publice responsabilă de prestarea serviciului;
- proprietarul serviciului;
- organizația care efectuează controlul asupra prestării serviciului;
- organizația care efectuează asigurarea securității serviciului şi resurselor informaționale, incluse în serviciu;
- organizația care realizează concepția celor trei „A” (autentificare, autorizare, administrare);
- statutul serviciului (în conformitate cu ciclul de viață);
- mijloacele de prestare a serviciului;
- categoria tipului de subiecți;
- categoria utilizatorului;
- categoria de plată;
- persoanele cu funcții de răspundere care prestează serviciul.

Toată informația păstrată în registru trebuie să permită obținerea ultimelor versiuni ale documentației privind serviciile publice prestate.

Datele din registru trebuie să fie revizuite periodic, cel puțin o dată în trei ani sau în caz de:

- modificare a modului de prestare a serviciilor publice;
- modificare a datelor cu condiția confirmării documentale a autenticității datelor de către proprietar;
- modificare a prevederilor legislației în vigoare privind prestarea serviciilor publice.

Persoanele responsabile de introducerea datelor în registru sînt obligate să-şi asume obligația de a nu divulga această informație. Obligația de a nu divulga informația rămîne valabilă şi după încetarea activității de prestare a serviciilor publice în conformitate cu legea.

După înregistrarea serviciului public se stabileşte formal data lansării procesului de prestare a serviciului respectiv, după care serviciul public se consideră inclus în circuitul economic.

6.4.6. Determinarea categoriei de acces la serviciile publice

Modul de acces la serviciile publice este stabilit în dependență de gradul de secretizarea informației conținute în aceasta şi de destinația acesteia.

Serviciile publice sînt deschise şi general accesibile. Excepția o constituie informația documentată atribuită la categoria cu acces limitat în conformitate cu legislația în vigoare.

Accesul la serviciile publice general accesibile trebuie să fie realizat fără autentificarea şi evidența utilizatorului. Evidența acțiunilor, identificarea şi autentificarea utilizatorului sînt obligatorii în cazul accesului la serviciile publice cu acces limitat.

Serviciile publice cu acces limitat se împart, după condițiile regimului lor juridic, în servicii publice ce conțin informație atribuită la secretul de stat şi servicii publice ce conțin informație confidențială. Atribuirea informației la secretul de stat se efectuează în conformitate cu Legea Republicii Moldova „Cu privire la secretul de stat" nr. 245 din 27.11.2008.

Procesul de prestare a serviciilor publice cu acces limitat sînt supuse protecției. Pentru asigurarea accesului la serviciile publice cu acces limitat sînt utilizate mecanismele semnăturii digitale şi un sistem informațional specializat. Modul de aplicare a mecanismelor semnăturii digitale este stabilit de prevederile legislației naționale în vigoare.

Pentru efectuarea lucrărilor de asigurare a protecției procesului de prestare a serviciilor publice cu acces limitat sînt mobilizate organizații ce dețin licențe pentru activitate în domeniul protecției criptografice sau tehnice a informației şi după caz certificat de securitate în conformitate cu legislația în vigoare. Pentru prelucrarea şi protecția informației cu acces limitat trebuie să fie utilizate mijloace tehnice certificate în modul stabilit.

Regimul utilizării informației atribuite la categoria cu acces limitat, în partea ce nu se referă la secret de stat, este stabilit în Legea Republicii Moldova „Privind accesul la informație" nr. 982-XIV din 11.05.2000.

Autoritățile administrației publice trebuie să asigure un acces echitabil pentru toți subiecții interesați (cetățeni, organizații, autorități ale administrației publice) la serviciile publice general accesibile şi la informația oficială ce ține de activitatea autorităților administrației publice.

Dreptul de a utiliza serviciile publice cu acces limitat îl dețin doar autoritățile administrației publice în conformitate cu gradul de secretizare a informațiilor.

Pentru a proteja informația contra denaturării intenționate sau neintenționate în procesul de prestare a serviciilor publice este necesar de îndeplinit următoarele cerințe:

- de ținut evidența listei de utilizatori ce operează cu sistemul şi a datelor de evidență ale acestora;
- de organizat o protecție sigură a datelor de evidență ale utilizatorilor contra accesului neautorizat;
- de ținut registrul de evidență (audit) a (al) accesului utilizatorilor la resursele informaționale.

6.5. Evidența electronică a serviciilor publice

Evidența electronică a serviciilor publice reprezintă evidența în care cel puțin o parte din datele de evidență sînt utilizate şi oferite utilizatorului exclusiv în formă electronică.

Sistemul de evidență electronică a serviciilor publice este destinat pentru:

- confirmarea efectuării procedurilor necesare de evidență de către persoanele abilitate ca participanți la procesele administrative;
- asigurarea importanței juridice a datelor de evidență electronice.

Sistemul de evidență electronică a serviciilor publice trebuie să includă următoarele subsisteme:

- de asigurare a încrederii pentru semnăturile digitale (confirmarea identității persoanelor abilitate);
- de confirmat electronic (confirmarea timpului de efectuare a înregistrărilor de evidență);
- de arhivare exterioară (asigurarea salvării datelor de evidență);

- de revelare a informației (asigurarea accesului deschis la datele de evidență);
- de înregistrare a sistemelor de evidență electronică de stat.

Pentru sistemele de evidență de stat a serviciilor publice este necesar să fie menținută starea de disponibilitate permanentă pentru a trece în regimul extraordinar de funcționare fără utilizarea tehnologiilor electronice, fapt pentru care evidența pe suport de hîrtie trebuie să dubleze evidența electronică în regim de timp real (fără a prejudicia importanța juridică a evidenței electronice).

La cele mai importante sisteme de evidență de stat a serviciilor publice, se atribuie:
- „Registrul de stat al populației”;
- „Registrul de stat al unităților de drept”;
- „Sistemul informațional geografic național”;
- „Resursele informaționale ale autorităților administrației publice”;
- „Resursele informaționale în sfera socială”;
- „Resursele informaționale în sfera economico-financiară”;
- „Cadastrele resurselor naturale şi ale potențialului tehnogen”.

Sistemele de evidență electronică de stat trebuie să asigure posibilitatea exercitării diferitor tipuri de control privind utilizarea acestora, inclusiv controlul intern şi extern, precum şi posibilitatea realizării auditului informațional privind corespundea cerințelor, stabilite față de aceste sisteme.

Obiectele controlului şi auditului sînt complexele de software şi hardware ce asigură ținerea evidenței electronice a serviciilor publice:
- utilajul de calcul şi telecomunicații;
- canalele de comunicație;
- utilajul tehnico-ingineresc care asigură funcționarea mijloacelor de calcul şi telecomunicații;
- software-ul aplicativ şi de sistem.

7. Asigurarea securității informaționale

Modul de acumulare, procesare, utilizare a informației încadrate în categoria confidențială, regulile de protecție a acesteia şi modul de acces la aceasta, sînt reglementate în conformitate cu legislația națională în vigoare.

Modul de acumulare, procesare, utilizare a informației încadrate în categoria date cu caracter personal se stabileşte în conformitate cu Legea „Cu privire la protecția datelor cu caracter personal” nr. 17-XVI din 15.02.2007.

Pentru asigurarea securității informaționale a sistemului de evidență a serviciilor publice este necesar de a îndeplini următoarele cerințe:
- asigurarea juridică, organizațională şi tehnică a securității serviciilor publice a sistemelor informaționale, a mijloacelor de comunicare şi a rețelelor informaționale;
- delimitarea volumelor şi conținutului informației care poate fi accesibilă diferitor categorii de utilizatori;
- identificarea pericolelor securității informaționale în procesul selectării şi procurării mijloacelor software şi hardware, creării şi exploatării sistemelor informaționale, profilaxiei şi prevenirii acestora, precum şi în procesul lichidării consecințelor nefavorabile în caz de survenire a acestora, inclusiv compensarea prejudiciului material;
- respectarea condițiilor de păstrare şi protecție a documentelor electronice şi de altă natură, ce asigură păstrarea atributelor ce le identifică;
- respectarea regulilor stabilite de utilizare a mijloacelor de protecție criptografică.

Mijloacele software şi hardware pentru protecția sistemului de evidență a serviciilor publice trebuie să asigure:
- depistarea şi prevenirea pericolelor securității informaționale;
- integritatea datelor la formarea, utilizarea, prelucrarea, prestarea serviciilor publice;

- protecția contra accesului neautorizat, introducerii completărilor şi modificărilor în serviciile publice;
- sistemul de rezervare şi restabilire a datelor;
- controlul integrității şi capacității de lucru a sistemului de asigurare a securității informaționale;
- identificarea serviciilor publice protejate;
- autentificarea serviciilor publice protejate şi a utilizatorilor;
- schimbul de date autentificat;
- delimitarea accesului utilizatorilor la date;
- înregistrarea acțiunilor de intrare a utilizatorilor în sistem şi de ieşire din sistem şi încălcărilor drepturilor de acces la serviciile publice protejate.

Anexa nr. 2
la Ordinul nr. 94
din 17.09.2009

REGLEMENTARE TEHNICĂ
Prestarea serviciilor publice electronice
Cerințe tehnice

1. Domeniu de aplicare

În prezenta reglementare sînt stabilite cerințele generale față de procesul prestării serviciilor publice prin mijloace electronice (în continuare – servicii publice).

În prezenta reglementare sînt stabilite cerințele față de organizarea procesului de prestare a serviciilor publice şi sînt specificate componentele obligatorii ale procesului de prestare a serviciilor publice, care asigură calitatea, transparența şi eficiența funcționării procesului.

În prezenta reglementare este stabilit un ansamblu de procese, lucrări şi sarcini destinate organizării şi gestionării procesului de prestare a serviciilor publice.

Obiectivul prezentei reglementării constă în stabilirea cerințelor care asigură un acces eficient la informația oficială, prestarea serviciilor publice cetățenilor, comunității de afaceri şi organelor administrației publice cu aplicarea mijloacelor electronice, perfecționarea calității serviciilor publice, sporirea eficienței activității administrației publice, transparența în activitatea organelor administrației publice, dezvoltarea bazei de implementare a guvernării electronice şi a democrației electronice.

Prezenta reglementare este destinată: clienților sistemelor informaționale (SI) automatizate, serviciilor şi produselor software; furnizorilor; elaboratorilor; administratorilor de SI; managerilor de proiect; managerilor responsabili de calitate şi utilizatorilor de produse software, care sînt participanți la procesul de prestare a serviciilor publice cetățenilor, comunității de afaceri, organelor administrației publice prin mijloacele electronice.

2. Baza juridico-normativă

Prezenta reglementare este elaborată în baza următoarelor acte legislative ale Republicii Moldova:
- Legea Republicii Moldova privind accesul la informație nr. 982-XIV din 11.05.2000;
- Legea Republicii Moldova cu privire la informatizare şi resursele informaționale de stat nr. 467-XV din 21.11.2003;
- Legea Republicii Moldova cu privire la documentul electronic şi semnătura digitală nr.264-XV din 15.07.2004;
- Legea Republicii Moldova privind comerțul electronic nr.284-XV din 22.07.2004;
- Legea Republicii Moldova privind activitatea de reglementare tehnică nr.420-XVI din 22.12.2006;
- Legea Republicii Moldova cu privire la protecția datelor cu caracter personal nr.17-XVI din 15.02.2007;

- Legea Republicii Moldova cu privire la registre nr.71-XVI din 22.03.2007.

3. Terminologie

În prezenta reglementare sînt utilizaţi următorii termeni:

Acord privind nivelul de deservire – acord încheiat în scris între furnizorul de servicii şi client (clienţi), în care se stipulează nivelurile de deservire convenite pentru un serviciu anumit.

Asamblare – ultima etapă a creării unei configuraţii disponibile pentru a fi exploatată.

Baza de date configurațională a elementelor de evidență – bază de date care conține toate datele necesare cu privire la fiecare element de evidență şi date despre legăturile importante dintre acestea.

Biblioteca software – totalitatea controlabilă a elementelor de evidență ale configurației tipului de software destinat pentru susținerea integrității stării lor generale şi a tipului, şi care în acelaşi timp stochează elemente în mod separat, pentru a contribui la elaborare, exploatare şi mentenanță.

Biblioteca software-ului etalon – biblioteca în care sînt stocate sub protecție versiunile etalon ale tuturor elementelor de evidență ale configurației tipului de software.

Catalogul serviciilor – un document de volum mic, de pînă la 7 pagini, în care sînt formulate toate serviciile prestate clientului, în caz de necesitate este indicat costul serviciului, ordinea generală de solicitare a serviciului.

Categoria - clasificarea grupei elementelor de evidență, a documentelor despre modificări sau probleme.

Ciclu de viață – succesiunea proceselor, acțiunilor şi sarcinilor implicate în elaborarea, exploatarea şi mentenanța sistemului şi care cuprind toată durata vieții sistemului.

Controlul configurațiilor – acțiuni incluse în controlul modificărilor operate în elementele de evidență după perfectarea formală a documentației de configurație a acestora.

Controlul procesului – proces de planificare şi reglare, al cărui scop constă în desfăşurarea eficientă şi rațională a procesului.

Conturul extern al guvernării electronice – include infrastructura publică care asigură interacțiunea cetățenilor şi organizațiilor cu organele administrației publice. Acest tip de contur este format din sisteme informaționale care deservesc procesele de interacțiune a populației şi organizațiilor cu organele administrației publice prin intermediul portalului guvernamental.

Conturul intern al guvernării electronice – include sistemele informaționale de deservire a proceselor din interiorul sistemului de administrare publică (G2G), inclusiv prestarea serviciilor interne (G2E) structurilor şi funcționarilor din administrație atît la nivel central cît şi la cel local.

Delta-release – release parțial care include doar acele elemente de evidență în limitele unei unități de release care au fost modificate sau elementele de evidență noi din momentul ultimului release deplin sau delta-release.

Documentație de configurație – documentația care determină cerințele față de elementul de evidență, proiectarea sistemului, asamblarea, producerea şi verificarea elementului de evidență.

Element de evidență – component al infrastructurii care se află sub controlul gestiunii configurațiilor (inclusiv hardware, software şi documentația).

Eroare cunoscută – incident sau problemă a cărei cauză de bază este cunoscută şi pentru care a fost găsită o soluție alternativă.

Gestionarea configurațiilor – procesul de identificare şi determinare a elementelor de evidență din sistem, a înregistrărilor şi a rapoartelor privind statutul elementelor de evidență şi solicitărilor de modificare, precum şi de verificare a plenitudinii şi corectitudinii elementelor de evidență.

Gestionarea modificărilor – procesul de control al modificărilor din infrastructură sau din orice altă componentă a serviciilor prestate, care pune în acțiune în termene minime modificările aprobate.

Graficul de modificări coordonat – graficul ce conține date despre toate modificările aprobate

pentru implementare şi termenele de implementare propuse.

NOTĂ - Graficul de modificări se coordonează cu clientul, gestionarea nivelului de deservire, cu Centrul Informațional de prestare a serviciilor şi cu gestionarea accesibilității.

Identificarea configurației – activitatea care determină structura produsului, ansamblul de elemente de evidență şi documentația caracteristicilor fizice şi funcționale ale elementului de evidență.

Identificatorul versiunii – numărul versiunii; data versiunii sau data versiunii şi marcajul de timp.

Infrastructura TI – sistemul structurilor organizaționale şi a mijloacelor tehnice de programă care asigură funcționarea şi dezvoltarea sistemului informațional şi a mijloacelor de interacțiune informațională.

NOTĂ - Infrastructura TI include totalitatea de mijloace hardware, sisteme operaționale, a rețelei de telecomunicații şi sistemului de comunicații, a bazelor de date, mijloacelor de suport, mijloacelor multimedia care asigură sistemul de formare, distribuire şi utilizare a tehnologiilor comunicaționale ce asigură interacțiunea organelor administrației publice, permițînd accesul la resursele informaționale.

Înregistrarea privind modificarea – înregistrarea de evidență ce conține date despre elementele de evidență care sînt influențate de modificarea aprobată şi modul în care sînt influențate.

Mediu – totalitatea de hardware şi software, de comunicații de rețea şi proceduri care operează împreună în vederea prestării serviciilor publice.

Mediul de program – software utilizat pentru întreținerea aplicațiilor, precum sînt sistemul operațional, sistemul de gestionare a bazei de date, mijloacele de elaborare, compilatoarele şi software-ul aplicativ.

Mijloace de elaborare automată a sistemelor – mijloc software pentru elaboratorii de software-ului, care acordă asistență în planificarea, analiza, proiectarea şi documentarea software-ului.

Mijloc de gestionare a configurațiilor – produs software ce asigură automatizarea susținerii modificărilor, configurațiilor şi a controlului versiunilor.

Politica gestionării accesului – regulile de acordare a accesului la sistemele computerizate şi la rețeaua de utilizatori individuali.

Prestarea serviciilor publice – ansamblu de procese interconexe orientate spre realizarea obiectivelor – interacțiunea dintre subiecții guvernării electronice ce se realizează pe două contururi clare – intern şi extern, care comunică între ele prin intermediul portalului guvernamental.

Problema – cauza primară necunoscută a unuia sau mai multor incidente.

Produs informațional – informație documentată prelucrată în conformitate cu necesitățile utilizatorilor şi prezentată sub formă de produs;.

NOTĂ - Produse informaționale sînt software-ul, bazele şi băncile de date şi altă informație.

Registrul modificărilor – registrul solicitărilor de modificare care au fost perfectate în timpul proiectului, ce arată informația despre fiecare modificare, evaluarea acesteia, deciziile luate.

Release – totalitatea elementelor de evidență noi şi/sau modificate care sînt supuse testării şi sînt date în exploatare în mod colectiv.

Release complex – toate componentele unei unități de release, care sînt colectate, testate, distribuite şi implementate în mod colectiv.

Serviciile informaționale – servicii orientate spre satisfacerea necesităților informaționale ale utilizatorilor prin intermediul furnizării produselor informaționale.

Serviciu public – serviciu, care condiționează trei tipuri de interacțiuni, părți componente ale guvernării electronice: interacțiunea „Guvern - Cetățean” (G2C); interacțiunea „Guvern - Business” (G2B); interacțiunea „Guvern - Guvern” (G2G) cu subcategoria „Interacțiunea dintre Guvern şi

angajații acestuia” (G2E).

Solicitare de deservire – orice incident ce nu reprezintă un defect în funcționarea infrastructurii.

Solicitare de modificare – forma utilizată pentru înscrierea datelor despre solicitarea de modificare pentru orice element de evidență a infrastructurii sau pentru procedurile şi elementele legate de această infrastructură.

Soluție de ocolire – metoda ce permite înlăturarea incidentelor sau a problemelor cu ajutorul unei decizii sau metode temporare, datorită căreia clientul nu mai depinde de un anumit aspect al serviciului legat de problemă.

Soluție permanentă – soluție, aplicarea căreia înlătură cauza de bază a problemei apărute.

Soluționarea problemei – procesul înlăturării problemei pe calea elaborării şi aplicării unei soluții permanente.

4. Cerințele față de organizarea procesului de prestare a serviciilor publice

Esența activității organizației ce prestează servicii publice constă în gestionarea prestării serviciilor publice. Rezultatele acestei activități reprezintă servicii publice justificate ca preț, sigure, reciproc coordonate şi de calitate corespunzătoare.

Sistemul de prestare a serviciilor publice este prevăzut pentru realizarea următorului complex de sarcini:

- sporirea fiabilității de funcționare a SI;
- reducerea timpului de depistare şi lichidare a defectelor în procesul de prestare a serviciilor publice;
- reglementarea activității subdiviziunilor şi sporirea manevrabilității serviciilor responsabile de exploatarea SI;
- crearea mecanismelor de evaluare a contribuției tehnologiilor informaționale (TI) în privința rezultatelor de producție şi a mecanismelor de justificare a investițiilor în infrastructura TI;
- implementarea mijloacelor de planificare şi evaluare a necesităților infrastructurii TI;
- optimizarea cheltuielilor pentru exploatarea SI;
- reducerea termenelor de implementare a noilor proiecte de prestare a serviciilor publice;
- asigurarea acumulării şi aplicării cunoştințelor şi experienței din sfera exploatării infrastructurii TI.

În prezentul capitol sînt stabilite cerințele de bază privind organizarea procesului de prestare a serviciilor publice ce țin de securitate şi calitate, condițiile de realizare şi aplicare, precum şi criteriile de organizare corectă şi evaluare efectivă a conformității serviciilor prestate.

În procesul de prestare a serviciilor publice, este necesar de îndeplinit următoarele procese:

- gestionarea capacităților;
- gestionarea finanțelor pentru prestarea serviciilor publice;
- gestionarea accesibilității;
- gestionarea nivelului de deservire;
- gestionarea continuității acordării serviciilor publice;
- gestionarea securității informaționale;
- gestionarea calității serviciilor publice;
- gestionarea serviciilor de rețea.

4.1. Procesul de gestionare a capacităților

4.1.1. Obiectivele procesului de gestionare a capacităților

Obiectivul procesului de gestionare a capacităților constă în asigurarea prestării nivelului necesar de servicii ce corespund cerințelor, cu cheltuieli minime.

Procesul de gestionare a capacităților mijloacelor de echipament şi de telecomunicații trebuie să fie orientat spre:

- furnizarea constantă a resurselor informaționale necesare în conformitate cu parametrii necesităților, timpului și prețului;
- prevenirea investițiilor nejustificate în SI şi tehnologiile prin utilizarea optimă a resurselor existente;
- sporirea oportună a capacității;
- gestionarea utilizării capacităților curente ale TI şi SI.

Procesul de gestionare a capacităților cu funcționare optimă trebuie să asigure realizarea următoarelor sarcini:

- reducerea riscurilor legate de serviciile existente prin gestionarea efectivă a resurselor şi monitorizarea permanentă a productivității utilajului;
- reducerea pericolului de întrerupere a lucrărilor proceselor de prestare a serviciilor publice în baza cooperării strînse cu procesul de gestionare a modificărilor la determinarea acțiunii modificărilor asupra capacităților TI şi mijloacelor de telecomunicații şi la prevenirea modificărilor urgente din cauza calculării greşite a capacității mijloacelor;
- elaborarea unor pronosticuri mai precise şi reacționarea rapidă la solicitările clientului sau ale utilizatorilor;
- asigurarea raționalității lucrului prin intermediul asigurării anticipate a echilibrului dintre cerere şi ofertă, legate de serviciile noi şi cele modificate;
- gestionarea (reducerea) cheltuielilor legate de capacitatea mijloacelor, în vederea folosirii mai raționale a acestora.

4.1.2. Cerințele de bază față de procesul de gestionare a capacităților

Față de procesul de gestionare a capacităților sînt înaintate trei categorii de cerințe:

- gestionarea capacităților organizației — îndeplinirea acestor cerințe este necesară pentru înțelegerea viitoarelor necesități ale utilizatorilor, determinarea tendințelor, prognozelor, modelarea, crearea prototipului, determinarea volumului şi documentarea viitoarelor necesități ale organizației;
- gestionarea capacităților de deservire – îndeplinirea acestor cerințe contribuie la determinarea şi înțelegerea nivelului de utilizare a serviciilor publice de către utilizatori, la monitorizarea, analiza, setarea şi crearea rapoartelor privind productivitatea serviciilor, la stabilirea configurațiilor de bază şi a profilurilor de utilizare a serviciilor, la gestionarea cererii pentru servicii;
- gestionarea capacităților resurselor – aceste cerințe sînt destinate pentru determinarea şi înțelegerea utilizării infrastructurii TI, monitorizarea, analiza şi crearea rapoartelor privind utilizarea elementelor de evidență, determinarea configurațiilor şi a profilurilor de bază ale utilizării elementelor de evidență. În procesul îndeplinirii acestei categorii de cerințe, o activitate importantă este monitorizarea activă a tendințelor de dezvoltare.

Tabelul 1. Cerințele înaintate față de procesul de gestionare a capacităților

Cerințe	Acțiuni	Descrierea acțiunilor
Gestionarea capacităților organizației	Elaborarea planului privind capacitățile	Descrierea capacităților existente ale infrastructurii TI şi a modificărilor preconizate în cererea de servicii publice, descrierea substituirii componentelor învechite şi a planurilor de dezvoltare tehnică. În planul privind capacitățile sunt descrise modificările aşteptate şi cheltuielile aferente acestora
	Modelarea	Pronosticarea tendințelor infrastructurii TI
	Determinarea	Determinarea configurațiilor hardware-ului

	hardware-ului şi a sistemelor de comunicaţii pentru funcţionarea software-ului	necesar pentru funcţionarea unor aplicaţii noi sau modificate. Rezultatul determinării dimensiunilor platformei tehnice este reflectat de indicatorii sarcinii de lucru
Gestionarea capacităţilor de deservire	Monitorizarea componentelor infrastructurii TI	Garantarea realizării nivelurilor convenite de deservire
	Analiza datelor monitorizării	Se efectuează de către subdiviziunea securităţii
	Setarea	Optimizarea sistemelor pentru sarcina de lucru curentă sau preconizată în baza rezultatelor analizei şi interpretării datelor monitorizării
	Implementarea	Introducerea capacităţii modificate sau noi
Gestionarea capacităţilor resurselor	Gestionarea cererii	Studierea impactului diferitor factori asupra cererii de utilizare a capacităţilor resurselor şi furnizarea informaţiilor pentru elaborarea, monitorizarea şi corectarea planului privind capacităţile şi a acordurilor privind nivelurile de deservire
	Completarea bazei de date a capacităţilor	Colectarea şi actualizarea informaţiilor tehnice, organizaţionale şi de orice altă natură privind gestionarea capacităţilor

4.1.3 Gestionarea eficienţei procesului de gestionare a capacităţilor

Reducerea riscurilor, sporirea calităţii serviciilor prestate, utilizarea eficientă a resurselor şi sistemelor informaţionale urmează să fie asigurate prin respectarea cerinţelor înaintate procesului de gestionare a capacităţilor. Respectarea cerinţelor trebuie să fie reflectată în indicatorii principali ai eficienţei activităţii procesului de gestionare a capacităţilor. Indicatorii menţionaţi sînt prezentaţi în tabelul 2.

Tabelul 2. Indicatorii eficienţei activităţii procesului de gestionare a capacităţilor

Indicatorul eficienţei	Descrierea indicatorului eficienţei
Predictabilitatea necesităţilor clientului	Determinarea modificărilor în sarcina de lucru şi în tendinţele acestora, determinarea exactităţii planului privind capacităţile
Tehnologie	Diverse variante de măsurare a productivităţii serviciilor publice prestate, ritmurile implementării noilor tehnologii şi posibilitatea de a îndeplini permanent Acordului privind nivelul de deservire
Cheltuieli	Reducerea numărului de achiziţii urgente, reducerea capacităţilor inutile sau costisitoare excedentare

Activitatea operațională a TI	Reducerea numărului de incidente cauzate de problemele de productivitate, de satisfacerea cerințelor utilizatorilor în orice moment şi de gradul de seriozitate privind atitudinea organizației față de procesul de gestionare a capacităților

Dările de seamă ale administrației privind procesul de gestionare a capacităților trebuie să conțină informații privind diferențele dintre utilizarea reala şi cea planificată a capacităților, despre tendințele diferențelor, despre impactul asupra nivelului de deservire, reducerea/sporirea preconizată a utilizării capacităților în perspectivă de durată scurtă sau lungă, precum şi date despre valorile limită pentru atingerea cărora va fi necesară achiziționarea unor capacități suplimentare.

4.2. Procesul de gestionare a finanțelor destinate pentru prestarea serviciilor publice

4.2.1. Obiectivele procesului de gestionare a finanțelor destinate pentru prestarea serviciilor publice

Obiectivul procesului de gestionare a finanțelor constă în asistența acordată organizației în gestionarea eficientă a resurselor şi sistemelor informaționale necesare pentru prestarea serviciilor.

La achitarea facturii pentru serviciile publice prestate, un moment important pentru clienți este aprecierea în ce măsură cheltuielile justifică avantajele obținute pentru organizație.

Procesul de gestionare a finanțelor pentru prestarea serviciilor publice, cu funcționare optimă, trebuie să asigure realizarea următoarelor sarcini:

- elaborarea bugetului – planificarea activității organizației şi controlul ei;
- evidența contabilă – determinarea elementelor de cheltuieli şi a metodelor de structurare a acestora;
- eliberarea facturilor – analiza variantelor posibile de eliberare a facturilor şi stabilirea tarifelor pentru servicii.

4.2.2. Cerințele de bază față de procesul de gestionare a finanțelor pentru prestarea serviciilor publice

Furnizarea informației ample pentru justificarea cheltuielilor, analiza serviciilor publice, restituirea cheltuielilor pentru serviciile publice, elaborarea bugetului şi a planurilor se efectuează luîndu-se în considerație următorii factori:

- calitatea – în domeniul activității operaționale: capacitatea (capacitatea de trecere); accesibilitatea; productivitatea; restabilirea după situații extraordinare; susținerea;
- costul – în domeniul cheltuielilor şi investițiilor;
- cerințele clientului – costul şi calitatea trebuie să fie în corespundere cu necesitățile clientului.

Față de procesul de administrare a finanțelor pentru prestarea serviciilor publice sînt înaintate următoarele cerințe:

- determinarea cheltuielilor pentru serviciile publice;
- determinarea şi clasificarea structurii cheltuielilor;
- repartizarea corectă a cheltuielilor conform serviciilor publice prestate clienților;
- utilizarea diferitor metode de eliberare a facturilor pentru utilizarea serviciilor publice;
- compensarea tuturor cheltuielilor, inclusiv a celor capitale, din contul clientului;
- verificarea regulată a facturilor pentru plata serviciilor publice din punct de vedere a corectitudinii şi corespunderii cu cerințele clientului;
- includerea devizului de cheltuieli în rapoartele prezentate clienților.

Pentru asigurarea rentabilității procesului de prestare a serviciilor publice, este necesar de implementat un sistem eficient de control al cheltuielilor care trebuie să îndeplinească următoarele

cerințe:

- susținerea în elaborarea strategiei de investiții care să contribuie la flexibilitatea organizației în baza utilizării mijloacelor tehnologice moderne;
- asistență la stabilirea priorităților în utilizarea resurselor informaționale;
- asigurarea acoperirii cheltuielilor pentru toate resursele informaționale utilizate de organizație;
- asistența pentru administrație la luarea deciziilor operative cotidiene pentru reducerea riscului financiar în procesul de adoptare a deciziilor pe termen lung;
- asigurarea flexibilității şi a capacității de a reacționa rapid la modificările în procesele de prestare a serviciilor publice.

4.2.3. Clasificarea cheltuielilor legate de procesul de prestare a serviciilor publice

Informația despre cheltuielile aferente prestării serviciile publice permite de a echilibra cheltuielile şi calitatea, precum şi de a oferi clienților un proces de prestare a serviciilor argumentat din punct de vedere financiar.

Pentru fiecare serviciu este necesar de a determina cheltuielile legate direct sau indirect de acesta:

- cheltuieli directe – cheltuielile legate în mod particular şi exclusiv de un anumit serviciu public (de exemplu, locațiunea unei linii telefonice pentru acces la rețeaua Internet);
- cheltuieli indirecte – cheltuielile ce nu sînt legate direct şi nemijlocit de un anumit serviciu public (de exemplu, cheltuielile pentru încăperi, servicii de mentenanță şi cheltuieli administrative).

Cheltuielile aferente prestării serviciilor se împart în permanente şi variabile:

- cheltuielile permanente nu depind de volumul serviciilor prestate (investițiile în hardware, software şi construcție etc.);
- cheltuieli variabile – cheltuieli al căror nivel se schimbă odată cu modificarea volumului de prestare a serviciilor (cheltuielile pentru personalul atras din exterior, cartuşele imprimatelor, hîrtie, încălzire şi electricitate etc.).

În procesul de prestare a serviciilor publice se formează următoarele tipuri de cheltuieli:

- cheltuieli de echipament – toate cheltuielile legate de hardware (servere, dispozitive de păstrare a informației, comunicații şi rețele, imprimante etc.);
- cheltuieli de software – cheltuielile directe şi indirecte privind mentenanța funcționării sistemului (software de sistem, sistemul de tranzacții, sistemul de gestiune a bazelor de date, sistemul de elaborare a aplicațiilor, aplicațiile de program etc.);
- cheltuieli organizaționale – cheltuieli directe şi indirecte privind personalul, care pot fi permanente sau variabile (retribuția muncii, cheltuieli de instruire, diurne pentru deplasări);
- cheltuieli pentru amplasare - toate cheltuielile directe sau indirecte legate de amplasare (încăperi pentru servere, oficii, alte încăperi şi echipamente);
- cheltuieli de transfer - cheltuieli legate de plățile interne efectuate între diferite subdiviziuni ale organizației;
- evidența cheltuielilor – cheltuielile legate de procesul de gestionare a finanțelor.

4.2.4. Gestionarea eficienței procesului de gestionare a finanțelor

Indicatorii eficienței procesului de gestionare a finanțelor pentru prestarea serviciilor determină nivelul de corespundere a acestui proces cu cerințele care asigură organizarea corectă a funcționării procesului. Indicatorii principali ai eficienței procesului de gestionare a finanțelor pentru prestarea serviciilor publice sînt:

- analiza exactă a costului serviciilor prestate;
- satisfacția clienților;
- realizarea obiectivelor financiare de către organizație;
- modificarea utilizării serviciilor de către clienți;
- prezentarea la timp a rapoartelor pentru procesul de gestionare a nivelului de deservire.

4.3. Procesul de gestionare a accesibilității

4.3.1. Obiectivele procesului de gestionare a accesibilității

Obiectivul procesului de gestionare a accesibilității este de a asigura un nivel rentabil şi coordonat de accesibilitate în prestarea serviciilor. Procesul de gestionare a accesibilității este neîntrerupt şi se încheie în momentul cînd se termină prestarea serviciului.

Procesul de gestionare a accesibilității trebuie să includă:

- servicii noi şi curente;
- relațiile cu furnizori interni şi externi;
- componentele infrastructurii şi aspectele organizaționale care influențează accesibilitatea, cum ar fi nivelul de cunoştințe ale personalului, procesele, procedurile şi instrumentele de administrare.

Procesul de gestionare a accesibilității trebuie îndeplinit luîndu-se în considerație următorii factori:

- criteriile de elaborare a arhitecturii informaționale pentru asigurarea accesibilității şi restabilirea serviciilor publice noi şi perfecționate;
- tehnologiile ce asigură stabilitatea infrastructurii TI;
- garanțiile accesibilității, siguranței şi deservirii componentelor infrastructurii;
- complexitatea infrastructurii TI;
- fiabilitatea componentelor – accesibilitatea serviciului într-o perioadă de timp aprobată, fără nici o defecțiune;
- capacitatea de a reacționa rapid şi efectiv la defecțiuni;
- calitatea deservirii şi calitatea activității organizațiilor de mentenanță şi a furnizorilor;
- calitatea şi limitele de competență ale proceselor de administrare operațională.

4.3.2. Cerințele de bază ale procesului de gestionare a accesibilității

În cadrul procesului de gestionare a accesibilității se execută următoarele acțiuni:

- planificarea - stabilirea cerințelor față de accesibilitatea serviciului, proiectarea sistemelor pentru realizarea nivelului necesar de accesibilitate şi a capacității necesare de restabilire;
- monitorizarea - efectuarea măsurărilor şi întocmirea rapoartelor.

Procesul de gestionare a accesibilității în condiții de funcționare optimă trebuie să asigure îndeplinirea următoarelor cerințe:

- crearea unui punct unic de contact pentru chestiunile de accesibilitate a serviciilor publice;
- corespunderea serviciilor prestate cu cerințele înaintate față de accesibilitatea serviciului în conformitate cu legislația în vigoare;
- garanția corespunderii noilor servicii cu cerințele impuse față de acestea şi cu standardul de accesibilitate convenit cu clientul;
- menținerea nivelului cheltuielilor la un nivel acceptabil;
- monitorizarea continuă a standardelor de accesibilitate şi perfecționarea acestora pe măsura necesităților;
- realizarea măsurilor de restabilire în caz de inaccesibilitate a serviciului;
- reducerea numărului refuzurilor de acces la sisteme şi reducerea perioadei de inaccesibilitate a serviciului;
- transferul de prioritate de la corectarea defectelor la îmbunătățirea serviciului.

În caz de întrerupere a procesului de prestare a serviciilor publice este necesar de a înlătura rapid şi corect defectul şi de a realiza standardele aprobate de accesibilitate. Procedura de restabilire include aspecte precum sînt: utilizarea procesului eficient de gestionare a incidentelor (a se vedea 5.1) şi procedurile corespunzătoare de escaladare, informare, copiere de rezervă şi restabilire.

4.3.3. Gestionarea eficienței procesului de gestionare a accesibilității

Este necesar de efectuat monitorizarea şi evaluarea conformității procesului dat cu cerințele

menționate. Indicatorii de bază ai eficacității funcționării procesului de gestionare a accesibilității:
- durata stagnărilor;
- frecvența survenirii stagnărilor;
- durata medie a reparației - durata medie dintre survenirea defectului şi restabilirea serviciului;
- durata medie între defecte - durata medie dintre restabilirea după un defect şi survenirea altuia;
- durata medie între incidentele de sistem – durata medie dintre două incidente succesive;
- coeficientul de accesibilitate (sau inaccesibilitate) a serviciului;
- durata totală de funcționare şi durata stagnării;
- numărul defectelor;
- informația despre defecte;
- durata de depistare, reacționare, restabilire şi reparație a defectului, incidentului sau problemei.

Nivelul de accesibilitate trebuie să asigure accesul permanent la serviciile publice pe calea reducerii timpului de stagnare şi a restabilirii rapide a prestării serviciilor.

4.4. Procesul de gestionare a nivelului de deservire

4.4.1. Scopul procesului de gestionare a nivelului deservirii

Gestionarea nivelului de deservire (serviciului) - este un proces în cadrul căruia au loc negocieri cu privire la prestarea serviciilor, se efectuează stabilirea, evaluarea, gestionarea şi îmbunătățirea calității serviciilor publice cu respectarea nivelului admisibil de cheltuieli. Gestionarea nivelului serviciului necesită o colaborare eficientă şi productivă cu clientul deoarece nivelurile serviciilor solicitate se stabilesc cu participarea acestuia.

Procesul de gestionare a nivelului de deservire este menit să stabilească echilibrul necesar dintre cererea şi oferta pentru serviciile de calitatea necesară, dintre comoditatea utilizării şi cost. Acest proces realizează elaborarea, coordonarea şi executarea Acordurilor cu privire la nivelul de deservire, acordurilor operaționale privind nivelul de deservire, contractelor externe şi planului de asigurare a calității serviciilor.

În cadrul procesului de gestionare a nivelului de deservire trebuie îndeplinite următoarele sarcini:
- integrarea elementelor necesare pentru prestarea serviciilor publice;
- documentarea şi descrierea serviciilor prestate;
- concordarea strategiei TI cu necesitățile organizației;
- controlul îmbunătățirii prestării serviciilor publice.

Nivelul deservirii trebuie analizat în mod regulat, atrăgîndu-se o atenție sporită la următoarele aspecte:
- acordul cu privire la nivelul deservirii din momentul ultimei analize;
- problemele apărute în cadrul serviciilor;
- identificarea tendințelor în activitatea serviciilor;
- modificarea serviciilor în limitele nivelurilor de deservire acordate;
- modificarea procedurilor şi calculelor costului resurselor adiționale;
- analiza urmărilor defectelor la prestarea nivelurilor acordate ale serviciilor.

Fiabilitatea deservirii trebuie să includă îmbinarea următoarelor caracteristici:
- fiabilitatea componentelor utilizate pentru prestarea serviciilor;
- durabilitatea - capacitatea deservirii sau a componentelor sale de a funcționa eficient indiferent de defectarea uneia sau a cîteva subsisteme;
- deservirea profilactică pentru prevenirea întreruperii funcționării.

Deservirea trebuie să cuprindă efectuarea lucrărilor de asigurare a funcționării procesului de prestare a serviciilor şi restabilire a acestuia după defecte, precum şi efectuarea profilaxiei şi a verificărilor regulamentare şi anume:
- luarea măsurilor de prevenire a defectelor;

- depistarea la timp a defectelor;
- efectuarea diagnosticării, inclusiv a autodiagnosticării automate a componentelor;
- lichidarea defectelor;
- restabilirea funcționării după defecțiune;
- restabilirea serviciului.

4.4.2. Cerințele de bază față de procesul de gestionare a nivelului de deservire

Cerințele față de nivelul prestării serviciilor – descrierea detaliată a necesităților clientului utilizate la elaborarea, modificarea şi inițierea serviciilor.

În lista cerințelor urmează să fie incluse următoarele:
- identificarea necesităților clientului;
- determinarea serviciilor necesare corespunzător necesităților şi cerințelor clientului, crearea unui plan de asigurare a calității serviciilor;
- perfectarea finală a acordului - coordonarea cu clientul a nivelului de deservire necesar şi cheltuielile legate de aceasta, fixarea înțelegerilor convenite în Acordul cu privire la nivelul deservirii, acordul operațional privind nivelul de deservire, contractele externe şi întocmirea sau reînnoirea catalogului de servicii;
- monitorizarea nivelurilor serviciilor;
- raportarea privind nivelul serviciilor;
- analiza serviciilor în vederea determinării direcțiilor de perfecționare a acestora;
- descrierea funcțiilor, pe care trebuie să le ofere nivelul de deservire solicitat, din punctul de vedere al clientului;
- timpul şi zilele în care serviciul trebuie să fie accesibil;
- cerințele față de continuitatea procesului de deservire;
- stabilirea funcțiilor informaționale necesare pentru prestarea serviciilor;
- existența referințelor la metodele operaționale şi standardele de calitate curente care trebuie luate în considerație la stabilirea nivelului de deservire;
- confruntarea calității serviciilor cu costul indicat în factură;
- stabilirea obligațiunilor clientului şi ale organizației care prestează servicii publice;
- existența referințelor la Acordul cu privire la nivelul de deservire.

Procesul de gestionare a nivelului de deservire trebuie să garanteze susținerea şi perfecționarea continuă a serviciilor publice solicitate de client, prin coordonarea nivelului calității serviciilor organizației, monitorizarea acestora şi prezentarea rapoartelor.

4.4.3. Gestionarea eficienței procesului de gestionare a nivelului de deservire

Indicatorii eficienței şi eficacității procesului de gestionare a nivelului de deservire:
- parametrii de deservire incluşi în Acordul cu privire la nivelul de deservire;
- parametrii monitorizați şi cu neajunsuri raportate;
- parametrii Acordului cu privire la nivelul de deservire, care sînt analizați în mod regulat;
- parametrii Acordului cu privire la nivelul de deservire, pentru care au fost obținute nivelurile convenite de prestare a serviciilor;
- neajunsurile relevate incluse în planul de perfecționare;
- tendințele relevate, ținîndu-se cont de nivelul real de deservire.

Indicatorii menționați servesc drept instrument pentru determinarea conformității procesului respectiv cu cerințele înaintate.

4.5. Procesul de gestionare a continuității în prestarea serviciilor publice

4.5.1. Scopurile procesului de gestionare a continuității în prestarea serviciilor publice

Obiectivul procesului de gestionare a continuității în prestarea serviciilor publice constă în susținerea procesului de gestionare a continuității în activitatea organizației. Esența acestei susțineri

constă în restabilirea infrastructurii TI şi a serviciilor publice necesare, inclusiv a serviciului de mentenanță şi a tuturor unităților instituționale care asigură prestarea serviciilor, în decursul unei anumite perioade de timp după survenirea situației excepționale.

Accesibilitatea serviciilor publice urmează să includă o îmbinare între măsurile de reducere a gradului de risc şi metodele de restabilire.

În procesul de gestionare a continuității serviciilor publice trebuie îndeplinite următoarele sarcini:

- evaluarea impactului defecțiunilor asupra activității serviciilor publice după survenirea situației excepționale;
- stabilirea serviciilor de importanță sporită pentru organizație care necesită măsuri suplimentare;
- determinarea perioadei de timp în decursul căreia serviciul urmează să fie restabilit;
- luarea măsurilor de prevenire, depistare, pregătire pentru situații excepționale sau de reducere a gradului lor de influență;
- stabilirea metodei generale de abordare a restabilirii serviciilor;
- elaborarea, testarea şi susținerea planului de restabilire cu un nivel suficient de detaliere, care ar ajuta la depăşirea situației excepționale şi la restabilirea activității normale într-o perioadă de timp prestabilită.

4.5.2. Cerințele de bază înaintate procesului de gestionare a continuității în prestarea serviciilor publice

În procesul de gestionare a continuității în prestarea serviciilor publice, trebuie îndeplinite următoarele cerințe:

- existența unui proces eficient de gestionare a configurațiilor
- mentenanța procesului de gestionare a continuității de către personalul organizației;
- existența instrumentelor moderne eficiente;
- efectuarea unei instruiri speciale pentru toți participanții la procesul respectiv;
- testarea regulată a planului de restabilire, fără aviz prealabil.

Pentru îndeplinirea cerințelor menționate este necesar de realizat următoarele activități:

- inițializarea;
- cerințele şi strategia;
- implementarea;
- gestionarea operațională.

Inițializarea – include activitățile de stabilire a sferei de acțiune a procesului de gestionare a continuității serviciilor publice. Pe parcursul inițializării se stabileşte politica organizației față de gestionarea continuității serviciilor publice; se selectează metoda de abordare a evaluării riscului; se evidențiază resursele pentru desfăşurarea mediului informațional în cazul survenirii situațiilor excepționale.

Cerințele şi strategia – includ tipurile de acțiuni indicate în tabelul 3.

Tabelul 3. Tipurile de acțiuni pentru activitatea „Cerințele şi strategia”

Tipuri de acțiuni	Lucrări
Analiza impactului asupra funcționării organizației	1. Constatarea cauzelor şi stabilirea influențelor potențiale a defectelor serioase a serviciilor 2. Efectuarea analizei serviciilor publice 3. Evaluarea factorilor de dependență între servicii şi resursele informaționale

Evaluarea riscurilor	1. Identificarea riscurilor aferente procesului de prestare a serviciilor publice 2. Identificarea pericolelor potențiale, a tipurilor de vulnerabilitate şi stabilirea măsurilor preventive corespunzătoare
Strategia de asigurare a continuității serviciilor TI	1. Realizarea acțiunilor preventive 2. Selectarea metodelor de restabilire a serviciilor publice

Implementarea – include tipurile de acțiuni indicate în tabelul 4.

Tabelul 4. Tipurile de acțiuni pentru activitatea „Implementarea”

Tipuri de acțiuni	Lucrări
Organizarea procesului şi planificarea implementării	Elaborarea planurilor detaliate pentru utilizarea mijloacelor de restabilire selectate: - planul de amplasare şi prestare a serviciilor; - planul de reacționare în situații excepționale; - planul de evaluare a prejudiciilor; - planul de restabilire a activităților; - planul privind telecomunicațiile, - planul de asigurare a securității; - planul privind resursele umane; - planul financiar
Aplicarea acțiunilor preventive şi a metodelor de restabilire	Realizarea acțiunilor preventive de reducere a gradului de influență concomitent cu activitatea în cadrul procesului de gestionare a accesibilității
Elaborarea planurilor şi procedurilor de restabilire	Planurile de restabilire trebuie să includă toate tipurile de activitate pentru restabilirea prestării serviciilor publice
Testarea inițială	Testarea eficienței planurilor şi procedurilor

Gestionarea operațională – include toate tipurile de acțiuni indicate în tabelul 5.

Tabelul 5. Tipurile de acțiuni pentru activitatea „Gestionarea operațională”

Tipuri de acțiuni	Lucrări
Instruirea şi informarea	Instruirea personalului în materie de tehnologii informaționale pentru acordarea de către personal a susținerii necesare în executarea lucrărilor de restabilire
Analiza şi auditul	Auditul şi verificarea actualității tuturor planurilor în toate aspectele procesului de gestionare a continuității serviciilor publice la orice modificare semnificativă a

	infrastructurii TI
Testarea	Testarea regulată a planurilor de restabilire a serviciilor publice
Gestionarea modificărilor	Efectuarea analizei influenţei oricărei modificări asupra planurilor de restabilire a serviciilor publice
Asigurarea garanţiilor	Verificarea corespunderii calităţii procesului (procedurilor şi documentaţiei) cu necesităţile

4.5.3. Gestionarea eficienţei procesului de gestionare a continuităţii în prestarea serviciilor publice

Gestionarea restabilirii SI şi reducerea stagnărilor în activitatea de prestare a serviciilor publice necesită respectarea cerinţelor înaintate procesului de gestionare a continuităţii în prestarea serviciilor publice, conformitatea cărora este reflectată în următorii indicatori:

- numărul erorilor depistate în planurile de restabilire;
- pierderea de către organizaţie a venitului în rezultatul unei situaţii excepţionale;
- costul procesului.

4.6. Procesul de gestionare a securităţii informaţionale

4.6.1. Obiectivele, sarcinile şi principiile procesului de gestionare a securităţii informaţionale

Obiectivul procesului de gestionare a securităţii informaţionale constă în controlul proceselor de asigurare cu informaţie, prevenirea divulgării, pierderii, scurgerii, denaturării şi distrugerii informaţiei şi prevenirea defecţiunilor în activitatea procesului de prestare a serviciilor publice.

Procesul de gestionare a securităţii informaţionale este necesar pentru susţinerea funcţionării continue a organizaţiei. Sarcina procesului constă în asigurarea continuă a securităţii serviciilor la nivelul coordonat cu clientul.

Procesul de gestionare a securităţii informaţionale trebuie să fie desfăşurat în baza următoarelor principii:

- principiul capacităţii echivalente a sistemului de protecţie – asigurarea protecţiei hardware-ului, software-ului, a sistemului de comunicaţii şi a sistemului de gestionare contra tuturor tipurilor de pericole;
- principiul continuităţii protecţiei – în procesul de prestare a serviciilor trebuie să fie asigurată continuitatea protecţiei informaţiei;
- principiul suficienţei rezonabile – aplicarea măsurilor şi a mijloacelor de protecţie rezonabile, raţionale care implică cheltuieli ce nu depăşesc costul încălcării securităţii informaţionale;
- principiul complexităţii – aplicarea tuturor tipurilor şi formelor de protecţie în volum deplin;
- principiul fiabilităţii - metodele, mijloacele şi formele de protecţie trebuie să blocheze în mod sigur toate căile de pătrundere şi canalele posibile de scurgere a informaţiei;
- principiul universalităţii – măsurile de securitate trebuie să blocheze căile pericolelor indiferent de punctul de acţiune potenţială a acestora;
- principiul planificării – elaborarea planurilor de acţiuni detaliate pentru asigurarea protecţiei informaţionale a tuturor componentelor sistemului de prestare a serviciilor publice;
- principiul centralizării – asigurarea independenţei organizaţionale şi funcţionale a procesului de asigurare a securităţii prestării serviciilor publice;
- principiul calificării personalului de deservire – prestarea serviciilor şi deservirea echipamentului trebuie să fie realizate de angajaţii pregătiţi în probleme de exploatare a tehnicii şi aspecte de ordin tehnic privind asigurarea securităţii informaţionale;

- principiul repartizării împuternicirilor – responsabilitatea pentru sistemul de protecție trebuie să fie repartizată între angajații de diferite niveluri şi pe diferite direcții ale activității de protecție.

4.6.2. Cerințele de bază față de procesul de gestionare a securității informaționale

Reieşind din aspectele accesibilității, integrității şi confidențialității informației, procesul de gestionare a securității informaționale trebuie să corespundă următoarelor cerințe:

- să asigure confidențialitatea informației importante;
- să asigure integritatea informației şi a proceselor legate de aceasta (crearea, introducerea, extragerea, păstrarea, transmiterea etc.);
- să asigure accesibilitatea la timp a informației;
- să asigure funcționarea fără deficiențe în procesul realizării unor operații concrete;
- să asigure monitorizarea în vederea asigurării capacității proceselor TI de a fixa orice activitate a utilizatorilor sau a proceselor;
- să țină evidența tuturor proceselor şi evenimentelor legate de informație.

Pentru realizarea cerințelor înaintate procesului de gestionare a securității informaționale este necesar de îndeplinit următoarele condiții:

- crearea schemei structurale de gestionare;
- crearea structurii organizaționale de gestionare;
- repartizarea detaliată a responsabilităților;
- coordonarea securității informaționale;
- coordonarea instrumentelor;
- descrierea procesului de autorizare a mijloacelor TI;
- acordarea consultațiilor de către specialişti;
- colaborarea între organizații, interacțiunea internă şi externă;
- efectuarea auditului independent al sistemelor informaționale;
- respectarea principiilor de securitate la accesarea informației persoanelor terțe.

În cadrul procesului de gestionare a securității informaționale sau în cadrul altor procese aflate sub controlul gestionării securității informaționale se realizează următoarele activități:

- controlul - politica şi organizarea securității informaționale, formularea planurilor de securitate, realizarea acestora, evaluarea realizării şi includerea evaluării în planurile anuale de securitate. Acest tip de activitate stabileşte subprocesele, funcțiile de securitate, rolurile şi responsabilitățile, descrie structura organizatorică, sistemul de raportare şi fluxurile de gestionare;
- planificarea – se stabileşte conținutul capitolului privind securitatea din cadrul Acordului cu privire la nivelul de deservire, cu participarea procesului de gestionare a nivelului de deservire şi sînt descrise acțiunile privind aspectele de securitate desfăşurate în cadrul acordurilor externe;
- realizarea;
- evaluarea realizării activităților planificate – necesar de aplicat următoarele tipuri de evaluare: evaluarea independentă, auditul intern, auditul extern;
- susținerea capitolelor corespunzătoare privind securitatea din cadrul Acordurilor cu privire la nivelul de deservire şi din planurile de securitate;
- întocmirea rapoartelor – se prezintă informația din cadrul altor procese cu privire la caracteristicile de securitate obținute şi problemele de securitate.

Realizarea procesului de gestionare a securității informaționale este susținută prin executarea sarcinilor prezentate în tabelul 6.

Tabelul 6. Sarcinile executate la realizarea procesului de gestionare a securității informaționale

Sarcinile procesului	Descrierea sarcinilor procesului

Clasificarea şi gestionarea resurselor informaționale	Furnizarea datelor de intrare pentru mentenanța bazei de date de Configurație a elementelor de evidență, clasificarea resurselor informaționale în conformitate cu principiile acordate
Securitatea personalului	Sarcinile şi responsabilitățile personalului, acordurile de confidențialitate pentru personal, instruirea personalului, instrucțiunile pentru personal privind soluționarea incidentelor legate de securitate şi înlăturarea defectelor de protecție, măsurile disciplinare, perfecționarea nivelului de informare în probleme de securitate
Gestionarea securității	Implementarea tipurilor de responsabilitate şi repartizarea obligațiilor, măsurilor de securitate care cuprind ciclul întreg de viață al sistemelor; separarea mediului de elaborare şi de testare de mediul operațional, proceduri de prelucrare a incidentelor; utilizarea mijloacelor de restabilire, implementarea măsurilor de protecție împotriva viruşilor; implementarea metodelor de gestionare pentru computere, aplicații, rețele şi serviciile de rețea; utilizarea corectă a suporturilor informaționale şi protecția acestora
Controlul accesului	Implementarea politicii de acces şi control al accesului, susținerea privilegiilor de acces ale utilizatorilor şi aplicațiilor la rețea, serviciile de rețea, computerele şi aplicațiile; susținerea barierelor de protecție în rețea, implementarea metodelor de identificare şi autorizare a sistemelor computerizate, a stațiilor de lucru şi a computerelor personale în rețea

Procesul de gestionare a securității informaționale asigură cu instrucțiuni privind structura activității legate de securitate, altele procese, cum ar fi:

- proces de gestionare a incidentelor - este un proces important care informează despre existența unor incidente legate de securitate. Orice incident, care poate împiedica executarea cerințelor de securitate indicate în Acordul cu privire la nivelul de deservire şi care poate crea obstacole în obținerea nivelului de bază al securității interne, se clasifică ca incident de securitate;
- procesul de gestionare a problemelor - este un proces responsabil de identificarea şi înlăturarea defecțiunilor structurale de securitate care pot conduce la apariția unor riscuri pentru sistemul de securitate. Orice măsuri de siguranță legate de introducerea modificărilor trebuie să fie realizate concomitent cu efectuarea acestor modificări, iar testarea acestora trebuie să fie efectuată în paralel. La testarea securității este verificată nu doar accesibilitatea funcțiilor de securitate, ci şi absența funcțiilor nedorite care ar putea reduce nivelul de securitate a sistemului.

4.6.3. Gestionarea eficienței procesului de asigurare a securității informaționale

Indicatorii în baza cărora se evaluează corespunderea procesului de asigurare a securității informaționale cu cerințele şi condițiile sînt următorii:

- parametrii serviciilor prestate indicați în Acordul cu privire la nivelul de deservire;
- deficiențele relevate incluse în planul de perfecționare;
- corectarea la timp a deficiențelor ajustate, identificate în rezultatul auditului şi analizei;

- numărul de pericole aferente securității identificate;
- numărul de depistări şi lichidări ale intruziunilor;
- probabilitatea realizării pericolelor, incidentelor, problemelor;
- indicatorii evaluării riscului;
- parametrii de reacționare la incidentele legate de încălcarea securității;
- rezultatele monitorizării securității informaționale;
- datele privind controlul curent al stării securității TI.

4.7. Procesul de gestionare a calității serviciilor publice

4.7.1. Obiectivele procesului de gestionare a calității serviciilor publice

Obiectivul principal al procesului de gestionare a calității serviciilor constă în formarea şi menținerea în stare actualizată a catalogului de servicii, a Acordului cu privire la nivelul de deservire, precum şi a acordurilor operaționale interne în care sînt stabilite cerințele față de personal şi față de serviciile prestate.

În Acordul cu privire la nivelul de deservire sînt enumerați toți parametrii serviciilor prestate din acordul încheiat cu organizația care prestează servicii informaționale.

Rezultatul procesului de gestionare a calității serviciilor este format din informația semnificativă şi oportună despre prestarea serviciilor, obținută în rezultatul unei monitorizări specializate eficiente:

- rapoarte privind starea necorespunzătoare a îndeplinirii serviciului;
- notificarea despre problemele care tind să obțină un caracter cronic;
- notificarea despre modalitățile de utilizare a serviciului;
- analiza aprecierilor cu privire la servicii.

Procesul de gestionare a calității serviciilor se realizează în conformitate cu următoarele principii:

- aplicarea metodei de abordare procesuală în organizarea prestării serviciilor;
- măsurarea indicatorilor calității proceselor;
- controlul proceselor în conformitate cu anumite criterii şi perfecționarea continuă a acestora.

4.7.2. Cerințele de bază față de procesul de gestionare a calității serviciilor

În procesul de gestionare a calității serviciilor este necesar de respectat următoarele cerințe:

- recepționarea informației de la procesele de administrare a rețelei, procesele de formare şi prestare a serviciilor şi de la procesele de deservire a clienților;
- elaborarea şi aprobarea unei liste complete a serviciilor prestate;
- planificarea îmbunătățirii calității serviciilor, prin formarea programului de dezvoltare a calității;
- adoptarea măsurilor necesare pentru menținerea nivelului serviciilor în limitele aprobate pentru fiecare clasă de servicii şi pentru satisfacerea necesităților clienților.

În cadrul procesului de gestionare a calității serviciilor, față de personalul care prestează serviciile publice sînt înaintate următoarele cerințe:

- personalul trebuie să conceapă clar cerințele clienților;
- personalul trebuie să poată descrie serviciile în termeni accesibili pentru client;
- personalul trebuie să descrie clar cerințele de prestare a serviciilor pentru executori.

4.7.3. Gestionarea eficienței procesului de gestionare a calității serviciilor

Indicatorii principali ai eficienței procesului de gestionare a calității serviciilor, ce caracterizează corespunderea serviciilor prestate cu cerințele calității indicate în Acordul cu privire la nivelul de deservire, sînt următorii:

- numărul de servicii comandate;
- numărul de solicitări de deservire primite;
- timpul utilizat pentru prestarea serviciilor;
- numărul solicitărilor de deservire expirate;

- numărul incidentelor survenite;
- timpul de staționare a echipamentului;
- durata de inaccesibilitate a serviciului;
- termenul de înlocuire a elementului defectat în infrastructura TI şi condițiile înlocuirii acestuia cu echipament temporar.

4.8. Procesul de gestionare a serviciilor de rețea

4.8.1. Obiectivele procesului de gestionare a serviciilor de rețea

Obiectivul gestionării serviciilor de rețea constă în asigurarea securității sistemelor conectate în rețea şi în controlul conexiunilor la sistemele conectate în rețea.

Gestionarea serviciilor de rețea trebuie să asigure transferul datelor dintr-un sistem în altul. Acest grup de servicii trebuie să includă semantica mediului comun de transferul datelor, rețeaua fizică care cuprinde rețelele locale şi globale, canalele şi protocoalele transferului de date.

Accesul direct la funcțiile serviciilor de rețea este necesar pentru telefonia computerizată, schimbul de informații video, conferința electronică. Sarcina gestionării serviciilor de rețea este de a stabili ansamblul de proceduri aplicate pentru instalarea dinamică, mentenanța şi întreruperea conexiunilor necesare pentru schimbul de date între utilizatorii rețelei şi nodurile de comutație.

4.8.2. Funcțiile şi controlul procesului de gestionare a serviciilor de rețea

Funcțiile de gestionare a serviciilor de rețea stabilesc succesiunea şi formatul necesar al mesajelor, schimbul cărora se efectuează prin interfața de rețea.

În procesul de gestionare a serviciilor de rețea este necesar de efectuat controlul conexiunilor la sistemele conectate prin rețea. Controlul limitării capacității conexiunilor de rețea se efectuează în conformitate cu cerințele politicii de gestionare a accesului.

Controlul se efectuează prin:
- gateway între rețele, care filtrează datele transmise prin rețea cu ajutorul tabelelor şi regulilor prestabilite;
- firewall-uri personale ale utilizatorilor, care filtrează traficul computerului protejat;
- interfețele serviciului între rețele;
- algoritmul de autentificare a utilizatorilor la distanță, a sistemelor computerizate şi a echipamentului;
- controlul deplin al accesului la SI;
- servicii de sistem şi programe aplicative care urmăresc conținutul traficului Web şi de poştă electronică recepționat de calculator.

4.8.3. Cerințele de bază față de organizarea procesului de gestionare a serviciilor de rețea

Față de procesul de gestionare a serviciilor de rețea sînt înaintate următoarele cerințe ce caracterizează evaluarea nivelului de corespundere cu cerințele procesului respectiv:
- monitorizarea stării echipamentului activ de rețea;
- prelucrarea evenimentelor critice care survin în rețea;
- notificarea personalului tehnic despre evenimentele critice în rețea;
- acumularea informației statistice despre funcționarea, productivitatea, încărcarea elementelor critice ale infrastructurii de rețea;
- asigurarea controlului capacității de muncă, accesibilității, productivității echipamentului de server şi aplicațiilor.

5. Gestionarea procesului de prestare a serviciilor

În prezentul capitol sînt examinate procesele integrate de gestionare a incidentelor, problemelor, configurațiilor, modificărilor şi a release-urilor.

5.1. Gestionarea incidentelor

Obiectivul procesului de gestionare a incidentelor constă în restabilirea rapidă a procesului de

prestare a serviciilor publice şi în minimalizarea impactului negativ al incidentelor, asigurînd-se susţinerea celor mai înalte niveluri ale calităţii deservirii şi accesibilităţii.

Incidentele survenite ca urmare a deficienţelor sau erorilor din infrastructura TI conduc la devieri reale sau potenţiale în raport cu activitatea planificată a serviciilor publice. La identificarea cauzei care a provocat incidentul este necesar de perfectat o înregistrare despre problemă cu ajutorul căreia se identifică eroarea de bază. Se realizează o succesiune logică, începînd cu notificarea iniţială şi finalizînd cu soluţionarea problemei iniţiale.

5.1.1. Cerinţele de bază faţă de procesul de gestionare a incidentelor

Faţă de procesul de gestionare a incidentelor sînt înaintate următoarele cerinţe:

- înregistrarea automată a incidentelor şi notificarea în caz de depistare a defecţiunii în mainframe-uri, în reţele şi servere;
- posibilitatea escaladării automate în vederea asigurării prelucrării la timp a incidentelor şi solicitărilor de deservire;
- nivelul înalt de flexibilitate şi marşrutizare a incidentelor;
- selectarea automată a datelor din Baza de date configurațională a elementelor de evidenţă privind elementele de evidenţă defectate şi afectate de incidente;
- software specializat;
- disponibilitatea mijloacelor şi modulelor de diagnosticare.

Centrul de guvernare electronică (CGE) de prestare a serviciilor este responsabil de monitorizarea procesului de reglare a tuturor incidentelor înregistrate. Incidentele pe care CGE de prestare a serviciilor nu le poate soluţiona imediat trebuie să fie transmise pentru a fi prelucrate de către grupuri specializate care dispun de abilităţi mai specializate, de timp suplimentar şi de alte resurse pentru soluţionarea incidentelor. Soluţionarea sau soluţia de ocolire trebuie să fie prezentată în termene cît mai restrînse pentru restabilirea deservirii utilizatorilor cu impact minim asupra activităţii lor. După înlăturarea cauzei incidentului şi restabilirea serviciului aprobat, incidentul urmează să fie închis şi este necesar de a întocmi documentaţia corespunzătoare.

Statutul incidentului trebuie să reflecte starea sa actuală în cadrul ciclului de viaţă. Este necesar ca înregistrarea despre incident să fie menţinută în stare actuală în decursul ciclului de viaţă al incidentului, ceea ce permite obţinerea unor date actualizate privind procesul de prelucrare a solicitării.

Este necesar de a înregistra următoarele actualizări ale înregistrării despre incident:

- colaboratorul care a efectuat modificarea înregistrării;
- descrierea detaliată a modificării;
- data şi ora modificării;
- cauza efectuării modificării;
- timpul utilizat.

Prioritatea incidentului este determinată de influenţa acestuia asupra proceselor din cadrul organizaţiei şi urgenţa cu care trebuie asigurată soluţionarea sau soluţia de ocolire. Indicatorii speciali pentru soluţionarea incidentelor sau prelucrarea solicitărilor urmează să fie incluşi în Acordul cu privire la nivelul de deservire.

Toate incidentele urmează să fie înregistrate în CGE de prestare a serviciilor în mod automat sau de către colaboratori.

După primirea notificării despre incident, CGE de prestare a serviciilor urmează să înregistreze datele de bază, inclusiv timpul şi detaliile obţinute privind simptomele, după care, în cazul existenţei unei solicitări de deservire, solicitarea este prelucrată. Pentru o înregistrare suplimentară despre incident conform Bazei configurationale de date a elementelor de evidenţă are loc selectarea elementelor de evidenţă care constituie cauza incidentului. Următoarele acţiuni efectuate de către

CGE de prestare a serviciilor sînt stabilirea priorității respective, evaluarea incidentului, oferirea unor recomandări privind soluționarea acestuia. După soluționarea reuşită a incidentului se efectuează închiderea înregistrării despre acesta şi înregistrarea acțiunilor legate de soluționarea acestuia. După o tentativă nereuşită de soluționare a incidentului sau în caz de depistare a necesității de a aplica un nivel mai înalt de mentenanță, are loc transmiterea incidentului către un grup specializat.

În procesul de soluționare se verifică conform bazei de date legăturile incidentului cu problemele, erorile şi incidentele cunoscute. În cazul existenței unei soluții de ocolire sau soluționare, incidentul trebuie să fie soluționat imediat, în caz contrar, procesul de gestionare a incidentelor este responsabil pentru soluționare sau căutarea unei soluții de ocolire cu o întrerupere minimă a proceselor organizației. Soluția de ocolire urmează să fie analizată de echipa de gestionare a problemelor, care actualizează înregistrarea respectivă despre problemă.

5.1.2. Acțiunile realizate în procesul de gestionare a incidentelor

Pentru a asigura productivitatea funcționării procesului de gestionare a incidentelor sînt necesare următoarele:

- o Bază de date configurațională a elementelor de evidență actualizată la timp;
- elaborarea unei baze de date ale problemelor şi erorilor, actualizate la timp, pentru păstrarea soluționărilor şi soluțiilor de ocolire existente;
- trebuie asigurată o legătură strînsă cu procesul de gestionare a nivelurilor de deservire pentru determinarea indicatorilor necesari privind timpul de reacționare la incident.

Procesul de gestionare a incidentelor recepționează informația necesară de prelucrat din următoarele surse:

- datele despre incident prezentate de către CGE de prestare a serviciilor, subdiviziunea de deservire a rețelelor sau serviciul de exploatare;
- datele despre configurația din Baza de date configurațională a elementelor de evidență;
- rezultatele relaționării incidentelor cu problemele şi erorile cunoscute; date referitoare la soluționarea acestora;
- răspunsul la solicitarea de modificare, care conduce la soluționarea incidentelor.

Pe parcursul realizării acțiunilor şi cerințelor procesului de gestionare a incidentelor este necesar de obținut următoarea informație:

- solicitarea de modificare pentru reglarea incidentului;
- înregistrarea actualizată a incidentului,
- incidentele soluționate şi închise;
- comunicațiile cu clienții;
- informația administrativă, raportarea.

Procesul de gestionare a incidentelor trebuie să fie compus din următoarele acțiuni:

- depistarea şi înregistrarea incidentelor;
- clasificarea şi mentenanța inițială;
- investigarea şi diagnosticarea;
- soluționarea şi restabilirea;
- închiderea incidentului;
- controlul, monitorizarea, urmărirea şi comunicațiile.

În vederea asigurării controlul asupra întregului ciclu de viață al incidentului, pentru fiecare acțiune urmează să fie înregistrate: numele/identificatorul grupului de specialişti care înregistrează acțiunile, tipul acțiunii (marşrutizarea, diagnosticarea, restabilirea, soluționarea, închiderea etc.), data/ora acțiunii, descrierea şi rezultatul acțiunii.

5.1.2.1. Depistarea şi înregistrarea incidentului

În procesul de depistare şi înregistrare a incidentului trebuie să parvină datele despre incident, în baza cărora are loc înregistrarea datelor principale despre acesta, după care urmează, notificarea grupului specializat de mentenanță în caz de necesitate şi începerea procedurilor de prelucrare a solicitării de deservire. Toate incidentele urmează să fie înregistrate, pentru ca acestea să fie introduse apoi în baza de date destinată gestionării incidentelor. Simptomele, datele esențiale necesare pentru diagnosticare şi informația despre elementele de evidență referitoare la incident trebuie să fie incluse în înregistrarea despre incident în timpul depistării şi înregistrării acestuia.

În înregistrările despre incident trebuie să fie incluse următoarele date:

- numărul unic de înregistrare;
- clasa incidentului;
- data / timpul creării sau modificării înregistrării;
- numele / identificatorul specialistului sau grupului de specialişti care creează sau modifică înregistrarea de evidență;
- numele / subdiviziunea / numărul de telefon / locația utilizatorului solicitant;
- mijlocul de feedback;
- descrierea simptomelor;
- categoria sau subcategoria;
- impactul / urgența / prioritatea;
- statutul incidentului (activ, în aşteptare, închis, soluționat, în funcțiune, nou, transmis specialistului);
- elementele de evidență implicate în incident;
- grupul de susținere / specialistul, căruia i-a fost transmis incidentul;
- problema / eroarea cunoscută care are legătură cu incidentul;
- data şi timpul soluționării;
- categoria închiderii;
- data şi timpul închiderii.

Aceste date sînt necesare pentru soluționarea incidentului, pentru restabilirea ulterioară şi pentru informația administrativă privind tipurile incidentelor şi statistica de survenire a acestora. Incidentul trebuie prelucrat în conformitate cu procedurile standard de gestionare a nivelului de deservire.

5.1.2.2. Clasificarea şi mentenanța inițială a incidentelor

În procesul de clasificare şi de mentenanță inițială urmează să parvină datele referitoare la configurație din Baza de date configurațională a elementelor de evidență, precum şi rezultatul relaționării incidentului cu problemele şi erorile cunoscute.

Pentru identificarea cauzei incidentului, este necesar de analizat înregistrările din baza de date a gestionării incidentelor şi de întreprins următoarele acțiuni:

- clasificarea incidentelor (a se vedea 5.1.3);
- relaționarea cu problemele şi erorile cunoscute;
- informarea procesului de gestionare a problemelor privind depistarea problemelor noi şi privind incidentele pentru care nu au fost identificate analogii;
- atribuirea nivelului de impact şi de urgență;
- determinarea priorității;
- evaluarea datelor referitoare la configurațiile interconexe;
- oferirea mentenanței inițiale;
- închiderea incidentului sau marşrutizarea acestuia către grupul specializat de mentenanță, informarea utilizatorului.

Incidentul urmează să fie clasificat. În procesul de clasificare, trebuie determinate cauzele incidentului precum şi acțiunile corespunzătoare de soluționare a acestuia. Clasificarea este utilizată

pentru determinarea serviciului prestat de care este legat incidentul, pentru determinarea relației acestuia cu Acordul cu privire la nivelul de deservire, pentru selectarea specialiştilor pentru prelucrarea incidentului, pentru determinarea priorității şi a impactului incidentului asupra proceselor organizației, pentru determinarea existenței legăturilor cu erorile şi soluțiile cunoscute. În procesul de clasificare a incidentelor, este necesar de furnizat o cantitate maximă de informație.

Un aspect important în gestionarea incidentului constă în determinarea priorității acestuia. Responsabilitatea pentru determinarea priorității îi revine procesului de gestionare a nivelului de deservire. Prioritatea incidentului este determinată în funcție de următorii factori: impactul asupra proceselor de prestare a serviciilor publice, urgența, proporțiile, limitele, complexitatea, accesibilitatea resurselor necesare pentru înlăturarea defecțiunii.

În procesul de determinare a gradului de influență, este necesar de a dispune de accesul la Baza de date configurațională a elementelor de evidență pentru stabilirea numărului de utilizatori supuşi influenței incidentului.

Urgența incidentului reprezintă viteza cu care acesta urmează să fie soluționat.

5.1.2.3. Investigarea şi diagnosticarea incidentelor

În decursul procesului de investigare şi diagnosticare a incidentului trebuie să parvină date actualizate despre incident, despre configurația din Baza de date configurațională a elementelor de evidență, precum şi să fie întreprinse acțiuni pentru analiza şi colectarea datelor despre incident, căutarea unei soluții de ocolire sau transmiterea incidentului respectiv către grupul de mentenanță.

După transmiterea incidentului către grupul de mentenanță, acesta urmează să întreprindă următoarele acțiuni:

- să prelucreze incidentul;
- să indice data şi timpul pentru actualizarea regulată a statutului incidentului;
- să prezinte recomandări CGE de prestare a serviciilor privind soluțiile de ocolire identificate;
- să compare incidentul cu erorile, problemele, soluțiile cunoscute;
- să determine modul de soluționare a incidentului, să actualizeze datele necesare;
- să transmită incidentul CGE de prestare a serviciilor pentru a fi închis.

Procesul de investigare şi diagnosticare poate fi repetat ciclic, pe măsura înlăturării cauzelor apariției incidentelor.

5.1.2.4. Soluționarea incidentului şi restabilirea serviciului

Rezultatele procesului de soluționare a incidentului şi de restabilire a serviciului trebuie să fie date actualizate despre incident, răspunsurile la solicitarea de modificare care conduc la soluționarea incidentelor, soluții de ocolire şi mijloace de soluționare a incidentelor.

În procesul de soluționare şi restabilire este necesar de întreprins acțiuni de soluționare a incidentului cu ajutorul mijlocului de soluționare, soluției de ocolire sau solicitării de modificare, precum şi acțiuni de restabilire. După soluționare reuşită a incidentului personalul specializat purcede la restabilirea serviciului.

5.1.2.5. Închiderea incidentului

Rezultatele procesului de închidere a incidentului trebuie să includă date actualizate despre incident şi incidentul soluționat.

În decursul procesului de închidere a incidentului, soluționarea incidentului trebuie să fie confirmată de către solicitant. După închiderea incidentului, CGE de prestare a serviciilor trebuie să se asigure că:

- informația despre acțiunile de soluționare a incidentului este laconică şi accesibilă;
- există o clasificare exactă a cauzei apariției incidentului;
- acțiunile întreprinse în vederea soluționării incidentului au fost coordonate cu clientul.

5.1.2.6. Controlul, monitorizarea, urmărirea şi comunicațiile

Controlul, monitorizarea, urmărirea şi comunicațiile trebuie să includă înregistrările referitoare la incidente. În decursul procesului de control, monitorizare, urmărire şi comunicare trebuie realizată monitorizarea escaladării incidentelor, informarea utilizatorilor.

CGE de prestare a serviciilor este responsabil pentru controlul şi monitorizarea asupra soluționării tuturor incidentelor deschise. Pentru aceasta trebuie să întreprindă următoarele acțiuni în mod regulat:

- să urmărească statutul şi procesul de soluționare a tuturor incidentelor deschise;
- să verifice corespunderea cu nivelurile de deservire;
- să specifice incidentele transmise între grupurile specializate;
- să acorde prioritate monitorizării incidentelor cu un grad înalt de influență;
- să informeze utilizatorii afectați de incident.

Rezultatele îndeplinirii acestor acțiuni sînt rapoartele de gestionare privind procesul de soluționare a incidentului, rapoartele şi comunicațiile cu clientul.

5.1.3. Clasificarea incidentelor

Clasificarea incidentelor trebuie realizată corect pentru următoarele scopuri:

- determinarea utilajului sau a serviciului cu care este legat incidentul;
- selectarea specialiştilor care vor asigura înlăturarea optimă a incidentului;
- determinarea priorității şi a impactului asupra funcționării procesului de prestare a serviciilor publice;
- determinarea criteriilor de relaționare la selectarea unei anumite decizii;
- determinarea matricei de raportare pentru informația administrativă.

Nivelurile de clasificare depind de nivelul necesar de detaliere. Clasificarea detaliată asigură utilizarea mai eficientă a informației administrative, care urmează să fie analizată periodic în vederea aplicării doar a celor mai recente date.

5.1.4. Indicatorii eficienței procesului de gestionare a incidentelor

În scopul perfecționării monitorizării şi informației administrative privind calitatea serviciilor, asigurării reducerii impactului asupra proceselor de prestare a serviciilor publice, utilizării eficiente a personalului, excluderii incidentelor şi cererilor de deservire ratate sau introduse incorect, este necesar de a măsura următorii indicatori:

- numărul total de incidente;
- timpul mediu efectiv utilizat pentru soluționarea incidentului sau identificarea unei soluții de ocolire;
- procentul incidentelor prelucrate în limitele timpului aprobat de reacționare;
- suma medie de cheltuieli legate de incident;
- procentul incidentelor închise de CGE de prestare a serviciilor fără apelare la grupurile specializate;
- incidentele prelucrate la fiecare stație de lucru a CGE de prestare a serviciilor;
- numărul şi procentul incidentelor soluționate la distanță.

5.2. Procesul de gestionare a problemelor

Obiectivul procesului de gestionare a problemelor constă în minimalizarea numărului şi gradului de impact negativ al incidentelor şi problemelor, cauzate de erorile din cadrul infrastructurii TI, exercitat asupra proceselor de prestare a serviciilor publice. Pentru realizarea acestui obiectiv este necesar de identificat cauzele incidentelor şi de efectuat acțiuni pentru îmbunătățirea sau corectarea situației.

Procesul de gestionare a problemelor trebuie să cuprindă acțiunile legate de reacționarea la incidente şi acțiunile preventive. Acțiunile de gestionare a problemelor trebuie să includă actualizarea soluțiilor de ocolire recomandate şi a înregistrării despre problemă în vederea susținerii

controlului incidentelor.

Rezultatul procesului de gestionare a problemelor trebuie să fie prezentarea informației privind problemele depistate, erorile cunoscute şi cererile de modificare perfectate.

5.2.1. Cerințele de bază față de procesul de gestionare a problemelor

Față de procesul de gestionare a problemelor sînt înaintate următoarele cerințe:

- informația păstrată trebuie să fie organizată şi uşor accesibilă;
- actualizarea documentației (tehnologiile, soluțiile externe accesibile, experiența practică, frecvența şi impactul incidentelor repetate) trebuie să fie efectuată în mod regulat;
- analiza detaliată a procesului de gestionare a problemelor şi perfectarea documentației corespunzătoare;
- existența personalului calificat;
- existența depozitului de informații bazat pe mijloace integrate de gestionare a serviciilor;
- utilizarea sistemelor profesionale.

Problemele şi erorile cunoscute sînt relevate cu ajutorul analizei incidentelor pe măsura survenirii acestora şi la intervale diferite de timp, cu ajutorul analizei infrastructurii TI, pregătirii bazei de cunoştințe, activității elaboratorilor şi furnizorilor la darea în exploatare a produselor noi.

5.2.2. Acțiunile procesului de gestionare a problemelor

În cadrul procesului de gestionare a problemelor este necesar de a efectua controlul problemelor şi erorilor care anticipează gestionarea problemelor. Toate problemele trebuie să fie cunoscute şi înregistrate în cadrul procesului de gestionare a problemelor.

Pentru realizarea procesului de gestionare a problemelor sînt necesare datele despre incidente, datele despre configurația din Baza de date configurațională a elementelor de evidență, soluțiile de ocolire.

La realizarea procesului de gestionare a problemelor trebuie de recepționat şi de documentat următoarea informație: erorile cunoscute, solicitările de modificare, înregistrările actualizate privind problemele, problemele soluționate, înregistrările închise despre probleme, informația administrativă.

Procesul de gestionare a problemelor constă din următoarele acțiuni:

- controlul problemelor;
- controlul erorilor;
- prevenirea preventivă a problemelor;
- determinarea tendințelor;
- obținerea informației administrative;
- analiza problemelor majore (se efectuează după soluționarea fiecărei probleme majore).

5.2.2.1. Controlul problemelor

Controlul problemelor constă în prelucrarea eficientă şi rezultativă a problemelor. Obiectivul principal este identificarea cauzei de bază care a provocat defecțiunea şi asigurarea CGE de prestare a serviciilor cu informație şi recomandări privind soluțiile de ocolire. Controlul problemelor depinde de calitatea controlului incidentelor şi furnizează recomandări privind soluțiile optime de ocolire.

În procesul de efectuare a controlului problemelor este necesar de întreprins următoarele acțiuni:

- identificarea şi înregistrarea problemei;
- clasificarea problemei;
- analiza şi diagnosticarea problemei;
- solicitarea de modificare;
- soluționarea şi închiderea problemei.

5.2.2.1.1. Identificarea şi înregistrarea problemei

Identificarea problemei trebuie să fie efectuată în cazul în care se respectă una sau mai multe din

condițiile enumerate mai jos:

- în cadrul mentenanței inițiale şi clasificării incidentului a eşuat relaționarea acestuia cu problemele existente şi erorile cunoscute;
- incidentul se repetă;
- incidentul nu este legat de problemele existente şi erorile cunoscute;
- analiza infrastructurii TI a depistat problema care potențial poate aduce la incidente;
- survenirea unui incident major semnificativ pentru care este necesar de a găsi o soluție structurală.

Înregistrările privind problemele trebuie să fie păstrate în Baza de date configurațională a elementelor de evidență. Înregistrările despre probleme sînt relaționate cu toate înregistrările aferente despre incidente.

5.2.2.1.2. Clasificarea problemelor

În procesul de clasificare este necesar de determinat volumul eforturilor necesare pentru identificarea şi restabilirea elementelor de evidență defectate, categoria, impactul, urgența şi prioritatea problemei. Categoriile de probleme sînt distribuite pe grupuri sau domenii de cunoştințe corespunzătoare (hardware, software, mijloace de comunicații, software de mentenanță etc.).

Influența problemei determină distribuirea eforturilor pentru mentenanța serviciilor publice. La stabilirea priorității problemei este necesar de luat în considerație urgența, impactul, riscurile şi accesibilitatea resurselor.

La rîndul său, urgența determină gradul de reținere ce poate fi admis la soluționarea problemei sau erorii. Urgența problemei este influențată de următoarele aspecte:

- accesibilitatea eliminării temporare a erorii;
- existența soluției de ocolire;
- posibilitatea reținerii planificate a soluționării problemei;
- impactul problemei, care indică gradul de vulnerabilitate a proceselor legate de prestarea serviciilor publice.

5.2.2.1.3. Analiza şi diagnosticarea problemelor

Analiza şi diagnosticarea problemei trebuie să determine cauza defecțiunii în elementul de evidență înregistrat, după care este necesar de inițiat activitatea sistemului de control al erorilor.

Pentru diagnosticarea problemei este necesar de a asigura proceduri eficiente de colectare a datelor analitice legate de soluționarea problemelor, precum şi necesită datele exacte de evidență despre ultimele modificări deoarece acestea pot indica cauzele problemelor.

În cadrul analizei structurale şi diagnosticări problemelor trebuie aplicate următoarele metode:

- Kepner şi Trego – conform acestei metode, analiza problemelor trebuie să reprezinte un proces sistematic, îndreptat spre soluționarea acestora. Metoda evidențiază fazele de analiză a problemelor:

1) identificarea problemei;
2) descrierea problemei, inclusiv esența, particularitățile, locația, timpul şi dimensiunile;
3) determinarea cauzelor posibile;
4) testarea celei mai probabile cauze;
5) verificarea cauzei reale;

- diagramele lui Ishikava – diagrame cauză-efect care indică factorii ce influențează problema;
- metoda “brainstorming”;
- metodele schemelor-bloc.

În procesul de analiză şi diagnosticare a problemelor este necesar de a dispune de accesul la documentația privind toate produsele din infrastructura TI, în calitate de informație de referință, atît pentru proces, cît şi pentru personalul serviciului de mentenanță. Această informație trebuie să includă documentația privind sistemele aplicative, software-ul de sistem, programele interne de

service, hardware-ul şi software-ul de rețea, diagramele generale ale configurațiilor rețelelor.

5.2.2.2. Controlul erorilor

Controlul erorilor trebuie să includă procesele implicate în desfăşurarea lucrărilor legate de erorile cunoscute pînă în momentul înlăturării acestora. Obiectivul principal al acestui proces constă în notificarea despre erori, monitorizarea şi înlăturarea acestora.

Controlul erorilor are menirea să unească mediul de elaborare cu mediul de exploatare. Erorile din software la etapa de elaborare pot influența activitatea în mediul de exploatare. Informația despre erorile cunoscute depistate în mediul de elaborare sau în mediul de mentenanță trebuie să fie transmisă în mediul de exploatare.

În cadrul controlului erorilor trebuie întreprinse următoarele acțiuni:

- identificarea şi înregistrarea erorilor;
- evaluarea erorilor;
- înregistrarea privind procesul de soluționare a erorilor;
- închiderea erorilor;
- monitorizarea problemelor şi a progresului în soluționarea erorilor.

Controlul erorilor este legat în mod direct şi acționează concomitent cu procesele de gestionare a modificărilor. Procesul de control al erorilor trebuie să fie format din etapele de depistare şi înregistrare a erorii, de evaluare a erorii, de înregistrare a deciziei privind eroarea, de închidere a erorii şi a problemei aferente.

Eroarea trebuie să fie determinată atunci cînd este identificat elementul de evidență, este stabilită cauza de bază a problemei şi este găsită o soluție de ocolire. Sursele datelor privind erorile cunoscute trebuie să fie subsistemele de control al problemelor în mediul de elaborare şi în mediul de exploatare. Înregistrarea despre eroarea cunoscută trebuie să conțină identificatorul solicitării de modificare.

Erorile trebuie să fie identificate şi înregistrate în procesul investigării şi diagnosticării – acțiunilor privind controlul problemelor.

Procedura soluționării fiecărei erori cunoscute trebuie să fie înregistrată în sistemul de gestionare a problemelor. Este necesar ca toate datele privind elementele de evidență, simptomele, acțiunile pentru soluționarea sau soluție ocolită, legate de toate erorile cunoscute, să se afle în baza de date a erorilor cunoscute. Aceste date trebuie să fie accesibile pentru relaționarea incidentelor, identificarea unor soluții de ocolire şi furnizarea informației administrative.

După implementarea modificărilor pentru înlăturarea erorii, înregistrările corespunzătoare despre eroarea cunoscută trebuie să fie închise împreună cu toate înregistrările conexe despre incidente şi probleme. Controlul erorilor este responsabil de monitorizarea desfăşurării lucrărilor legate de soluționarea erorilor cunoscute.

Pregătirea solicitării de modificare face parte din obligațiile procesului de control al erorilor.

5.2.2.3. Prevenirea premeditată a problemelor

Prevenirea premeditată a problemelor trebuie să includă acțiunile orientate spre depistarea şi soluționarea problemelor pînă la survenirea acestora, reducînd la minimum impactul negativ asupra prestării serviciilor publice.

În acest scop este necesar de întreprins următoarele acțiuni:

- analiza tendințelor;
- acțiuni de mentenanță;
- asigurarea organizației cu informație.

Prevenirea premeditată a problemelor trebuie să asigure îmbunătățirea calității prestării serviciilor publice şi o utilizare mai eficientă a resurselor informaționale accesibile.

Sarcina de bază a gestionării preventive a problemelor constă în direcționarea eficientă a

resurselor limitate de mentenanță a serviciilor, determinarea zonelor problematice care exercită cel mai negativ impact asupra procesului de prestare a serviciilor.

Activitatea preventivă principală din cadrul procesului de gestionare a problemelor constă în analiza tendințelor şi a direcțiilor acțiunilor de prevenire a apariției problemelor. Rapoartele privind analiza incidentelor şi a problemelor trebuie să ofere informații despre măsurile preventive care pot spori calitatea serviciilor publice prestate. Analiza incidentelor şi a problemelor trebuie să determine tendințele, defecțiunile de un anumit tip care se află la etape incipiente, incidentele ce se repetă şi problemele legate de survenirea lor.

5.2.2.4. Determinarea tendințelor

Determinarea tendințelor conduce la determinarea zonelor potențial problematice care necesită a fi investigate. Determinarea şi analiza tendințelor trebuie să ducă la identificarea defecțiunilor în infrastructura TI, determinarea zonelor problematice generale care necesită o atenție sporită din partea serviciului de mentenanță.

5.2.2.5. Obținerea informației administrative

Obținerea informației administrative trebuie să asigure înțelegerea esenței eforturilor şi resurselor aplicate de către organizație pentru investigarea, diagnosticarea şi soluționarea problemelor şi a erorilor cunoscute.

Informația administrativă trebuie să includă:

- numărul solicitărilor de modificare perfectate;
- influența solicitărilor de modificare asupra accesibilității şi fiabilității serviciilor publice prestate;
- timpul utilizat pentru investigarea şi diagnosticarea problemei pentru fiecare unitate organizațională;
- numărul şi influența incidentelor ce survin pînă la închiderea problemei de bază;
- proporția eforturilor depuse pentru reacționare în vederea susținerii, în raport cu eforturile planificate în procesul de gestionare a problemelor;
- planurile de soluționare a problemelor deschise în raport cu resursele şi bugetul;
- descrierea acțiunilor întreprinse.

5.2.2.6. Analiza problemelor majore

În procesul de soluționare a fiecărei probleme majore este necesar de efectuat analiza acesteia. Analiza este necesară pentru determinarea acțiunilor corecte şi incorecte în vederea eliminării problemei, a măsurilor de prevenire a survenirii repetate a problemei respective.

Procesul de gestionare a problemelor trebuie să efectueze monitorizarea influenței pe termen lung a problemelor şi erorilor cunoscute asupra serviciilor publice prestate.

5.2.3. Indicatorii eficienței procesului de gestionare a problemelor

Informația istorică privind controlul incidentelor şi problemelor oferă posibilitatea de a obține metricele care indică calitatea deservirii şi productivitatea procesului de prestare a serviciilor publice. Frecvența şi durata problemelor reprezintă metrica eficienței în raport cu nivelurile aprobate de deservire.

Pentru îmbunătățirea calității serviciilor publice prestate, reducerea numărului incidentelor, îmbunătățirea procesului de instruire a personalului, sporirea procentului de cereri, soluționate în timpul primei solicitări, CGE de prestare a serviciilor urmează să ia în considerație următorii indicatori:

- numărul total de probleme;
- numărul total de erori;
- timpul mediu efectiv consumat pentru soluționarea problemelor sau căutarea soluției de ocolire;
- cheltuielile medii pentru soluționarea problemei sau erorii;

- numărul şi procentajul problemelor soluționate la distanță;
- numărul problemelor prevenite în cadrul infrastructurii TI, inclusiv şi de procesul de gestionare a accesibilității.

Interacțiunea dintre procesul de gestionare a problemelor şi procesul de gestionare a accesibilității conduce la sporirea calității deservirii.

Procesul de gestionare a problemelor trebuie să analizeze în mod regulat realizările obținute conform tuturor indicatorilor speciali.

5.3. Procesul de gestionare a modificărilor

Obiectivul procesului de gestionare a modificărilor constă în asigurarea aplicării metodelor şi procedurilor standard pentru prelucrarea productivă şi la timp a modificărilor, pentru minimalizarea impactului incidentelor legate de modificări asupra calității serviciilor publice prestate.

Informația despre procesele de gestionare a modificărilor trebuie să fie deschisă pentru trecerea la o stare nouă în timpul efectuării modificărilor.

Pentru realizarea procesului în cauză este necesară existența solicitărilor de modificare, a Bazei de date configurationale a elementelor de evidență şi a graficului coordonat al modificărilor.

În procesul de gestionare a modificărilor este necesar de elaborat graficul coordonat al modificărilor, solicitările de modificare şi rapoartele de gestionare a modificărilor.

5.3.1. Cerințele de bază față de procesul de gestionare a modificărilor

Procesul de gestionare a modificărilor trebuie să gestioneze zilnic modificările ce au loc.

Față de procesul de gestionare a modificărilor sînt înaintate următoarele cerințe:
- filtrarea modificărilor;
- elaborarea planului modificărilor;
- analiza şi închiderea solicitărilor de modificare;
- raportarea administrativă.

5.3.1.1. Filtrarea modificărilor

Filtrarea modificărilor trebuie îndeplinită în raport cu următoarele obiecte informaționale:
- hardware;
- dispozitivele şi software-ul de comunicații;
- software-ul de sistem;
- software-ul aplicativ aflat în exploatare;
- documentația şi procedurile de mentenanță şi susținere a sistemelor aflate în exploatare.

În cadrul procesului de gestionare a modificărilor este necesar de a oferi confirmarea pentru oricare din modificările propuse. Gestionarea modificărilor nu este responsabilă de identificarea componentelor afectate de modificare, actualizarea înregistrărilor despre modificări, release-urile componentelor noi sau modificate. Toate acțiunile în procesul de modificare trebuie să fie înregistrate pe măsura efectuării lor în registrul de gestionare a modificărilor.

Pe măsura înregistrării modificărilor în cadrul procesului de gestionare a modificărilor este necesar de efectuat examinarea succintă a fiecărei solicitări, iar solicitările nepractice urmează să fie filtrate.

Pînă la aprobarea fiecărei modificări este necesară examinarea riscurilor pentru procesele de prestare a serviciilor publice, precum şi examinarea evaluării impactului şi a resurselor. Aprobarea modificării trebuie să includă aprobarea financiară, tehnică şi organizațională. Aprobarea financiară determină limitele bugetului modificării. Aprobarea tehnică determină fezabilitatea, rationalitatea şi posibilitatea de realizare a modificării fără a prejudicia procesul de prestare a serviciilor. Aprobarea organizațională determină cerințele condiționate de prestarea serviciilor publice şi aşteptările participanților la interacțiune şi a utilizatorilor de servicii publice.

5.3.1.2. Elaborarea planului modificărilor

Pentru îmbunătățirea procesului de gestionare a modificărilor este necesară coordonarea elaborării şi distribuirii planului şi graficului coordonat al modificărilor, precum şi a accesibilității planificate a serviciilor. Această documentație urmează să fie general accesibilă.

Planul şi graficul coordonat al modificărilor trebuie să conțină informații despre toate modificările aprobate pentru implementare şi datele preconizate pentru implementarea acestora. Accesibilitatea preconizată a serviciului trebuie să conțină date despre modificările în cadrul Acordului cu privire la nivelul de deservire şi despre accesibilitatea serviciilor, ținîndu-se cont de modificările planificate.

5.3.1.3. Analiza solicitărilor de modificare

În procesul de gestionare a modificărilor trebuie de efectuat analiza tuturor modificărilor introduse. Scopul analizei este de a constata dacă:

- modificarea a dus la efectul scontat şi a atins scopurile fixate;
- utilizatorii sînt satisfăcuți de rezultate;
- toate carențele au fost determinate;
- nu au survenit efecte secundare în funcționalitatea, accesibilitatea, productivitatea, securitatea, posibilitatea de deservire;
- volumul resurselor utilizate pentru introducerea modificării a corespuns volumului planificat;
- modificarea a fost introdusă la timp;
- planul de recul a funcționat corect.

În cazul în care modificarea nu şi-a atins scopurile, este necesar de a lua decizia cu privire la acțiunile ulterioare. Procesul de gestionare a modificărilor inițiază acțiunile ulterioare pentru înlăturarea tuturor problemelor sau neajunsurilor care au apărut în sistemul de gestionare a modificărilor în rezultatul unor modificări ineficiente.

5.3.1.4. Raportarea administrativă

La crearea rapoartelor administrative este necesar de a examina următoarea informație şi statistică:

- numărul de modificări implementate în perioada de timp respectivă;
- distribuirea modificărilor conform cauzelor efectuării lor;
- numărul de modificări efectuate cu succes;
- numărul de returnări la starea anterioară în procesul efectuării modificărilor;
- numărul şi cauzele incidentelor care au dus la modificări;
- numărul solicitărilor de modificare;
- numărul de modificări implementate analizate şi numărul de modificări ce urmează să fie analizate;
- numărul de solicitări de modificare respinse;
- solicitările ce urmează să fie implementate.

Această informație este utilizată ca bază pentru evaluarea productivității şi eficienței procesului de gestionare a modificărilor.

Auditul procesului de gestionare a modificărilor trebuie efectuat cel puțin o dată pe an.

Auditul trebuie să includă verificarea următoarelor elemente:

- solicitările de modificare selectate la întîmplare;
- înregistrările despre modificări;
- analiza solicitărilor de modificare.

5.3.2. Acțiunile procesului de gestionare a modificărilor

Procesul de gestionare a modificărilor joacă un rol de supraveghere în testarea tuturor modificărilor.

Solicitările de modificare pot fi legate de orice parte a infrastructurii TI, orice serviciu şi activitate. Este necesar de a determina procedurile de documentare a solicitărilor de modificare.

Toate solicitările de modificare acceptate sînt înregistrate şi primesc un număr de identificare.

În procesul de realizare a gestionării modificărilor trebuie de îndeplinit următoarele acțiuni:

- determinarea cauzelor solicitărilor de modificare;
- stabilirea formularului solicitării de modificare;
- stabilirea priorităților solicitărilor de modificare;
- elaborarea, testarea şi implementarea modificărilor;
- aplicarea software-ului pentru gestionarea modificărilor.

5.3.2.1. Depistarea cauzelor solicitărilor de modificare

Pentru elaborarea solicitărilor de modificare trebuie depistate următoarele cauze:

- decizia indicată în raportul privind incidentul sau problema;
- insatisfacția utilizatorului de nivelul deservirii;
- propunerea de introducere sau eliminare a elementului de evidență;
- propunerea de modernizare a componentelor infrastructurii TI;
- modificarea cerințelor sau a conținutului proceselor ce asigură prestarea serviciilor publice;
- prevederile noi sau modificările în legislație;
- schimbarea locației;
- modificări în serviciile prestate.

5.3.2.2. Stabilirea formularului solicitării de modificare

Formularul solicitării de modificare trebuie să conțină următoarele elemente:

- numărul de ordine al solicitării de modificare cu referință încrucişată la numărul raportului privind problema;
- descrierea şi identificarea elementului care trebuie să fie modificat;
- cauza introducerii modificării;
- consecințele în cazul neimplementării modificării;
- versiunea elementului modificat;
- rechizitele persoanei care propune modificarea;
- data propunerii modificării;
- prioritatea modificării;
- evaluarea influenței şi resursele;
- recomandările comitetului consultativ pentru modificări;
- introducerea planificată;
- date privind grupul elaboratorilor modificării;
- evaluarea şi gestionarea riscurilor;
- statutul solicitării de modificare.

Raportul privind rezultatele finalizării modificării trebuie transmis persoanelor responsabile de gestionarea modificărilor, după care modificarea este aprobată. Pe măsura avansării modificării în ciclul de viață, este necesar de actualizat solicitarea de modificare şi Baza configurațională de date a elementelor de evidență.

5.3.2.3. Stabilirea priorităților solicitărilor de modificare

Fiecărei solicitări de modificare trebuie să i se atribuie o prioritate, reieşind din influența problemei şi urgența necesității restabilirii. La atribuirea priorității, o importanță deosebită o are evaluarea riscului implementării sau devierii de la modificare. Pentru fiecare prioritate este necesar de determinat anumite limite de timp. Prioritățile se împart în:

- urgente – reținerea de scurtă durată a examinării modificării duce la întreruperea prestării serviciilor sau la probleme grave; înalte – modificarea are o influență considerabilă asupra activității a cîțiva utilizatori;
- medii – influența modificării este nesemnificativă, dar măsurile de înlăturare nu pot fi amînate

pînă la următorul release conform graficului;

- reduse – modificarea este justificată şi necesară, dar poate aştepta pînă la următorul release conform graficului.

Prioritatea trebuie să indice ordinea în care urmează să fie înlăturate problemele.

5.3.2.4. Elaborarea, testarea şi introducerea modificărilor

Solicitările de modificare aprobate trebuie transmise grupurilor tehnice corespunzătoare pentru elaborare şi pregătirea pentru implementarea modificării. Pregătirea pentru implementarea modificării trebuie să includă:

- asamblarea noului modul;
- crearea versiunii noi a unui sau mai multor module de program;
- procurarea externă sau primirea echipamentului;
- pregătirea modificării hardware-ului;
- pregătirea documentației noi sau actualizate;
- pregătirea utilizatorilor.

Pentru fiecare modificare autorizată este necesară pregătirea şi documentarea procedurilor de recul, pentru activizarea lor în cazul survenirii erorilor cu impact negativ asupra calității serviciilor prestate.

Pentru prevenirea impactului negativ al modificărilor asupra calității serviciilor publice prestate, este necesar de a testa modificarea în prealabil.

Testarea modificării trebuie să ia în considerație următoarele aspecte:

- productivitatea;
- securitatea;
- posibilitatea deservirii;
- capacitatea de susținere;
- fiabilitatea şi accesibilitatea;
- funcționalitatea.

Gestionarea modificărilor trebuie să evalueze riscurile pentru procesele de prestare a serviciilor publice la fiecare modificare implementată fără o testare deplină. Testarea trebuie să includă un nivel suficient de testare regresivă pentru a se demonstra exhaustiv absența impactului negativ a modificării asupra altor componente ale infrastructurii.

Graficul implementării modificărilor trebuie să fie elaborat astfel încît să aibă o influență minimă asupra serviciilor aflate în exploatare.

Toate modificările trebuie să fie prevăzute şi planificate şi este necesar de a lua în considerație accesibilitatea resurselor pentru elaborarea şi testarea acestor modificări.

Pentru modificările urgente este necesară elaborarea procedurilor pentru prelucrarea rapidă a acestora fără pierderea nivelului normal al controlului administrativ.

5.3.2.5. Utilizarea software-ului pentru gestionarea modificărilor

Software-ul procesului de gestionare a modificărilor trebuie să dețină următoarele caracteristici:

- solicitările de modificare şi înregistrările despre probleme sînt păstrate într-o bază de date în format uşor accesibil;
- posibilitatea găsirii legăturii între solicitările de modificare, înregistrările problemelor şi elementele de evidență;
- posibilitatea relaționării solicitărilor de modificare cu proiectele;
- crearea automată a solicitărilor de evaluare a influenței elementelor de evidență implicate;
- susținerea înregistrării acțiunilor conform etapelor autorizării şi implementării solicitărilor;
- înregistrarea informației privind elaborarea şi testarea modificărilor;
- determinarea procedurilor de recul în caz de modificări nereuşite;

- notificarea automată privind efectuarea analizei modificărilor implementate;
- pregătirea automată a informației administrative legate de modificări;
- capacitatea asamblării modificărilor;
- crearea automată a solicitărilor de modificare;
- urmărirea procesului de gestionare a modificărilor şi consecutivității acțiunilor întreprinse.

Software-ul trebuie să dispună de capacitatea actualizării la distanță a bazelor de date centralizate.

5.3.3. Indicatorii eficienței procesului de gestionare a modificărilor

Pentru îmbunătățirea coordonării serviciilor publice, furnizarea mai multor informații privind modificări, îmbunătățirea evaluării riscurilor, reducerea impactului negativ al modificărilor asupra calității serviciilor, reducerea numărului de modificări, îmbunătățirea gestionării problemelor şi accesibilității, sporirea productivității activității utilizatorilor şi prelucrarea volumelor mari de modificări, este necesar de a utiliza următorii indicatori:

- numărul impactelor negative asupra calității serviciilor;
- numărul de incidente survenite în rezultatul implementării modificărilor;
- numărul de reculuri ale modificărilor;
- numărul de modificări urgente;
- corespunderea dintre graficul aprobat al modificărilor şi implementarea reală a modificărilor;
- lipsa solicitărilor de modificare cu prioritate înaltă în lista de aşteptare;
- analiza regulată a solicitărilor de modificare şi a modificărilor implementate;
- coeficientul implementării reuşite a modificărilor;
- procentul solicitărilor de modificare respinse în mod nejustificat.

Pentru gestionarea eficientă a procesului de prestare a serviciilor este necesară efectuarea organizată a modificărilor, fără erori şi decizii incorecte. Pentru prestarea satisfăcătoare a serviciilor este necesar de gestionat modificările în mod rațional.

5.4. Procesul de gestionare a configurațiilor

Obiectivul procesului de gestionare a configurațiilor constă în evidența tuturor activelor şi configurațiilor informaționale în cadrul organizației şi serviciilor acesteia, furnizarea documentației pentru susținerea proceselor de gestionare a serviciilor, furnizarea şi verificarea informației despre configurație, precum şi asigurarea bazei pentru procesele de gestionare a incidentelor, problemelor, modificărilor, release-urilor.

Gestionarea configurațiilor trebuie să cuprindă identificarea, evidența şi rapoartele privind componentele informaționale ale infrastructurii TI. Elementele care trebuie să fie controlate de gestionarea configurațiilor includ toate componentele infrastructurii TI şi software-ul.

Gestionarea configurațiilor trebuie să fie legată de elaborarea de sistem, testarea, gestionarea modificărilor şi gestionarea release-urilor, să mențină şi să asigure securitatea bazei configurationale, a conținutului, documentației şi a rapoartelor acesteia.

Sistemul de gestionare a configurațiilor trebuie să asigure:

- controlul securității;
- susținerea elementelor de evidență cu grad diferit de dificultate;
- adăugarea uşoară a elementelor noi de evidență şi eliminarea celor vechi;
- verificarea automată a datelor introduse;
- instalarea automată a tuturor conexiunilor elementului nou de evidență în momentul adăugării acestuia;
- susținerea elementelor de evidență cu diferite coduri de modele, numere de versiuni şi copii;
- păstrarea înregistrărilor istorice cu privire la toate elementele de evidență;
- mijloacele flexibile de raportare.

5.4.1. Cerințele de bază față de procesul de gestionare a configurațiilor

Față de procesul de gestionare a configurațiilor urmează să fie înaintate următoarele cerințe:

- planificarea – stabilirea destinației, volumului, politicii, scopurilor, procedurilor pentru gestionarea configurației;
- identificarea configurațiilor – selectarea structurii configurației a tuturor elementelor de evidență, care aparțin infrastucturii, interacțiunile dintre acestea şi documentației de configurație. Identificarea trebuie să includă distribuirea identificatorilor, numerelor versiunilor elementelor de evidență, aplicarea marcajului pe fiecare element de evidență şi înregistrarea datelor despre ele în Baza de date configurațională a elementelor;
- controlul configurațiilor – asigurarea primirii şi înregistrării elementelor de evidență autorizate şi identificate pe parcursul ciclului de viață a acestora. Controlul trebuie să asigure disponibilitatea documentației corespunzătoare supuse controlului la adăugare, modificare, schimbare sau excluderea fiecărui element de evidență;
- evidența statutelor configurațiilor prevede raportarea după toate datele curente şi istorice pentru fiecare element de evidență pe parcursul ciclului de viață a acestuia. Evidența statutelor trebuie să urmărească modificările în elementele de evidență şi înregistrările acestora;
- efectuarea verificărilor şi auditului configurațiilor – succesiunea examinărilor şi auditurilor pentru a verifica existența fizică a elementelor de evidență şi corectitudinea înregistrării acestora în sistemul de gestionare a configurațiilor.

5.4.1.1. Planificarea gestionării configurațiilor

Planificarea gestionării configurațiilor trebuie să determine:

- strategia, politica, limitele şi obiectivele gestionării configurațiilor;
- politicile, standardele şi procesele aferente procesului de gestionare a serviciilor;
- rolurile şi responsabilitățile gestionării configurațiilor;
- analiza stării curente a activelor şi configurațiilor;
- acțiunile tehnice şi administrative ale procesului de gestionare a configurațiilor;
- politica proceselor de gestionare a modificărilor şi gestionării release-urilor;
- interacțiunea între proiecte, furnizori, aplicații şi grupurile de susținere;
- amplasarea depozitelor şi bibliotecilor pentru păstrarea hardware-ului, software-ului şi documentației.

Gestionarea configurațiilor trebuie să includă planificarea detaliată a controlului infrastructurii TI şi serviciilor în toate sistemele distribuite. Mijloacele sistemelor de gestionare a configurațiilor ale proiectelor aflate în proces de elaborare trebuie să funcționeze în mod integrat.

Acțiunile de bază ale procesului de gestionare a configurațiilor pentru planificare sînt:

- analiza detaliată a interacțiunii procesului de gestionare a configurațiilor cu alte procese de gestionare a prestării serviciilor;
- analiza posibilităților procesului de gestionare a configurațiilor;
- examinarea datelor configurationale;
- colectarea şi reexaminarea datelor privind cerințele şi specificațiile funcționale;
- selectarea mijloacelor de automatizare a Bazei de date configurationale a elementelor de evidență;
- determinarea tipurilor elementelor de evidență, atributelor acestora, tipurilor de interconexiuni;
- elaborarea proceselor şi a procedurilor de gestionare a configurațiilor;
- planificarea şi asigurarea depozitelor sigure ale elementelor de evidență, împreună cu procesul de gestionare a release-urilor.

5.4.1.2. Identificarea configurațiilor

Identificarea configurațiilor trebuie să determine selectarea, identificarea şi marcarea structurilor configurationale şi a elementelor de evidență. Identificarea configurației trebuie să includă atribuirea

unor identificatori elementelor de evidență şi documentația configurațională a acestora, şi să determine nivelul la care trebuie să fie efectuat controlul şi nivelul divizării elementelor generalizate de evidență pe componente.

5.4.1.2.1. Baza de date configurațională a elementelor de evidență

Identificarea şi documentarea configurației trebuie să sporească eficiența gestionării modificărilor. Procesul de gestionare a configurațiilor necesită utilizarea mijloacelor de susținere pentru păstrarea copiilor etalon ale software-ului şi documentației, inclusiv ale Bazei de date configurționale a elementelor de evidență.

Baza de date configurațională a elementelor de evidență trebuie să conțină legăturile între toate componentele sistemului, inclusiv incidentele, problemele, erorile cunoscute, modificările şi release-urile. Baza de date configurațională a elementelor de evidență trebuie să conțină informația privind incidentele, erorile şi problemele cunoscute, inclusiv datele despre angajați, furnizori, utilizatori, subdiviziuni organizaționale pentru fiecare element de evidență. Ea trebuie să fie actualizată în mod automat, atunci cînd este modificat statutul elementelor de evidență şi al release-urilor.

Configurația infrastructurii TI trebuie să fie divizată în părți, cărora le sînt atribuiți identificatori unici, ceea ce permite controlul şi înregistrarea eficientă a elementelor de evidență, formarea rapoartelor detaliate.

5.4.1.2.2. Componentele procesului de identificare a configurației

Procesul de identificare a configurației trebuie să includă hardware-ul şi software-ul utilizat pentru asamblarea, release-urile, verificarea, instalarea, distribuirea, susținerea, restabilirea şi trecerea la cheltuieli a elementelor de evidență. Componentele obligatorii pentru care este necesar de efectuat identificarea configurațiilor sînt următoarele:

- hardware-ul, inclusiv componentele de rețea;
- software-ul de sistem;
- sistemele şi aplicațiile organizației elaborate la comandă;
- pachetele de program gata, produsele standard şi produsele lucrului cu bazele de date;
- bazele configurționale;
- release-urile de software;
- documentația configurațională, licențele, acordurile privind mentenanța, acordul cu privire la nivelul de deservire.

Componentele trebuie să fie clasificate conform tipurilor elementelor de evidență (de exemplu, produsele de program, software-ul de sistem, hardware-ul), ceea ce permite determinarea şi documentarea elementelor utilizate, a statutului şi amplasării acestora.

5.4.1.2.3. Atributele elementelor de evidență

La gestionarea configurațiilor este necesar de a planifica atributele care trebuie să fie înregistrate. Atributele diferă pentru diferite tipuri de elemente de evidență.

Pentru înregistrarea elementelor de evidență trebuie folosită următoarea listă de atribute:

- denumirea elementului de evidență;
- numărul copiei, numărul de serie (identificatorul unic al elementului de evidență);
- categoria elementului de evidență;
- tipul elementului de evidență;
- numărul modelului, pentru hardware;
- data expirării termenului de garanție;
- numărul versiunii elementului de evidență;
- locație elementului de evidență;
- posesorul responsabil;
- sursa, furnizorul elementului de evidență;

- licența;
- datele de livrare şi primire;
- statutul elementului de evidență;
- legăturile elementului de evidență cu toate celelalte elemente de evidență;
- numerele solicitărilor de modificare, modificărilor, problemelor, incidentelor.

Baza configurațională trebuie determinată pentru un scop anumit, iar informația şi elementele de evidență care fac parte din aceasta trebuie să fie controlate.

Este necesară determinarea sistemului de gestionare a informației pentru identificarea elementelor de evidență, documentației configurationale, modificărilor, bazelor configurationale, release-urilor şi asamblărilor. Sistemul de gestionare a informației trebuie să fie unic şi să ia în considerație structura corporativă a organizației. Acesta trebuie să permită gestionarea interconexiunilor ierarhice între elementele de evidență, modificări şi incidente.

Toate elementele de evidență trebuie să fie marcate cu identificatorul configurației. Toate mijloacele de evidență ale hardware-ului necesită marcare fizică ce nu poate fi înlăturată. Toate cablurile şi liniile de conexiune trebuie să fie marcate clar la fiecare capăt şi în toate punctele de verificare.

Copiile etalon ale software-ului în biblioteca software-ului etalon trebuie să aibă marcajul software, care să conțină denumirea elementului de evidență şi numărul versiunii. Toți purtătorii care conțin software trebuie să fie marcați în mod clar cu denumirea elementului de evidență, numărul copiei şi numărul versiunii fiecărui element al software-ului, care se conține pe purtător.

5.4.1.3. Controlul configurațiilor

Scopul controlului configurațiilor constă în asigurarea înregistrării în Baza de date configurațională numai pentru elementele de evidență autorizate şi identificabile. Procedurile de control al configurațiilor trebuie să asigure integritatea datelor organizației, sistemelor şi proceselor.

Procesul de control al configurațiilor trebuie să asigure accesul numai software-ului autorizat şi licențiat în biblioteca software-ului etalon, precum şi protecția acestora. Numai personalul autorizat poate avea acces la biblioteca software-ului etalon. Elementele existente aflate sub controlul gestionării configurațiilor nu trebuie să fie modificate fără autorizare. Toate versiunile neautorizate ale elementelor de evidență şi înseşi elementele de evidență trebuie să fie lichidate sau transmise sub controlul gestionării configurațiilor.

Procedurile permanente de control al configurațiilor trebuie să includă:
- înregistrarea tuturor elementelor de evidență noi şi a versiunilor acestora;
- actualizarea înregistrărilor privind elementele de evidență (modificarea statutului, actualizarea atributelor, modificări în posesie sau roluri, actualizarea atributelor, modificări în posesiune sau roluri, versiuni noi ale documentației, controlul licențelor);
- actualizarea solicitărilor de modificare;
- protecția integrității configurațiilor;
- actualizarea Bazei de date configurationale a elementelor de evidență.

După efectuarea controlului calității, software-ul devine autorizat pentru primire şi copiere în biblioteca software-ului etalon. Software-ul nu trebuie să fie deteriorat sau modificat în timpul proceselor de copiere şi distribuire. Documentația corespunzătoare, certificatele privind testarea şi licența trebuie să fie amplasate în biblioteca controlată a documentelor.

Modificările în atributele elementelor de evidență în Baza de date configurațională a elementelor de evidență trebuie să fie actualizate împreună cu solicitările respective de modificare.

Este necesar de a efectua controlul eliminării şi înlăturării elementelor de evidență din motive financiare şi pentru asigurarea securității. Este necesară existența procedurilor de trecere la cheltuieli a hardware-ului sau software-ului în scopul asigurării actualizării elementelor corespunzătoare de

evidență. Procesele de achiziție, păstrare, expediere, primire, eliberare a mărfurilor trebuie să asigure integritatea hardware-ului, software-ului şi documentației.

Gestionarea configurațiilor trebuie să asigure integritatea elementelor de evidență păstrate de tip software cu ajutorul:

- selectării purtătorului pentru păstrare, în scopul minimalizării erorilor legate de restabilirea şi deteriorarea posibilă a datelor;
- efectuării verificărilor şi actualizărilor elementelor de evidență din arhivă;
- păstrării duplicatelor în locuri controlabile.

Dublarea permanentă a elementelor de evidență este importantă pentru asigurarea lipsei elementelor străine.

5.4.1.4. Evidența statutelor configurațiilor

Rapoartele privind evidența statutului elementelor de evidență trebuie să includă identificatorii unici ai componentelor elementelor de evidență, statutul curent, bazele configurationale, release-urile, versiunile de software, persoana responsabilă pentru modificarea statutului, istoria modificărilor, problemele deschise.

Pînă la trecerea în mediul de exploatare, release-urile noi, asamblările, echipamentul şi standardele trebuie supuse verificării în baza cerințelor înaintate. Pentru confirmarea verificării este necesară prezența certificatului cu privire la testare.

5.4.1.5. Verificarea şi auditul configurațiilor

Pentru verificarea Bazei de date configurationale a elementelor de evidență în ceea ce priveşte corespunderea cu starea fizică a tuturor elementelor de evidență este necesară existența planurilor controalelor regulate de audit al configurațiilor. Auditurile trebuie să confirme existența versiunilor corecte şi autorizate ale elementelor de evidență. La efectuarea auditului configurațiilor este necesară verificarea faptului dacă înregistrările despre modificări şi release-uri sînt autorizate de gestionarea modificărilor.

Auditul configurațiilor trebuie efectuat în urma:

- implementării unui sistem nou de gestionare a configurațiilor;
- unor modificări majore în infrastructura TI;
- release-ului software-ului;
- restabilirii care urmează după un accident major;
- depistării unor elemente de evidență neautorizate.

Mijloacele de audit automat trebuie să efectueze verificări sistematice la un anumit interval de timp. Auditul permanent al configurațiilor contribuie la utilizarea mai eficientă a resurselor.

5.4.1.6. Întocmirea rapoartelor administrative

Rapoartele administrative privind procesul de gestionare a configurațiilor trebuie să includă următoarele:

- rezultatele auditului configurațiilor;
- informația despre elementele de evidență neînregistrate sau înregistrate incorect depistate;
- informația despre numărul de elemente de evidență înregistrate şi versiunile acestora, cu clasificare în categorii, tipuri şi statut;
- informația privind rapiditatea introducerii modificărilor în Baza de date configurațională;
- informația despre rețineri şi cauze în activitatea procesului de gestionare a configurațiilor;
- analiza eficienței, creşterii şi auditului în gestionarea configurațiilor;
- valoarea şi locația elementelor de evidență.

În baza rapoartelor administrative se va stabili dezvoltarea ulterioară a gestionării configurațiilor, luîndu-se în considerație sarcina planificată pentru procesul de gestionare a configurațiilor şi creşterea preconizată.

5.4.2. Acțiunile procesului de gestionare a configurațiilor

În procesul de gestionare a configurațiilor este necesar de îndeplinit următoarele acțiuni:

- furnizarea informației corecte şi exacte privind configurațiile şi specificațiile fizice şi funcționale ale acestora personalului procesului de gestionare şi susținere a serviciilor publice;
- determinarea şi documentarea procedurilor procesului de gestionare a configurațiilor;
- identificarea, marcarea, înregistrarea denumirilor şi versiunilor elementelor de evidență;
- controlul şi păstrarea copiilor etalon autorizate şi verificate ale specificațiilor, documentației şi software-ului;
- urmărirea şi înregistrarea datelor privind configurațiile în conformitate cu starea actuală a infrastructurii informaționale;
- raportare privind metricele elementelor de evidență;
- auditul şi raportarea privind încălcările standardelor infrastructurii şi procedurilor de gestionare a configurațiilor.

În cadrul realizării procesului de gestionare a configurațiilor trebuie să fie aplicate bibliotecile fizice şi electronice de software care urmează să fie identificate cu ajutorul următoarei informații:

- conținutul, locația şi purtătorul pentru fiecare bibliotecă;
- condițiile furnizării elementului la păstrare;
- măsurile de protecție a bibliotecii şi procedurile de restabilire;
- condițiile şi controlul accesului pentru grupurile de utilizatori pentru înregistrarea, citirea, actualizarea, copierea, transferul sau eliminarea elementelor de evidență.

Mijloacele de susținere permit efectuarea controlului software-ului aplicativ de la analiza şi proiectarea inițială de sistem pînă la exploatare. Mijloacele de gestionare a configurațiilor infrastructurii TI trebuie să transmită informația procesului de gestionare a configurațiilor din sistemul de gestionare a configurațiilor pentru elaborarea software-ului în Baza de date configurațională a elementelor de evidență fără introducere repetată.

Mijloacele de gestionare a configurațiilor trebuie să efectueze susținerea automată a următoarelor acțiuni:

- identificarea elementelor de evidență conexe;
- implementarea modificărilor;
- înregistrarea modificărilor la statutele elementelor de evidență în cazul introducerii modificărilor autorizate şi a release-urilor;
- înregistrarea bazelor configurationale ale elementelor de evidență şi ale pachetelor elementelor de evidență.

În procesul de gestionare a configurațiilor trebuie să fie utilizate tehnologiile Internet şi diferite mijloace software de susținere, cum sînt:

- sistemele de gestionare a circuitului de documente;
- mijloacele de construire a arhitecturii sistemului;
- mijloacele de elaborare automată a sistemelor;
- mijloacele de gestionare a auditului bazelor de date;
- mijloacele de distribuire şi instalare;
- mijloacele de comparare, implementare a release-urilor şi asamblării;
- mijloacele de comprimare, gestionare a listelor şi a bazelor configurationale;
- mijloacele de depistare şi restabilire.

5.4.3. Indicatorii eficienței procesului de gestionare a configurațiilor

Pentru furnizarea informației exacte privind elementele de evidență, controlul elementelor de evidență valoroase, accesibilitatea informației privind modificările efectuate în software, participare la planificarea acțiunilor în situații excepționale, îmbunătățirea securității prin intermediul

controlului versiunilor utilizate ale elementelor de evidență, precum şi pentru acordarea posibilității de reducere a utilizării software-ului nesancționat este necesar de aplicat următorii indicatori speciali:

- numărul de elemente neautorizate de evidență ale configurației;
- incidentele şi problemele care reprezintă consecința unor modificări efectuate incorect;
- modificările timpului mediu şi ale cheltuielilor pentru diagnosticarea şi reglarea adresărilor în CGE de prestare a serviciilor;
- modificarea numărului şi gravității situațiilor de încălcare a Acordului cu privire la nivelul de deservire;
- solicitările de modificare care nu au fost soluționate cu succes;
- timpul ciclului între aprobarea şi implementarea modificărilor;
- numărul de licențe de software pierdute şi neutilizate;
- datele primite în rezultatul efectuării auditului configurațiilor;
- modificările numărului şi semnificației incidentelor şi problemelor;
- numărul de modificări lunare în Baza de date configurațională a elementelor de evidență din cauza erorilor depistate.

5.5. Procesul de gestionare a release-urilor

Obiectivele procesului de gestionare a release-urilor:

- planificarea şi supravegherea desfăşurării reuşite a software-ului şi a hardware-ului aferent acestuia;
- proiectarea şi implementarea procedurilor pentru distribuirea şi instalarea modificărilor;
- asigurarea instalării doar a versiunilor corecte, autorizate şi testate;
- interacțiunile cu clienții şi controlul aşteptărilor clientului în timpul planificării şi desfăşurării release-urilor noi;
- aprobarea conținutului exact al release-ului şi al planului de desfăşurare al acestuia;
- implementarea release-urilor noi de hardware şi software în mediul de exploatare cu utilizarea proceselor de gestionare a configurațiilor (a se vedea 5.4) şi gestionare a modificărilor (a se vedea 5.3);
- asigurarea păstrării în siguranță a copiilor întregului software;
- asigurarea securității şi posibilității de urmărire la desfăşurarea sau modificarea hardware-ului.

În procesul de gestionare a release-urilor este necesar de acordat atenție protecției mediului de exploatare şi a serviciilor acestuia prin intermediul procedurilor şi verificărilor.

Gestionarea release-urilor trebuie să fie finanțată din contul bugetului şi nu trebuie inclusă în cheltuielile privind prestarea serviciilor clienților.

5.5.1. Cerințele de bază față de procesul de gestionare a release-urilor

În procesul de gestionare a release-urilor este necesar de respectat cerințele de planificare, proiectare, asamblare, configurare şi testare a hardware-ului şi software-ului.

Cerințele de bază respectate în procesul de gestionare a release-urilor sînt următoarele:

- elaborarea politicii şi planificarea release-urilor;
- proiectarea, asamblarea şi configurarea release-urilor;
- primirea release-urilor;
- planificarea desfăşurării release-urilor;
- testarea release-urilor multilaterale conform criteriilor de primire stabilite;
- confirmarea finalizării release-ului pentru implementarea ulterioară;
- comunicațiile, pregătirea şi instruirea personalului;
- efectuarea auditului hardware-ului şi software-ului pînă la şi după implementarea modificărilor;
- instalarea echipamentului nou şi modernizat;

- păstrarea software-ului controlat în sisteme centralizate şi distribuite;
- release-ul, distribuirea şi instalarea software-ului.

5.5.1.1. Elaborarea politicii şi planificarea release-urilor

5.5.1.1.1. Elaborarea politicii release-urilor

Politica release-urilor trebuie să includă regulile de numerotare a release-urilor, frecvența lor şi nivelurile în infrastructură care vor fi controlate de aceste release-uri. Numărul necesar şi frecvența release-urilor trebuie să fie determinate în funcție de dimensiunile şi tipul sistemelor. Fiecare release trebuie să aibă un identificator unic, care va fi folosit în procesul de gestionare a configurațiilor conform schemei determinate în politica release-urilor. Identificarea release-urilor trebuie să includă referința la componenta infrastructurii (elementul de evidență), pe care îl prezintă acest release, şi numărul versiunii. În caz de modificare a infrastructurii, politica release-urilor trebuie să fie revizuită şi extinsă.

Politica release-urilor trebuie să explice clar rolurile şi obligațiile în procesul de gestionare a release-urilor.

Politica release-urilor trebuie să includă următoarea informație:
- nivelul controlului infrastructurii pentru fiecare tip de release;
- regulile de denumire şi numerotare a release-urilor;
- determinarea release-urilor complexe şi parțiale;
- indicații privind frecvența efectuării release-urilor complexe şi parțiale;
- rezultatele scontate pentru fiecare tip de release;
- indicații referitor la modul şi locul în care trebuie să fie documentate release-urile;
- crearea şi testarea planurilor de recul;
- descrierea procesului de control al gestionării release-urilor;
- documentarea configurației bibliotecii software-ului etalon şi determinarea criteriilor de primire pentru adăugarea software-ului nou.

5.5.1.1.2. Planificarea release-urilor

Planificarea release-urilor trebuie să includă:
- constituirea acordului comun privind conținutul release-ului;
- convenirea asupra etapelor în timp;
- alcătuirea graficului generalizat al release-urilor;
- desfăşurarea sondajelor de opinie pentru evaluarea hardware-ului şi software-ului utilizat;
- planificarea nivelurilor de încărcare a personalului;
- coordonarea rolurilor şi obligațiilor;
- propuneri privind procurarea software-ului şi hardware-ului nou;
- elaborarea planurilor de recul;
- elaborarea planului de asigurare a calității release-ului;
- planificarea primirii de către grupurile de susținere şi de către client.

5.5.1.2. Proiectarea, asamblarea şi configurarea release-urilor

Este necesar de a planifica şi documenta procedurile pentru asamblarea release-urilor de software. Instrucțiunile privind asamblarea release-ului fac parte din determinarea release-ului.

Acțiunile de asamblare trebuie să includă compilarea şi legarea modulelor aplicațiilor elaborate independent şi a întregului software procurat. Asamblarea trebuie să conțină acțiuni de creare a bazelor de date şi completare a acestora cu date de test sau date statistice din indicatoare.

Toate software-urile, parametrii, datele de test, software-urile de susținere a executării programelor, necesare pentru release, trebuie să se afle sub controlul gestionării configurațiilor. Evidența deplină a rezultatelor asamblării trebuie să fie înregistrată în Baza de date configurațională a hardware-ului.

Controlul asamblării şi release-urilor trebuie să asigure asamblarea corectă şi distribuirea versiunilor actualizate de hardware şi software.

Procedurile de asamblare şi automatizarea trebuie să fie controlate ca elemente de evidenţă separate. Procedurile de gestionare a asamblării şi distribuirii software-ului trebuie să fie testate pînă la începutul utilizării lor. La prima etapă de exploatare, este necesar de a acorda timp pentru soluţionarea problemelor legate de introducerea inovaţiilor.

Procedurile, şabloanele, recomandările trebuie să fie planificate pentru îndeplinirea eficientă a release-urilor de hardware şi software.

5.5.1.3. Primirea release-urilor

Testarea trebuie să includă procedurile de instalare şi integritatea funcţională a sistemului gata. Este necesar de a efectua confirmarea finalizării fiecărei etape de testare.

Primirea release-ului trebuie efectuată în mediul de testare controlat care poate fi restabilit în baza configuraţiei cunoscute a software-ului şi hardware-ului. Aceste configuraţii trebuie să fie caracterizate în descrierea release-ului şi să fie păstrate în Baza de date configurațională a elementelor de evidenţă împreună cu toate celelalte elemente de evidenţă.

Dacă release-ul este respins, atunci acesta trebuie să fie replanificat pentru un alt timp de gestionare a modificărilor şi trebuie să fie urmărit în rapoartele de gestionare a modificărilor în calitate de modificări nereuşite.

Rezultatul final al acţiunilor de verificare trebuie să fie confirmarea finalizării depline şi exacte a întregului release.

5.5.1.4. Planificarea desfăşurării release-urilor

Planificarea desfăşurării trebuie să extindă planul release-ului şi să includă următoarea informaţie:

- pregătirea orarului exact şi detaliat al evenimentelor împreună cu informaţia despre persoană si sarcinile executate;
- listele elementelor de evidenţă pentru instalare şi trecerea la cheltuieli;
- formarea descrierii release-ului şi comunicaţiilor;
- planificarea comunicaţiilor cu utilizatorul final;
- elaborarea planului de achiziţii;
- procurarea software-ului şi hardware-ului.

În cazul unui eşec parţial sau total în desfăşurarea release-ului, trebuie să fie elaborat un plan de recul pentru documentarea acţiunilor de restabilire a serviciului. Sînt posibile două abordări:

- desfăşurarea nereuşită revine integral la starea iniţială pînă la restabilirea completă a serviciilor la starea lor anterioară cunoscută;
- întreprinderea măsurilor privind restabilirea mai completă a prestării serviciilor, dacă acestea nu pot fi restabilite integral (este posibilă varianta delta-release-ului).

Planul de recul trebuie să fie verificat în procesul evaluării riscurilor în planul general de desfăşurare şi să fie recunoscut drept suficient de către client.

5.5.1.5. Testarea de primire şi confirmarea finalizării release-ului

Pînă la desfăşurarea release-ului în mediul de exploatare, acesta trebuie să fie supus testării şi primirii obligatorii de către client, care se împarte în:

- testarea funcţională;
- testarea operaţională;
- testarea exploataţională;
- testarea integraţională.

Pînă la desfăşurarea release-ului, utilizatorul trebuie să confirme finalizarea release-ului. Cea mai frecventă cauză a modificărilor şi release-urilor nereuşite este testarea insuficientă.

5.5.1.6. Comunicaţiile, pregătirea şi instruirea personalului

Personalul de gestionare a release-urilor trebuie să fie instruit în teoria şi practica gestionării modificărilor şi gestionării configurațiilor, elaborarea şi mentenanța software-ului, utilizarea mijloacelor de suport şi a programelor auxiliare.

Personalul care interacționează cu clientul, personalul clientului şi personalul CGE de prestare a serviciilor trebuie să fie la curent cu acțiunile planificate şi modul în care aceste acțiuni pot influența prestarea serviciilor. Este necesar de înştiințat toate părțile interesate despre problemele şi modificările survenite, pentru a le informa cu privire la situația curentă şi pentru a le forma aşteptările.

5.5.1.7. Release-ul, distribuirea şi instalarea software-ului

Distribuirea release-urilor de software din mediul de asamblare în mediul de exploatare trebuie să aibă loc concomitent cu toate modificările din hardware. Distribuirea software-ului trebuie să fie proiectată astfel, încît să fie menținută integritatea software-ului în timpul prelucrării, ambalării şi livrării. După distribuirea software-ului şi după ce release-ul ajunge la locul de destinație, este necesar de a verifica completitudinea acestui release.

Baza de date configurațională a elementelor de evidență trebuie să fie actualizată după instalarea sau înlăturarea software-ului sau hardware-ului, ceea ce va asigura existența datelor actualizate în Baza de date configurațională a elementelor de evidență.

În procesul de gestionare a release-urilor trebuie efectuat controlul următoarelor componente:

- aplicații software de elaborare proprie;
- software la comandă;
- software auxiliar;
- software de sistem;
- hardware şi specificațiile sale;
- instrucțiuni privind asamblarea şi documentație.

Toate componentele enumerate mai sus trebuie să fie gestionate în mod eficient, de la elaborarea sau procurarea lor şi pînă la setare şi configurare, de la testare şi implementare şi pînă la funcționare în mediul de exploatare.

5.5.2. Tipurile şi clasificarea release-urilor

5.5.2.1. Tipurile release-urilor

Unitatea de release descrie o parte a infrastructurii software-ului. Unitatea de release depinde de tipul sau elementul software-ului şi hardware-ului.

La selectarea nivelului unității de release trebuie să se țină cont de următorii factori:

- volumul modificărilor necesare;
- volumul resurselor şi timpul necesar pentru asamblarea, testarea, distribuirea şi implementarea release-urilor la fiecare nivel;
- simplitatea implementării;
- complexitatea interfețelor între unitatea propusă şi restul infrastructurii;
- spațiul accesibil pe disc în mediul de asamblare, în mediul de testare, în mediul de distribuire şi în mediul de exploatare.

Există următoarele tipuri de release-uri:

- release-ul complex – toate componentele unității de release sînt asamblate, testate, distribuite şi implementate împreună. În acest release este exclus pericolul utilizării unor versiuni învechite ale elementelor de evidență. Neajunsul unei astfel de abordări este creşterea volumului, eforturilor şi resurselor computerizate implicate în asamblarea, testarea, distribuirea şi implementarea release-urilor. Este necesară efectuarea unei testări regresive pentru excluderea înrăutățirii funcțiilor de sistem sau a comportamentului sistemului;
- delta-release-ul (parțial) – cuprinde în cadrul unității de release doar acele elemente de evidență

care au fost modificate sau elementele de evidență noi;

- release-ul de pachet – gruparea unor release-uri separate care reduce posibilitatea utilizării unui software vechi sau incompatibil, ceea ce contribuie la testarea deplină a funcționării mixte a grupurilor de programe şi sisteme.

5.5.2.2. Clasificarea release-urilor

Release-ul trebuie folosit pentru descrierea grupului de modificări din cadrul serviciului. Release-ul constă din decizii privind înlăturarea problemelor şi îmbunătățirile serviciilor prestate. Release-ul trebuie format din software-ul necesar nou sau modificat şi din hardware-ul nou sau modificat necesare pentru implementarea deciziilor aprobate.

Release-urile se clasifică în modul următor:

- release-urile mari de software şi modernizarea hardware-ului – funcțiile noi voluminoase care duc la înlocuirea acțiunilor inutile de corectare a unor probleme;
- release-uri mici de software şi modernizarea hardware-ului – îmbunătățiri şi corectări nesemnificative;
- corectări urgente ale software-ului şi hardware-ului – corectările unui număr mic de probleme cunoscute.

Dependența dintre versiunea specială a software-ului şi hardware-ul necesar pentru funcționarea acesteia duce la îmbinarea software-ului şi hardware-ului într-un release cu alte cerințe funcționale.

Pe măsură ce creşte eficiența gestionării release-urilor, creşte şi eficacitatea activității personalului implicat în prestarea serviciilor.

5.5.3. Mijloacele specializate ale sistemului de gestionare a release-urilor

Gestionarea release-urilor trebuie să utilizeze:

- mijloace de gestionare a modificărilor – pentru înregistrarea informației privind modificările planificate, pentru păstrarea informației despre release-uri şi referințele la modificări;
- mijloace de gestionare a configurațiilor – pentru înregistrarea elementelor de evidență ale software-ului şi hardware-ului în Baza de date configurațională a elementelor de evidență;
- mijloace de gestionare a configurațiilor software-ului – pentru gestionarea versiunilor codului de program în timpul elaborării care pot prelucra pachete de modificări, pentru integrarea cu informația despre problemă şi solicitările de modificare;
- mijloace ale procesului de gestionare a asamblării – pentru asamblarea automată a release-urilor noi ale aplicațiilor de program, pentru generarea şi lansarea versiunilor executate ale fişierelor;
- mijloace de distribuire etalon a software-ului – pentru livrarea garantată a fişierelor de program, pentru optimizarea capacității de transmitere a rețelei, pentru păstrarea versiunilor noi ale aplicațiilor în stare de aşteptare;
- mijloace de efectuare a auditului software-ului şi hardware-ului –pentru identificarea software-ului instalat şi pentru depistarea celor mai critice momente în configurația hardware-ului;
- mijloace de gestionare a stațiilor de lucru – pentru configurarea corectă a parametrilor sistemului de operare şi controlul acestora, pentru păstrarea tuturor fişierelor de instalare pe server şi actualizarea acestor fişiere pe măsura adăugării release-urilor noi în biblioteca software-ului etalon;
- mijloace de gestionare a server-elor – pentru controlul la distanță al operațiilor pe server, pentru monitorizarea la distanță a registrului de înregistrare a evenimentelor, pentru monitorizarea utilizării resurselor procesorului, memoriei şi spațiului pe disc.

5.5.3.1. Baza de date configurațională a elementelor de evidență

Baza de date configurațională a elementelor de evidență trebuie să conțină următoarea informație pentru susținerea procesului de gestionare a release-urilor:

- descrierea release-urilor planificate, inclusiv elementele de evidență ale hardware-ului şi software-ului, împreună cu referințele la solicitările inițiale de modificare;

- înregistrările privind elementele de evidență asupra cărora acționează release-urile planificate şi cele din trecut;
- informația şi locația specială de destinație a componentelor release-ului.

5.5.3.2. Biblioteca software-ului etalon

Biblioteca software-ului etalon este un depozit sigur în care sînt păstrate în siguranță versiunile etalon ale tuturor elementelor de evidență de tip software, atît software elaborat în organizație, cît şi procurat. Acest depozit trebuie să fie format din una sau mai multe biblioteci sau depozite de fişiere separate de depozitele fişierelor pentru elaborare, testare sau exploatare.

Biblioteca software-ului etalon este parte a politicii release-urilor şi trebuie să conțină:
- tipul purtătorului, locația fizică, hardware-ul şi software-ul presupus;
- acordurile privind atribuirea denumirilor pentru depozitele de fişiere şi purtătorii fizici;
- mediile suportate;
- măsurile de securitate pentru perfectarea modificărilor şi lansării software-ului;
- perioada de păstrare a release-urilor vechi de software;
- planul de dezvoltare a capacităților pentru bibliotecă;
- procedurile de audit;
- procedurile de asigurare a protecției bibliotecii contra modificărilor greşite.

Depozitul hardware-ului etalon este locul pentru păstrarea în siguranță a hardware-ului etalon de rezervă (componentele de rezervă şi modulele asamblate).

5.5.4. Indicatorii eficienței procesului de gestionare a release-urilor

Pentru garanția calității software-ului şi hardware-ului, îmbunătățirea utilizării resurselor, susținerea înregistrărilor depline ale modificărilor în mediul de exploatare, de controlul şi protecția activelor de hardware şi software, efectuarea unui număr mare de modificări în sisteme este necesar de analizat următorii indicatori:
- corespunderea asamblării şi implementării release-ului cu graficul şi limitele bugetului;
- rata deficiențelor la asamblare;
- securitatea şi gestionarea exactă a bibliotecii software-ului etalon;
- absența în biblioteca software-ului etalon a elementelor de evidență care nu au trecut verificarea calității;
- corespunderea spațiului pe disc cerințelor bibliotecii software-ului etalon;
- respectarea tuturor restricțiilor legislative privind software-ul procurat;
- distribuirea exactă a release-urilor;
- implementarea la timp a release-urilor;
- absența cazurilor de utilizare a unor software neautorizate;
- înregistrarea exactă şi la timp a tuturor acțiunilor privind asamblarea, distribuirea şi implementarea în Baza de date configurațională a elementelor de evidență;
- corespunderea conținutului planificat al release-ului cu conținutul real;
- cota release-urilor reuşite;
- concordarea proceselor legate de release-urile platformelor de hardware sau ale mediilor de program;
- numărul minim de întreruperi în prestarea serviciilor;
- stabilitatea mediului de testare şi mediului de exploatare;
- numărul de erori care ajung în mediul de exploatare;
- posibilitatea apariției şi utilizării copiilor ilegale de software;
- utilizarea TI şi a resurselor umane;
- numărul de release-uri desfăşurate pentru clienți;
- timpul depistării versiunilor şi copiilor incorecte de software;

- perioada de emitere a release-urilor;
- perioada de asamblare şi control al software-ului.

6. Infrastructura TI a prestării serviciilor publice

Infrastructura TI reprezintă sistemul structurilor organizaționale şi al mijloacelor tehnice care asigură formarea, distribuirea şi utilizarea tehnologiilor informațional-comunicaționale, care permit asigurarea interacțiunii organelor administrației publice, oferind acces la resursele informaționale.

Componentele de bază ale infrastructurii TI sînt următoarele:

- mijloacele hardware – reprezintă complexul dispozitivelor electronice, electrice şi mecanice care intră în componența sistemelor şi rețelelor informaționale ale organelor administrației publice;
- sistemele operaționale – asigură executarea programelor şi aplicațiilor, distribuirea resurselor, planificarea, introducerea-ieşirea şi gestionarea datelor, precum şi determină grupul conex de protocoale de nivele superioare pentru îndeplinirea funcțiilor de bază ale rețelei;
- bazele de date - reprezintă o totalitate de date conexe, organizate conform unor reguli stabilite care stabilesc principiile generale de descriere, păstrare şi procesare a datelor;
- rețeaua de telecomunicații – reprezintă totalitatea componentelor de bază ale prelucrării informației şi telecomunicațiilor care asigură schimbul de date prin intermediul complexului de mijloace software şi hardware conexe;
- mijloacele de susținere – asigură susținerea funcționării tuturor sistemelor şi rețelelor informaționale (de exemplu, mijloacele gestionării productivității serverului, mijloacele de gestionare a păstrării datelor);
- mijloacele multimedia – asigură chemarea semnalului televizat către monitor, ieşirea video complexă, desfăşurarea imaginilor video vii pe ecran, filtrarea digitală şi manevrarea scării imaginilor video, compresiunea de aparate digitale şi decompresiunea video, precum şi accelerarea operațiilor grafice legate de grafica tridimensională.

Fiecare componentă a infrastructurii TI trebuie folosită pentru automatizarea gestionării acțiunilor realizate, legate de fiecare sarcină în ciclul de viață al serviciilor publice – de la planificarea unui serviciu nou pînă la scoaterea acestuia din utilizare.

Complexitatea componentelor infrastructurii TI trebuie să depindă de nomenclatura serviciilor publice prestate, precum şi de nivelul interacțiunii organelor administrației publice şi de funcțiile îndeplinite de acestea.

6.1. Cerințele față de componentele infrastructurii TI

Pentru a obține un nivel înalt de calitate a serviciilor publice prestate, este necesar de a asigura funcționarea cuvenită, optimizarea, utilizarea şi securitatea tuturor componentelor infrastructurii TI prin intermediul realizării tuturor proceselor de gestionare a prestării serviciilor publice.

Cerințele față de componentele infrastructurii TI în cadrul etapelor ciclului de viață trebuie să includă următoarele:

- planificarea şi elaborarea componentei noi:

1) este necesar de verificat compatibilitatea şi posibilitatea integrării componentei noi cu componentele existente ale infrastructurii, examinîndu-se procesele de gestionare şi arhitectura fiecărei componente;

2) este necesar de evaluat avantajele în urma implementării, cerințele şi necesitățile componentei noi, stabilitatea funcționării componentei noi şi durata preconizată a ciclului de viață al acesteia, precum şi analiza şi gestionarea riscurilor legate de implementarea componentei noi;

3) este necesar de determinat tipul elaborării componentei noi: elaborarea funcțională (formarea setului de specificații funcționale ale cerințelor şi criteriilor privind componentele) sau elaborarea tehnică (stabilirea parametrilor tehnici ai componentei noi în infrastructura curentă);

- implementarea componentelor:

1) este necesar de elaborat, de susținut şi de gestionat planul de desfăşurare a componentelor care să conțină perioada de timp şi resursele necesare pentru implementarea fiecărei componente a infrastructurii;

2) este necesar de selectat o echipă de specialişti cu calificare necesară şi abilități pentru executarea implementării;

3) este necesar de evaluat riscurile care pot surveni în procesul implementării componentelor, nivelul corespunderii caracteristicilor funcționale şi tehnice cu cerințele fixate, stabilitatea şi caracterul adecvat al întregii infrastructuri TI în raport cu fiecare componentă nouă;

4) este necesar de aplicat diferite nivele de integrare: integrarea evenimentelor (capacitatea de a efectua schimbul de informații între componente), integrarea datelor (capacitatea de a distribui un set comun de date diferitor componente) şi integrarea funcțională (capacitatea componentelor de a interacționa şi de a coordona comportamentul lor funcțional între ele);

5) este necesar de asigurat existența şi accesibilitatea documentației privind implementarea pentru suportul şi deservirea tehnică ulterioară a componentelor infrastructurii;

- deservirea componentelor:

1) deservirea trebuie să reprezinte un proces neîntrerupt;

2) toate sarcinile de deservire trebuie să fie coordonate şi aprobate de persoanele responsabile din cadrul organizației;

3) deservirea trebuie să includă monitorizarea şi controlul evenimentelor legate de toate componentele infrastructurii TI;

4) rezultatele deservirii componentelor trebuie să includă stabilitatea şi fiabilitatea componentelor, documentația ce conține datele privind deservirea componentelor, precum şi registrul sau baza de date cu toate evenimentele de deservire, alarme şi semnale.

La toate etapele ciclului de viață al componentelor infrastructurii TI este necesar de îndeplinit cerințele securității față de componentele infrastructurii şi față de mijloacele de asigurare a securității.

6.2. Criteriile de selectare a componentelor infrastructurii TI

La alegerea componentelor infrastructurii TI pentru prestarea serviciilor publice este necesar de a lua în considerație următorii factori:

- cerințele tot mai complicate ale utilizatorilor;
- insuficiența abilităților în domeniul TI;
- restricțiile bugetare;
- dependența organizației de serviciile publice de calitate;
- complexitatea în creştere a infrastructurii;
- apariția modificărilor în standardele internaționale şi în legislație;
- scara ascendentă şi frecvența modificărilor în prestarea serviciilor publice.

La planificarea achizițiilor de componente ale infrastructurii TI este necesar de utilizat următoarele criterii de evaluare a acestora:

- corespunderea în proporție de 80% cu cerințele de exploatare;
- conformitatea tuturor cerințelor obligatorii;
- necesitatea minoră sau lipsa necesității unor lucrări de finisare;
- structura rezonabilă a datelor şi a procesării acestora;
- orientarea spre cerințele concrete ale prestării serviciilor publice şi nu spre tehnologii;
- flexibilitatea în implementare, utilizare;
- comoditatea în procesul de utilizare, facilitatea generală în utilizare, oferită de interfața utilizatorului;
- integrarea şi contradictorialitatea cu componentele existente ale infrastructurii diferitor furnizori;

- asigurarea continuității, rezervării, controlului şi securității;
- dependența de furnizori, parteneri;
- corelația dintre prețul şi calitatea componentelor;
- cheltuielile pentru administrare şi susținere sînt în limitele bugetului.

În procesul de selectare a componentelor infrastructurii TI pentru sistemul de prestare a serviciilor publice este necesar de luat decizia privind utilizarea componentelor moderne ce sînt implementate sau elaborarea completă a noilor componente. Dacă se ia decizia de a elabora o componentă nouă, este necesar de stabilit dacă elaborarea va fi realizată de propriul personal sau în baza utilizării serviciilor de outsourcing.

În caz de adoptare a deciziei privind utilizarea serviciilor de outsourcing pentru elaborarea componentelor infrastructurii TI, se vor lua în considerație următorii factori:

- cheltuielile de elaborare prin utilizarea forțelor proprii în raport cu costul serviciilor de outsourcing;
- riscurile de încălcare a regimului de securitate informațională;
- riscurile de încetare a colaborării cu organizația care prestează servicii de outsourcing şi dezvoltarea ulterioară a aplicației elaborate.

7. Monitorizarea procesului de prestare a serviciilor publice

7.1. Monitorizarea şi evaluarea procesului de prestare a serviciilor publice

Organizația care prestează servicii publice trebuie să efectueze monitorizarea consecventă a productivității pentru evaluarea rezultatelor şi productivității proceselor de prestare a serviciilor.

Monitorizarea şi evaluarea serviciilor este procesul de primire de către personal a datelor actuale privind starea serviciilor prestate: starea proceselor, încărcarea serverelor, timpul de reacție a aplicațiilor.

Se deosebesc următoarele tipuri de monitorizare şi evaluare a prestării serviciilor:

- monitorizarea internă şi evaluarea internă – sînt planificate şi efectuate cu forțele organizației care prestează servicii publice;
- monitorizarea externă şi evaluarea externă – sînt efectuate de o structură independentă, special invitată pentru efectuarea lor.

Monitorizarea trebuie să includă un complex de urmăriri dinamice, evaluare analitică şi pronosticare a stării de integritate a sistemului informațional de prestare a serviciilor.

7.1.1. Obiectivele şi sarcinile monitorizării şi evaluării prestării serviciilor publice

Obiectivele şi sarcinile monitorizării şi evaluării prestării serviciilor sînt următoarele:

- efectuarea monitorizării proceselor de prestare a serviciilor;
- procesul de urmărire şi evaluare a productivității prestării serviciilor – trebuie să fie reflectat în registre, înregistrări de control şi rapoarte;
- evaluarea caracterului adecvat al controlului intern;
- automatizarea evaluării continue a eficienței controlului intern;
- obținerea garanțiilor independente ale calității serviciilor prestate;
- asigurarea conformității cu documentele normative;
- actualizarea Bazei de date configurationale a elementelor de evidență în procesul scanării automate a elementelor infrastructurii, care permite efectuarea evaluării continue a riscurilor şi diminuarea acestora;
- asigurarea auditului independent.

Funcțiile de bază ale sistemului de monitorizare şi evaluare sînt următoarele:

- informațională – furnizarea datelor privind desfăşurarea procesului de prestare a serviciilor;
- analitică – analiza procesului de prestare a serviciilor pentru furnizarea informației administrative şi luarea deciziilor;

- de pronosticare – determinarea tendințelor şi pronosticurilor pentru planificarea procesului de gestionare a nivelului de deservire;
- de diagnosticare – determinarea factorilor care asigură stabilitatea şi fiabilitatea prestării serviciilor;
- de orientare – determinarea punctelor forte şi slabe ale procesului de prestare a serviciilor;
- profilactică – efectuarea auditului în scopul minimalizării impactului negativ asupra prestării serviciilor.

7.1.2. Componentele procesului de monitorizare

Procesul de monitorizare trebuie să includă indicatorii lucrului, raportarea sistematică şi la timp, care include parametrii eficienței prestării serviciilor, şi acțiunile imediate pentru reacționarea la solicitări.

Procesul de monitorizare trebuie să includă următoarele componente:

- metoda de abordare a monitorizării – stabileşte structura generală şi metoda de abordare a monitorizării care determină posibilitățile, metodologia şi procesul însoțit de evaluarea procesului de prestare a serviciilor;
- determinarea şi colectarea datelor de control – determinarea ansamblului de scopuri, compararea lor, identificarea datelor accesibile pentru măsurarea scopului;
- determinarea metodei de monitorizare – sînt folosite diferite metode de control, care iau în considerație scopurile şi scara de acoperire a procesului de prestare a serviciilor;
- evaluarea lucrărilor executate în procesul de prestare a serviciilor – revizuirea periodică a lucrărilor executate, analiza cauzelor devierilor de la scopurile stabilite, acțiunile de corectare pentru înlăturarea cauzelor de bază, precum şi efectuarea analizei încrucişate a cauzelor primare ale devierilor;
- gestionarea resurselor – controlul utilizării şi distribuirii resurselor în procesul de prestare a serviciilor prin intermediul evaluării sistematice a operațiunilor care efectuează distribuirea resurselor şi nivelarea obiectivelor strategice curente şi viitoare;
- gestionarea riscurilor – evaluarea sistematică a riscurilor şi influențelor legate de acestea;
- raportarea administrativă – se indică nivelul de realizare a obiectivelor planificate, resursele planificate şi utilizate, ansamblul de contraobiective şi determinarea lucrărilor de minimalizare a riscurilor;
- acțiunile de corectare – îndeplinirea acțiunilor de corectare bazate pe controlul şi evaluarea procesului de prestare a serviciilor. Controlul este efectuat prin intermediul urmăririi rezultatelor acțiunilor transmise, revizuirilor acestui proces, stabilirii persoanelor responsabile de corectare;
- efectuarea auditului intern sau extern pentru stabilirea corespunderii nivelului serviciilor prestate în baza standardelor şi procedurilor, metodelor general acceptate şi legislației.

Procesul de monitorizare trebuie să realizeze urmărirea permanentă a indicatorilor eficienței prestării serviciilor.

7.2. Procesele de gestionare şi audit al prestării serviciilor publice

Procesele de gestionare şi audit al prestării serviciilor sînt destinate controlului proceselor de prestare a serviciilor în organizație. Obiectivul acestor procese constă în crearea unui instrument eficient pentru clasificarea şi evaluarea proiectelor legate de prestarea serviciilor şi garantarea respectării calității la executarea comenzilor de prestare a serviciilor.

7.2.1. Analiza modelului de maturitate a proceselor de gestionare a TI

Analiza modelului de maturitate a proceselor de gestionare a TI este destinată pentru determinarea statutului şi stării procesului de gestionare a TI, precum şi pentru organizarea gestionării eficiente a TI şi SI. Nivelul modelului de maturitate a proceselor de gestionare a TI stabilesc modalitățile de control al corectitudinii realizării proceselor principale şi metodele de corectare a acestora.

În funcție de nivelul de dezvoltare şi maturitate al proceselor de gestionare a TI, trebuie determinată strategia şi tactica dezvoltării operaționale a funcțiilor şi componentelor infrastructurii TI.

Scara modelelor de maturitate trebuie să includă următoarele niveluri:

- nivelul zero – „Nu există” – nu există procese de gestionare a prestării serviciilor informaționale, precum şi nu există date despre probleme;
- nivelul unu – „De bază” – nu există o schemă exactă şi nici procedura de realizare a proceselor de gestionare a TI, există probleme în gestionarea prestării serviciilor publice şi necesitatea pricepută de a le soluționa;
- nivelul doi – „Repetat” – procesele de gestionare a TI sînt realizate într-o anumită dependență şi consecutivitate; probleme existente în gestionarea prestării serviciilor publice sînt examinate în vederea minimalizării lor;
- nivelul trei - „Formalizat” - procedura de realizare a proceselor de gestionare a TI este documentată şi este adusă la cunoştință; există o legătură urmărită în mod riguros între rezultat şi indicatorii productivității proceselor de prestare a serviciilor publice; sînt implementate procese de planificare şi monitorizare. Indicatorii productivității sînt fixați şi urmăriți în vederea sporirii eficienței întregii organizații;
- nivelul patru – „Gestionat” – toate procesele de gestionare a TI sînt supuse monitorizării; devierile sînt urmărite şi corectate; există o înțelegere deplină a problemelor de gestionare în prestarea serviciilor publice la toate nivelurile organizației; este efectuată instruirea permanentă a personalului. Determinarea şi menținerea în starea actuală a Acordului cu privire la nivelul de deservire, distribuirea responsabilității, determinarea nivelului de cunoaştere a proceselor sînt practici general acceptate;
- nivelul cinci – „De optimizare a proceselor de gestionare a TI” – cele mai bune practici de gestionare a TI sînt realizate în conformitate cu standardele şi în baza TI moderne; există o înțelegerea aprofundată a gestionării în prestarea serviciilor publice la toate nivelurile organizației. Instruirea şi comunicarea sînt susținute de cele mai moderne mijloace informațional-comunicaționale.

În gestionarea prestării serviciilor este necesar de aplicat următoarele concepții:

- factorii critici ai succesului;
- indicatorii principali ai scopului;
- indicatorii principali ai rezultatului.

7.2.2. Factorii critici ai succesului

Factorii critici ai succesului determină cele mai importante condiții, resurse şi acțiuni necesare pentru realizarea scopurilor şi sarcinilor proceselor TI. Aceşti factori trebuie să fie gestionați, orientați spre succes şi să descrie îndeplinirea acțiunilor strategice, tehnice, organizaționale sau procedurale necesare.

Factorii critici ai succesului sînt următorii:

- gestionarea procesului de prestare a serviciilor contribuie la realizarea scopurilor organizației: strategice, tactice, utilizarea tehnologiilor pentru dezvoltarea proceselor de prestare a serviciilor, suficiența resurselor şi satisfacerea cerințelor;
- determinarea, formalizarea şi realizarea acțiunilor de gestionare a procesului de prestare a serviciilor în baza cerințelor organizației clientului;
- elaborarea metodelor de gestionare pentru sporirea productivității, utilizarea optimă a resurselor şi sporirea eficienței proceselor;
- gestionarea riscurilor şi studierea deficiențelor acestora;
- determinarea gradului de conformitate cu standardele stabilite şi legislația în vigoare;

- efectuarea auditului pentru evitarea defecțiunilor şi erorilor în sistemul de control intern;
- standardizarea proceselor TI şi orientarea acestora spre realizarea cerințelor proceselor de gestionare a serviciilor publice;
- determinarea grupurilor utilizatorilor de procese TI şi a cerințelor acestora;
- asigurarea posibilității de stabilire a limitelor proceselor TI şi a gestionării optime a resurselor în cadrul acestor procese;
- existența procedurilor de control şi sporire a calității proceselor TI.

7.2.3. Indicatorii principali ai scopului

Indicatorii principali ai scopului determină complexul de măsurări care informează conducerea despre realizarea cerințelor înaintate.

Pentru indicatorii principali ai scopului trebuie să se evidențieze următoarele criterii informaționale:
- utilitatea informației necesare pentru susținerea procesului de prestare a serviciilor;
- riscurile lipsei integrității şi confidențialității;
- rentabilitatea proceselor şi operațiilor;
- confirmarea siguranței, eficienței şi concordanței procesului de prestare a serviciilor.

Trebuie evidențiați indicatorii de bază ai scopului:
- îmbunătățirea gestionării productivității şi costului de prestare a serviciilor;
- reducerea timpului pentru punerea în vînzare a unui serviciu nou;
- îmbunătățirea gestionării calității serviciilor;
- îmbunătățirea gestionării inovațiilor şi riscurilor;
- integrarea şi standardizarea proceselor de prestare a serviciilor publice;
- realizarea cerințelor şi aşteptărilor clientului conform Acordului cu privire la nivelul de deservire;
- corespunderea nivelului serviciilor prestate cu legislația în vigoare, instrucțiunile, standardele şi obligațiile contractuale.

7.2.4. Indicatorii principali ai eficienței prestării serviciilor publice

Indicatorii principali ai eficienței prestării serviciilor publice caracterizează şirul de acțiuni necesare pentru determinarea gradului de realizare a scopurilor stabilite, reflectarea corespunderii mijloacelor, metodelor şi abilităților folosite la prestarea serviciilor publice.

Indicatorii principali ai eficienței sînt:
- sporirea rentabilității proceselor TI;
- îmbunătățirea lucrului şi planificării acțiunilor de perfecționare a proceselor de prestare a serviciilor;
- creşterea sarcinii în infrastructura TI;
- sporirea gradului de satisfacție a utilizatorilor;
- sporirea productivității colaboratorilor.

Funcționarea optimă a procesului de gestionare şi auditare a prestării serviciilor trebuie să asigure şi să creeze următoarele avantaje:
- ridicarea nivelurilor de gestionare şi securitate a procesului de prestare a serviciilor;
- controlul proceselor de prestare a serviciilor;
- controlul realizării scopurilor de asigurare a calității serviciilor prestate;
- controlul rezultatelor fiecărui proces TI;
- urmărirea şi perfecționarea procesului de prestare a serviciilor;
- utilizarea optimă a resurselor.

7.2.5. Efectuarea auditului post-implementare

Efectuarea auditului post-implementare al sistemului de prestare a serviciilor publice este

necesară pentru obținerea operativă a informației sistematizate şi veridice pentru evaluarea calității, posibilităților serviciilor informaționale prestate şi corespunderii acestora cu cerințele prezentate în capitolele 4 şi 5.

Auditul post-implementare al sistemului de prestare a serviciilor publice trebuie efectuat de către auditori externi, prin intermediul următoarelor tipuri de audit:

- examinarea sistemului – colectarea informației pentru utilizarea acesteia în efectuarea lucrărilor ulterioare;
- evaluarea de către experți a sistemului – evaluarea corespunderii finanțării deciziilor şi/sau investițiilor de proiect în sistemul de prestare a serviciilor publice, evaluarea exploatării sistemului şi pregătirii utilizatorilor, evaluarea posibilității de reprofilare a infrastructurii TI;
- auditul TI operațional al sistemului – colectarea, analiza informației şi oferirea recomandărilor privind îmbunătățirea funcționării atît a unor elemente separate de evidență, cît şi a întregii infrastructuri TI;
- auditul proceselor – auditul TI şi SI critice pentru procesul de prestare a serviciilor publice în baza criteriilor de calitate şi eficiență stabilite;
- auditul criteriului procesului de prestare a serviciilor – colectarea, analiza informației şi prezentarea recomandărilor privind criteriul selectat al procesului de prestare a serviciilor, spre exemplu, securitatea, productivitatea, siguranța, accesibilitatea. La efectuarea auditului în baza unui anumit criteriu de evaluare, este examinat nu doar un element separat al infrastructurii TI, ci totalitatea mijloacelor software, hardware, a proceselor de mentenanță şi deservire a acestora;
- auditul complex al sistemului – este efectuată determinarea şi analiza interconexiunilor proceselor de prestare a serviciilor publice, a cerințelor acestora, a tehnologiilor informaționale şi conexe, a totalității mijloacelor software şi hardware.

Rezultatele efectuării auditului post-implementare al sistemului de prestare a serviciilor publice sînt următoarele:

- determinarea corespunderii posibilităților funcționale ale sistemului de prestare a serviciilor şi necesităților participanților la interacțiune pentru fiecare serviciu public în parte;
- confirmarea formalizării adecvate a regulilor şi cerințelor de organizare a interacțiunii participanților pentru fiecare serviciu public, descrierea proceselor principale de prestare a serviciilor şi crearea hărții fluxurilor informaționale;
- confirmarea existenței documentației tehnice corespunzătoare în care sînt descrise caracteristicile tehnice, infrastructura TI şi particularitățile arhitecturale ale structurii SI de prestare a serviciilor publice;
- determinarea raționalității utilizării, dezvoltării sau înlocuirii pe viitor a SI de prestare a serviciilor publice;
- determinarea listei riscurilor identificate, legate de utilizarea sistemului de prestare a serviciilor publice;
- elaborarea unor recomandări concrete, orientate spre îmbunătățirea calității prestării serviciilor şi optimizarea procesului de prestare a serviciilor;
- propunerea direcțiilor de reducere a cheltuielilor pentru susținerea şi dezvoltarea sistemului de prestare a serviciilor publice;
- propunerea direcțiilor de reducere a riscurilor apărute în urma situațiilor excepționale la prestarea serviciilor;
- depistarea neajunsurilor şi lacunelor în sistemul de prestare a serviciilor;
- elaborarea propunerilor privind perfecționarea calificării angajaților care participă la prestarea serviciilor, procurarea sau modernizarea mijloacelor software şi hardware;
- acceptarea recomandărilor privind asigurarea continuității în funcționarea SI de prestare a

serviciilor publice.

7.3. Gestionarea eficienței prestării serviciilor publice

Gestionarea optimă a procesului de prestare a serviciilor publice contribuie la utilizarea cît mai eficientă a informației.

Procesul de prestare a serviciilor trebuie să corespundă cerințelor organizaționale din perspectiva confidențialității, integrității, accesibilității, eficienței, economicității şi fiabilității.

7.3.1. Resursele procesului de prestare a serviciilor publice

Pentru a asigura funcționarea sigură şi eficientă a sistemului de prestare a serviciilor publice, este necesar de a folosi următoarele resurse:

- resursele umane – angajații organizației cu abilitățile şi experiența necesare pentru planificarea, organizarea, completarea, mentenanța, susținerea şi monitorizarea sistemului de prestare a serviciilor publice;
- aplicațiile – software-ul aplicativ utilizat în lucrul cu sistemul de prestare a serviciilor publice;
- tehnologiile – sistemele operaționale, bazele de date, sistemele de gestionare etc, care permit realizarea procesului de prestare a serviciilor publice;
- echipamentul – toate mijloacele de echipament ale SI, cu luarea în considerație a deservirii lor;
- datele – datele externe şi interne, structurate şi nestructurate, grafice, sonore şi multimedia.

7.3.2. Cerințele față de prestarea serviciilor publice

În procesul de prestare a serviciilor publice este necesar de îndeplinit următoarele cerințe:

- cerințele față de calitatea şi fiabilitatea deservirii;
- continuitatea procesului de prestare a serviciilor – pregătirea şi planificarea mijloacelor de lichidare a situațiilor excepționale;
- cerințele de încredere – eficiența şi productivitatea operațiilor, fiabilitatea informației; conformitate cu documentele normative;
- cerințele de securitate – confidențialitatea; integritatea; accesibilitatea, imposibilitatea de refuz;
- informarea despre procesul de prestare a serviciilor, furnizarea documentației corespunzătoare;
- productivitatea procesului de prestare a serviciilor – furnizarea informației prin utilizarea optimă a resurselor;
- confidențialitatea – protecția informației contra dezvăluirii nesancționate;
- accesibilitatea – posibilitatea obținerii informației necesare în decursul unei anumite perioade de timp, protecția informației şi a purtătorilor acesteia contra furtului sau distrugerii;
- cerințele față de resursele exploatationale de bază;
- cerințele tehnico-exploatationale față de locurile de muncă;
- cerințele tehnico-exploatationale pentru organizarea serviciilor de informații şi de deservire;
- cerințele față de deservirea tehnică;
- cerințele față de informație – veridicitatea, plenitudinea, caracterul concret, operativitatea informației furnizate, precum şi comoditatea şi accesibilitatea obținerii acesteia.

7.3.3. Criteriile de evaluare a eficienței procesului de prestare a serviciilor

Criteriile eficienței procesului de prestare a serviciilor publice se bazează pe evaluarea resurselor informaționale şi a tuturor componentelor infrastructurii TI.

În procesul de prestare a serviciilor publice trebuie de evaluat indicatorii care contribuie la realizarea procesului gestionat şi măsurat de prestare a serviciilor publice şi care caracterizează următoarele:

- conformitatea procesului de prestare a serviciilor publice cu standardele şi cerințele adoptate;
- autenticitatea informației prelucrate şi eficacitatea acesteia;
- securitatea informațională – confidențialitatea, integritatea, accesibilitatea, imposibilitatea de refuz;

- calitatea şi costul prelucrării informației, precum şi descrierii furnizării acesteia către destinatar.

Criteriile eficienței realizării procesului de prestare a serviciilor publice, care se bazează pe evaluarea resurselor şi componentelor infrastructurii TI utilizate, trebuie să fie următoarele:

- eficiența –actualitatea, caracterul adecvat şi corespunderea informației cu sarcinile organizației, precum şi oportunitatea prezentării acesteia, corectitudinea, caracterul necontradictoriu şi aplicabilitatea;
- conformitatea — criteriul conformității cu cerințele legilor, standardelor, instrucțiunilor, dispozițiilor şi acordurilor care reglementează organizarea procesului de prestare a serviciilor publice;
- confidențialitatea – protecția informației contra divulgării nesancționate;
- integritatea — exactitatea, caracterul complet şi plenitudinea informației, precum şi argumentarea acesteia din punct de vedere al valorilor şi aşteptărilor organizării;
- accesibilitatea – nivelul de accesibilitate necesar în prezent şi viitor al accesibilității informației pentru realizarea proceselor în cadrul organizației, posibilitatea obținerii informației necesare în perioada de timp determinată de cerințele proceselor interne din cadrul organizației;
- productivitatea – furnizarea informației prin intermediul utilizării optime (productive şi economе) a resurselor şi componentelor infrastructurii TI, respectarea cerințelor stipulate în legi, instrucțiuni şi înțelegeri ce influențează asupra realizării proceselor în cadrul organizației.

Anexa nr. 3
la Ordinul nr. 94
din 17.09.2009

REGLEMENTARE TEHNICĂ
Asigurarea securității informaționale la prestarea serviciilor publice electronice.
Cerințe tehnice

1. Domeniu de aplicare

Prezenta reglementare tehnică a fost elaborată ca parte componentă a bazei legislative pentru reglementare în domeniul tehnologiilor infocomunicaționale, susținerea strategiei naționale de creare a societății informaționale, precum şi pentru implementarea tehnologiilor infocomunicaționale în toate domeniile de interacțiune între stat, afaceri şi societate.

În prezenta reglementare tehnică sînt stabilite cerințele de bază a procesului de prestare a serviciilor publice electronice (în continuare - servicii publice) privind asigurarea securității resurselor informaționale, sistemelor informaționale (SI) şi de evaluare a conformității cu aceste cerințe şi sînt determinate toate cerințele ce sînt necesare a fi realizate pentru organizarea şi susținerea procesului de management al securității informației în procesul de prestare a serviciilor publice.

Scopul prezentei reglementări tehnice constă în descrierea metodologiilor, metodelor şi mijloacelor de asigurare a securității în procesul de prestare a serviciilor publice în spațiul informațional al Republicii Moldova, precum şi îndeplinirea cerințelor de securitate stabilite în acordurile cu beneficiarii şi utilizatorii serviciilor şi în legislația în vigoare a Republicii Moldova, şi în asigurarea nivelului minim adoptat de asigurare a securității informaționale în procesul prestării serviciilor publice.

Asigurarea securității informaționale a procesului de prestare a serviciilor publice în Republica Moldova este o parte componentă a politicii de stat în formarea societății informaționale, în ridicarea eficienței autorităților administrației publice şi în asigurarea nivelului înalt al calității pentru sistemul de prestare a serviciilor publice.

Prezenta reglementare tehnică se aplică în scopul managementului şi asigurării securității

resurselor şi sistemelor informaţionale, mijloacelor hardware şi software, precum şi a mijloacelor de telecomunicaţii care participă în procesul de prestare a serviciilor publice, încălcarea securităţii cărora poate duce la cauzarea unui prejudiciu esenţial utilizatorilor de servicii publice, societăţii şi statului.

2. Baza juridico-normativă

Prezenta reglementare tehnică este elaborată în baza următoarelor acte legislative ale Republicii Moldova:

- Legea Republicii Moldova „Privind accesul la informaţie" nr. 982-XIV din 11.05.2000;
- Legea Republicii Moldova „Cu privire la evaluarea conformităţii produselor" nr. 186 din 24.04.2003;
- Legea Republicii Moldova „Cu privire la informatizare şi la resursele informaţionale de stat" nr. 467-XV din 21.11.2003;
- Legea Republicii Moldova „Cu privire la documentul electronic şi semnătura digitală" nr. 264-XV din 15.07.2004;
- Legea Republicii Moldova „Privind comerţul electronic" nr. 284-XV din 22.07.2004;
- Legea Republicii Moldova „Privind activitatea de reglementare tehnică" nr. 420-XVI din 22.12.2006;
- Legea Republicii Moldova „Cu privire la protecţia datelor cu caracter personal" nr. 17-XVI din 15.02.2007;
- Legea Republicii Moldova „Cu privire la registre" nr. 71-XVI din 22.03.2007;
- Legea Republicii Moldova „Cu privire la secretul de stat" nr. 245 din 27.11.2008.

3. Terminologie

În prezenta reglementare sînt utilizaţi următorii termeni:

Acces autorizat la informaţie - accesul la informaţie ce nu încalcă regulile cu privire la delimitarea accesului.

Acces neautorizat - obţinerea de către persoana interesată a informaţiei protejate cu încălcarea actelor normative stabilite sau de către proprietarul informaţiei cu încălcarea drepturilor sau regulilor de acces la informaţia protejată.

Acord cu privire la nivelul de deservire – acord încheiat în formă scrisă între furnizorul de servicii şi solicitant (solicitanţi), în care sînt descrise nivelurile convenite de deservire cu privire la un serviciu anumit.

Algoritm - recomandare exactă cu privire la succesivitatea determinată a acţiunilor pentru atingerea scopului propus prin efectuarea paşilor concreţi.

Algoritmele cifrării asimetrice - algoritmele cifrării în care pentru cifrare şi descifrare sînt utilizate două chei diferite ce se numesc respectiv publică şi privată (cunoaşterea uneia din aceste chei nu face posibilă descoperirea celeilalte chei).

Algoritmele cifrării simetrice - algoritmele cifrării în care pentru cifrare şi descifrare este utilizată una şi aceeaşi cheie sau cheia descifrării poate fi uşor obţinută din cheia cifrării.

Algoritm criptografic - algoritmul transformării datelor complet sau parţial secrete şi care utilizează un set de parametri secreţi în procesul de lucru.

Arhitectura sistemului informaţional - un set de decizii cheie în organizarea sistemului informaţional precum şi un set de elemente şi interfeţe structurale din care constă acest sistem, împreună cu comportamentul descris în noţiunile de cooperare a acestor elemente.

Atestarea - forma evaluării conformităţii procesului de exploatare a sistemului informaţional cu cerinţele securităţii.

Autenticitate - calitate a datelor de a fi autentice care constă în faptul că datele au fost create de participanţi legali la procesul informaţional, iar datele nu au fost supuse unor denaturări ocazionale

sau intenționate.

Cerințe de securitate - cerințe înaintate față de tehnologiile informaționale, realizarea cărora asigură confidențialitatea, integritatea şi disponibilitatea informației.

Cheie criptografică - parametru utilizat de algoritmul criptografic.

Cifrare - proces de transformare a datelor publice în date cifrate cu ajutorul codului (cifrului).

Confidențialitate - asigurarea accesului la informație doar pentru utilizatorii autorizați.

Configurație - totalitatea obiectelor sistemului informațional.

Descifrare - proces de transformare a datelor cifrate în date deschise cu ajutorul cifrului.

Disponibilitate - asigurarea accesului la informație şi la resursele legate de aceasta pentru utilizatorii autorizați, în măsura necesității.

Ecranare - mijloc de delimitare a accesului clienților dintr-o multitudine la serverele din altă multitudine în vederea controlării fluxurilor informaționale.

Evaluarea riscurilor - evaluarea pericolelor, consecințelor acestora, a vulnerabilității informației şi a mijloacelor de procesare a informației, precum şi a probabilității de survenire a acestora.

Gestionarea discretă (selectivă) a accesului - delimitarea accesului între persoane şi obiectele nominalizate. Persoana cu un anumit drept de acces poate transmite acest drept oricărei alte persoane.

Hardware - echipament utilizat pentru introducerea, procesarea şi scoaterea datelor în sistemele informaționale.

Incident - un eveniment sau o succesiune de evenimente nedorite sau inopinate în sistemul de protecție a informației capabile într-o mare măsură să compromită operațiile standard şi să pună în pericol protecția informației.

Infrastructură bazată pe chei publice - totalitate de mijloace hardware şi software, politici, proceduri şi obligațiuni legale care asigură implementarea şi funcționarea sistemelor criptografice de chei publice bazate pe certificatele de asigurare a securității mesajelor (confidențialitate, integritate, autenticitate, negare) din ambele direcții.

Infrastructura TI – totalitate de centre informaționale de calcul, de bănci de date şi de cunoştințe din sistemul automatizat integrat de telecomunicații şi de organizare care asigură utilizatorilor condiții generale de acces la informația păstrată.

Integritate - păstrarea acurateței şi completitudinii informațiilor, precum şi metodelor de procesare.

Managementul accesului prin mandat este bazată pe compararea mențiunilor privind confidențialitatea informației ce se conține în obiecte (fişiere, mape, desene) şi accesul oficial al persoanei la informația cu nivelul confidențial corespunzător.

Mediul funcționării - mediul în care funcționează sistemul informațional.

Mențiunea privind sensibilitatea - anumite marcaje ale resurselor şi sistemelor informaționale, cum sînt de exemplu, gradul de secretizare, categoriile.

Mijloace de asigurare a securității - mijloace hardware şi software care realizează ansamblul de funcții ce asigură îndeplinirea cerințelor privind protecția informației şi controlul eficienței protecției informației.

Mijloc de gestionare a configurațiilor - produs software
ce asigură menținerea automatizată a modificărilor, configurațiilor şi controlului versiunilor.

Mijloc de protecție criptografică a informației - mijloace hardware şi software, sisteme şi complexe ce
realizează algoritmele transformării criptografice a informației utilizate în scopul protejării integrității şi confidențialității informației.

Modul criptografic - ansamblul de software şi hardware sau o anumită combinare a acestora,

care realizează logica criptografică sau procesele de protecție, inclusiv algoritmele criptografice sau generarea cheilor, şi care se conține în interiorul unui anumit volum fizic.

Monitorizare - proces de colectare şi analiză a datelor, de prezentare a rapoartelor cu privire la executarea lucrărilor.

Negare - imposibilitatea de a anula acțiunile executate.

Pachet de autentificare - mecanism de confirmare a autenticității identificatorului declarat al utilizatorului.

Parafă de secretizare - mențiune aplicată pe purtătorul material de informații atribuite la secret de stat şi/sau indicată în documentația de însoțire a acestuia, care atestă gradul de secretizare a informațiilor conținute de purtător.

Pericol - totalitatea evenimentelor şi acțiunilor potențial posibile, a căror producere cauzează prejudicii resurselor informaționale sau infrastructurii informaționale.

Prestarea serviciilor publice – ansamblu de procese interconexe orientate spre realizarea scopurilor – interacțiunea dintre subiecții guvernării electronice care se desfăşoară pe două circuite distincte - conturul intern şi conturul extern, care comunică între ele prin intermediul portalului guvernamental.

Politica de management a accesului - reguli de acordare a accesului la sistemele şi rețelele computerizate pentru anumiți utilizatori.

Politica de securitate a informației - un set de reguli şi proceduri recomandate instituției pentru protecția datelor sensibile.

Profilul protecției - document cu o structură riguroasă, în care sînt prevăzute cerințele securității pentru o anumită clasă de mijloace software.

Proprietarul resurselor şi sistemelor informaționale, al tehnologiilor şi mijloacelor de asigurare a acestora - subiectul care exercită dreptul de posesiune, folosință şi dispoziție asupra obiectelor indicate şi realizează împuternicirile de administrare în limitele stabilite de legislația în vigoare.

Protecția datelor - totalitate de activități tehnico-organizaționale, de mijloace software şi hardware şi acte normative, utilizate pentru păstrarea confidențialității, integrității şi accesibilității informației, precum şi pentru asigurarea negării.

Protecție criptografică - protecția proceselor informaționale împotriva tentativelor orientate spre abaterea proceselor informaționale de la condițiile normale de desfăşurare.

Risc - influențare interioară sau exterioară asupra sistemului, care poate să acționeze negativ asupra domeniului proiectului sau poate să ducă la eşuarea acestuia.

Resursă – totalitate a bunurilor care aparțin unei întreprinderi sau instituții (resursele informaționale, tehnice, software şi alte resurse care intră în componența sistemelor informaționale).

Securitatea sistemelor informaționale - stare a sistemelor informaționale ce asigură utilizarea securității la obiectele exploatate la care lipseşte riscul inadmisibil legat de cauzarea prejudiciului persoanei, societății şi statului.

Serviciu public – serviciu care generează trei tipuri de interacțiuni între părțile componente ale guvernării electronice: interacțiunea „Guvern - Cetățean” (G2C); interacțiunea „Guvern – Business” (G2B); interacțiunea „Guvern – Guvern” (G2G) cu subcategoria interacțiunea dintre Guvern şi angajații acestuia (G2E).

Sistem informațional - totalitate de mijloace software şi hardware destinate colectării, procesării, păstrării şi furnizării informației şi resurselor informaționale în vederea susținerii procesului de adoptare a deciziilor, gestionare şi sporire a transparenței în cadrul organizației.

Software - totalitatea programelor sistemului de procesare a informației şi a documentelor de program, necesare pentru exploatarea acestor programe.

Tunelare - utilizarea unui protocol special cu ajutorul căruia două oficii la distanță organizează între ele un tunel (şedință de legătură) sigur, în rezultatul căruia datele se transmit între rețele.

Vulnerabilitate - punctul slab din sistem, a cărui utilizare poate provoca funcționarea neadecvată a sistemului.

4. Scopurile, sarcinile şi principiile de management al securității în procesul de prestare a serviciilor publice

Asigurarea securității informaționale este un proces continuu care constă în fundamentarea şi realizarea celor mai raționale forme, metode, procedee şi căi de formare, perfecționare şi dezvoltare a sistemelor de securitate, în administrarea neîntreruptă, controlul, depistarea zonelor limitate şi vulnerabile, precum şi a pericolelor potențiale.

Securitatea informațională reprezintă starea de protecție a informației şi infrastructurii de susținere la toate etapele proceselor de creare, procesare, transmitere şi protecție împotriva unor acțiuni ocazionale sau intenționate, cu caracter natural sau artificial, care pot cauza prejudicii procesului de prestare a serviciilor publice.

Securitatea informațională trebuie să fie asigurată prin intermediul utilizării complexe a tuturor mijloacelor de protecție pentru toate elementele de structură ale sistemului şi componentele infrastructurii TI şi la toate etapele ciclului tehnologic ale activității acestuia. Pentru a atinge nivelul optim al managementului securității informaționale este necesar de utilizat toate mijloacele, metodele şi activitățile în calitate de mecanism integru unic.

Sistemul securității informaționale reprezintă un ansamblu organizat de măsuri, mijloace, metode şi activități legislative, organizaționale şi economice ce asigură securitatea informațională.

Scopul sistemului securității informaționale în procesul de prestare a serviciilor publice constă în prevenirea divulgării, pierderii, scurgerii, denaturării şi distrugerii informației, dereglării activității sistemului de prestare a serviciilor publice.

Subiectul protecției în procesul de prestare a serviciilor publice îl constituie resursele informaționale şi SI, inclusiv şi cele cu acces limitat, ce constituie secret de serviciu şi de stat, amplasate pe bază magnetică şi/sau optică, masivele informaționale şi bazele de date, software-ul, cîmpurile fizice informative de natură diferită.

Obiectul protecției prestării serviciilor publice sînt mijloacele şi sistemele de informatizare (sistemele automatizate şi rețelele de calcul de diferite niveluri şi destinații, liniile de telecomunicații, mijloacele tehnice de transmitere a informației, mijloacele de multiplicare şi reflectare a informației, mijloacele şi sistemele tehnice auxiliare), mijloacele tehnice şi sistemele de pază şi protecție a resurselor şi sistemelor informaționale.

Securitatea resurselor informaționale şi a SI caracterizează o stare a resurselor informaționale şi a SI care susține infrastructura acestora, în cadrul căreia trebuie asigurată, cu probabilitatea necesară, protecția informației în procesul de prestare a serviciilor împotriva scurgerii, acțiunilor neautorizate şi nepremeditate.

Asigurarea securității informaționale reprezintă o abordare multidimensională pentru instituția ce prestează servicii publice. Asigurarea securității informaționale trebuie să fie realizată în cadrul a patru nivele:

- nivelul legislativ (legi, acte normative, standarde);
- nivelul administrativ (acțiuni cu caracter general întreprinse de conducere);
- nivelul procedural (măsuri concrete de securitate care implică nemijlocit populația);
- nivelul tehnic (măsuri tehnice concrete).

În procesul prestării serviciilor publice pentru asigurarea securității resurselor informaționale este necesar de asigurat cel puțin trei aspecte ale securității:

- confidențialitate – asigurarea accesibilității informației numai celor autorizați să aibă acces;

- integritate – păstrarea acurateței şi completitudinii informațiilor, precum şi metodelor de procesare;
- disponibilitate – asigurarea faptului că utilizatorii autorizați au acces la informație, precum şi la resursele asociate, atunci cînd este necesar.

4.1. Scopurile asigurării securității informaționale

Scopurile asigurării securității informaționale în procesul prestării serviciilor constau în asigurarea integrității şi confidențialității informației, protecția şi garantarea disponibilității, veridicității şi integrității informației, evitarea scurgerii de informație, minimalizarea prejudiciilor cauzate de evenimentele care reprezintă un pericol pentru securitatea informațională.

Pentru a asigura securitatea informațională în procesul de prestare a serviciilor publice este necesar de realizat următoarele scopuri:

- asigurarea confidențialității informației în conformitate cu clasificarea realizată;
- asigurarea integrității informației la toate etapele şi a proceselor aferente acesteia (crearea, procesarea, păstrarea, transmiterea şi distrugerea) în procesul de prestare a serviciilor publice;
- asigurarea oportună a disponibilității informației în procesul de prestare a serviciilor publice;
- asigurarea supravegherii, orientate spre înregistrarea oricărei activități a utilizatorilor şi proceselor;
- asigurarea autenticității şi negării al tranzacțiilor şi acțiunilor întreprinse de participanții la procesul de prestare a serviciilor publice;
- evidența tuturor proceselor şi evenimentelor privind introducerea, procesarea, păstrarea, furnizarea şi distrugerea informației.

4.2. Sarcinile sistemului securității informaționale

Pentru a realiza scopurile asigurării securității în procesul de prestare a serviciilor publice este necesar de îndeplinit următoarele sarcini:

- identificarea resurselor şi sistemelor informaționale şi clasificarea acestora în funcție de valoarea şi importanța acestora în procesul de prestare a serviciilor publice (componentele analizei trebuie să includă date, aplicații, tehnologii, mijloace de telecomunicații şi hardware, încăperi, resurse umane etc.);
- identificarea pericolelor securității informaționale şi determinarea surselor potențiale de pericole pentru fiecare resursă şi sistem informațional;
- identificarea punctelor vulnerabile pentru fiecare pericol identificat;
- evaluarea riscurilor pentru resursele şi sistemele informaționale identificate;
- selectarea activităților de management a securității informaționale în baza analizei corelației dintre costul realizării lor, pe de o parte, şi efectul diminuării riscurilor şi prejudiciile potențiale în caz de încălcare a securității, pe de altă parte;
- elaborarea şi implementarea mecanismelor şi măsurilor de reacționare operativă la pericolele securității informaționale şi manifestarea tendințelor negative în funcționarea resurselor şi sistemelor informaționale de prestare a serviciilor publice;
- elaborarea şi implementarea sistemului de controale care să permită funcționarea eficientă a mecanismului şi a măsurilor de asigurare a securității;
- organizarea procesului de reprimare eficientă a atentatelor asupra resurselor si sistemelor informaționale;
- organizarea procesului de asigurare a continuității prestării serviciilor şi crearea condițiilor pentru compensarea maximal posibilă şi localizarea prejudiciului cauzat prin intermediul acțiunilor nelegitime cauzate de persoane fizice şi juridice, diminuarea impactului negativ al efectelor încălcării securității informaționale;
- organizarea procesului de asigurare a securității în caz de existență a furnizorilor de servicii care

au acces la resursele şi sistemele informaţionale în procesul de prestare a serviciilor publice.

4.3. Principiile de asigurare a securităţii informaţionale

Sistemul de asigurare a securităţii informaţionale în procesul de prestare a serviciilor publice trebuie să fie creat pe următoarele principii:

- principiul echirezistenţei – prevede asigurarea protecţiei echipamentului, software-ului şi sistemelor de administrare împotriva tuturor tipurilor de pericole;
- principiul continuităţii – prevede asigurarea continuă a securităţii resurselor informaţionale, SI pentru prestarea continuă a serviciilor publice;
- principiul suficienţei rezonabile – prevede aplicarea unor măsuri şi mijloace de protecţie rezonabile, raţionale şi care implică cheltuieli ce nu depăşesc costul încălcărilor securităţii informaţionale;
- principiul complexităţii - pentru asigurarea securităţii cu ajutorul întregii diversităţi de elemente de structură, pericole şi canale de acces neautorizat trebuie aplicate toate tipurile şi formele de protecţie în volum deplin (este inadmisibilă utilizarea unor forme sau mijloace tehnice separate);
- principiul controlului complex - efectuarea cercetărilor şi controalelor speciale, analizei inginereşti speciale a echipamentului, cercetărilor de verificare a software-ului, este necesar de realizat monitorizarea continuă a mesajelor de avarie şi a parametrilor erorilor, este necesar de efectuat testarea permanentă a hardware-ului şi software-ului precum şi controlul integrităţii mijloacelor software atît în procesul încărcării mijloacelor software, cît şi în procesul de funcţionare a acestora;
- principiul fiabilităţii - metodele, mijloacele şi formele de protecţie trebuie să asigure blocarea sigură a tuturor căilor de pătrundere şi a canalelor eventuale de scurgere a informaţiei, în acest scop, este permisă dublarea mijloacelor şi măsurilor de securitate;
- principiul universalităţii - măsurile de securitate trebuie să blocheze căile de pericol indiferent de locul acţiunii lor posibile;
- principiul planificării - planificarea trebuie să se efectueze prin elaborarea detaliată a planurilor de acţiuni cu privire la asigurarea protecţiei informaţionale a tuturor componentelor sistemului de prestare a serviciilor publice;
- principiul managementului centralizat - în cadrul unei structuri determinate trebuie asigurată autonomia organizatorico-funcţională a procesului de asigurare a securităţii în procesul de prestare a serviciilor publice;
- principiul orientării spre realizarea scopului - este necesar de protejat ceea ce trebuie să fie protejat în interesul unui scop anumit;
- principiul activităţii - măsurile de protecţie pentru asigurarea securităţii activităţii procesului de prestare a serviciilor trebuie să fie realizate cu un grad de insistenţă suficientă;
- principiul calificării personalului de deservire - echipamentul trebuie să fie deservit de colaboratori instruiţi nu numai în probleme de exploatare tehnică, dar şi în problemele tehnice privind asigurarea securităţii informaţiei;
- principiul responsabilităţii - responsabilitatea pentru asigurarea securităţii informaţionale trebuie stabilită într-un mod clar, transmisă personalului corespunzător şi aprobată de toţi participanţii la procesul de asigurare a securităţi informaţionale.

5. Metodologia managementului securităţii informaţiei în procesul de prestare a serviciilor publice

Metodologia managementului securităţii informaţiei în procesul de prestare a serviciilor publice cuprinde următoarele etape:

- elaborarea şi menţinerea politicii de securitate a informaţiei;
- managementul riscurilor;

- securitate organizațională;
- clasificarea resurselor şi organizarea mediului de control;
- securitatea personalului;
- securitatea fizică;
- managementul comunicațiilor şi activității operaționale a tehnologiilor informaționale (TI);
- controlul accesului;
- elaborarea şi mentenanța SI;
- managementul continuității activității;
- conformitatea;
- managementul securității informației la atragerea organizațiilor terțe.

5.1. Elaborarea şi menținerea politicii de securitate a informației

Scopul politicii de securitate a informației constă în asigurarea soluționării problemelor de securitate a informației şi implicarea conducerii de vîrf în procesul respectiv.

Politica de securitate a informației reprezintă cel mai important document în sistemul de management al securității instituției şi este unul din mecanismele cheie ale securității, în baza căruia urmează să fie edificat întregul sistem de măsuri şi mijloace de asigurare a securității în procesul de prestare a serviciilor publice.

În procesul de elaborare şi menținere a politicii de securitate a informației este necesar de respectat următoarele cerințe:

- politica de securitate a informației instituției trebuie să fie elaborată şi realizată de conducerea de vîrf prin determinarea unei poziții clare în soluționarea problemelor de securitate;
- politica de securitate a informației trebuie să stabilească responsabilitatea conducerii, precum şi să specifice metoda de abordare a managementului securității de către instituție;
- politica de securitate a informației trebuie să includă în mod obligatoriu următoarele:

1) determinarea securității, scopurilor şi sferei sale de acțiune, precum şi dezvăluirea importanței securității în calitate de instrument de asigurare a posibilității de utilizare în comun a informației;

2) specificarea scopurilor şi principiilor securității formulate de conducere;

3) specificarea succintă a politicilor de securitate a informației, a principiilor, regulilor şi cerințelor celor mai importante pentru instituție;

4) determinarea obligațiilor generale şi concrete ale colaboratorilor în cadrul managementului securității, inclusiv informarea privind incidentele de încălcare a securității;

5) referințele la documentele ce completează politica de securitate a informației, de exemplu politicile şi procedurile mai detaliate ale securității pentru SI concrete, precum şi regulile de securitate care trebuie respectate de către utilizatori;

- politica de securitate a informației trebuie să fie aprobată, emisă şi adusă la cunoştința tuturor colaboratorilor instituției în modul corespunzător în formă accesibilă şi comprehensibilă;
- este necesar de desemnat persoana responsabilă de politica de securitate a informației, care să fie responsabilă de realizarea şi revizuirea politicii cel puțin o dată în an;
- revizuirile periodice trebuie să includă:

1) verificarea eficienței politicii, reieşind din natura, numărul şi consecințele incidentelor de încălcare a securității înregistrate;

2) determinarea costului activităților de management a securității şi influența acestora asupra eficienței executării proceselor;

3) evaluarea impactului modificărilor în TI.

O politică de securitate a informației eficientă trebuie să stabilească un set necesar şi suficient de cerințe ale securității, care să permită diminuarea riscurilor securității pînă la un nivel acceptabil. Cerințele respective trebuie să fie stabilite în funcție de particularitățile proceselor din cadrul

instituției ce prestează servicii publice, trebuie să fie susținute de conducere, să fie asimilate pozitiv şi îndeplinite de colaboratorii instituției.

În planul de asigurare a securității sînt stabilite toate acțiunile privind realizarea scopurilor asigurării securității, implementarea complexului de hardware şi software şi sînt determinate procedurile de perfecționare a procesului de asigurare a securității, de desfăşurare a instructajelor şi seminarelor de instruire şi ridicare a nivelului de informare a personalului.

Cerințele privind planul de asigurare a securității în procesul de prestare a serviciilor publice trebuie să includă următoarele:

- cerințe privind planul de asigurare a securității:

1) este necesar de elaborat şi de realizat planul de asigurare a securității în procesul de prestare a serviciilor;

2) planul de asigurare a securității trebuie să conțină o prezentare succintă a cerințelor de securitate la prestarea serviciilor şi o descriere a măsurilor şi mijloacelor de asigurare a securității aplicate sau planificate pentru a fi implementate în vederea îndeplinirii cerințelor respective;

3) planul de asigurare a securității trebuie să fie examinat şi aprobat de persoanele cu funcții de răspundere corespunzătoare;

4) planul de asigurare a securității trebuie să fie revizuit şi corectat periodic, luîndu-se în considerație modificările în sistemul de prestare a serviciilor publice sau problemele apărute în procesul realizării acestuia, şi evaluarea eficienței măsurilor şi mijloacelor de asigurare a securității;

- cerințe privind regulile de comportare a personalului care participă la procesul de prestare a serviciilor publice:

1) este necesar de stabilit regulile de comportament al personalului cu privire la asigurare securității;

2) regulile de comportament trebuie să caracterizeze obligațiile personalului şi acțiunile aşteptate din partea acestuia în privința asigurării securității;

3) trebuie depusă, din partea fiecărui specialist, o confirmare în scris a faptului că acesta a luat cunoştință şi este de acord să respecte regulile de comportament stabilite.

5.2. Managementul riscurilor

Managementul riscurilor reprezintă un proces de identificare, control şi minimalizare sau eliminare a riscurilor securității care influențează asupra resurselor şi sistemelor informaționale ce participă la procesul de prestare a serviciilor publice, în limitele unor cheltuieli admisibile.

Managementul riscurilor trebuie să includă următoarele etape:

- determinarea domeniului şi limitelor procesului de management al riscurilor;
- analiza şi evaluarea riscurilor;
- selectarea şi implementarea măsurilor şi mijloacelor de minimalizare a riscurilor;
- monitorizarea procesului de gestionare a riscurilor şi a eficienței activităților selectate pentru reducerea riscului.

Managementul riscurilor trebuie să corespundă următoarelor cerințe:

- este necesar de elaborat, de documentat şi de actualizat periodic politica de management al riscurilor, precum şi procedurile şi măsurile legate de realizare a acestei politici;
- este necesar de evaluat riscurile şi prejudiciul potențial care poate fi cauzat în rezultatul accesului neautorizat, utilizării, divulgării, modificării sau distrugerii resurselor şi sistemelor informaționale;
- este necesar de reevaluat riscurile la anumite intervale stabilite sau după introducerea unor modificări esențiale în cadrul sistemului informațional de prestare a serviciilor publice;
- cerințele privind cercetarea pericolelor şi vulnerabilităților:

1) este necesar de identificat pericolele şi vulnerabilitățile noi la intervale stabilite;

2) cercetarea pericolelor şi vulnerabilităţilor trebuie să fie efectuată cu ajutorul unor metodici şi mijloace instrumentale speciale;

3) mijloacele instrumentale destinate cercetării pericolelor şi vulnerabilităţilor trebuie să ofere posibilitatea actualizării listelor de pericole şi vulnerabilităţi;

4) listele de pericole şi vulnerabilităţi trebuie să fie actualizate la intervale stabilite.

5.2.1. Determinarea domeniului şi limitelor procesului de management al riscurilor

La etapa respectivă este necesar de determinat domeniul de aplicare a managementului riscurilor, adică de stabilit categoriile de resurse şi procese interne în cadrul instituţiei, care vor fi examinate în decursul procesului respectiv, precum şi de stabilit nivelul de detaliere în determinarea riscurilor.

5.2.2. Analiza şi evaluarea riscurilor

Utilizarea sistemului de prestare a serviciilor este legată de o anumită totalitate de riscuri.

Analiza riscurilor reprezintă un proces de identificare a factorilor capabili să afecteze negativ procesul de prestare a serviciilor publice. Scopul acestui proces constă în stabilirea punctelor vulnerabile privind resursele din sistemul de prestare a serviciilor, a căror utilizare poate duce la încălcarea securităţii prestării serviciilor publice.

Evaluarea riscurilor reprezintă analiza sistematică a:

- prejudiciului probabil care poate fi cauzat în rezultatul dereglărilor în protecţie, luîndu-se în consideraţie consecinţele posibile ca urmare a pierderii confidenţialităţii, integrităţii sau disponibilităţii informaţiei şi a altor resurse;
- probabilităţii survenirii unei asemenea încălcări, luîndu-se în consideraţie pericolele şi punctele vulnerabile existente, precum şi măsurile şi mijloacele de asigurare a securităţii.

Pentru a controla eficienţa procesului de prestare a serviciilor publice, procesul de analiză şi evaluare a riscurilor trebuie să fie efectuat periodic, cel puţin o dată în an, prin aplicarea metodei de abordare a evaluării proporţiilor riscurilor.

Pentru a stabili conţinutul pericolelor şi al punctelor vulnerabile, este necesar de utilizat următoarele surse:

- rezultatele analizei conformităţii măsurilor şi mijloacelor aplicate de asigurare a securităţii cu cerinţele stabilite ale securităţii;
- surse publicate şi electronice ce conţin pericole şi puncte vulnerabile cunoscute ale mijloacelor de asigurare a securităţii;
- rezultatul funcţionării mijloacelor automatizate de identificare a pericolelor şi vulnerabilităţilor;
- rezultatele testării mijloacelor automatizate de asigurare a securităţii.

Este necesar de efectuat analiza şi evaluarea periodică a riscurilor securităţii şi a mijloacelor realizate de control pentru asigurarea:

- evidenţei modificărilor în cerinţele şi prioritătile instituţiei;
- luării în consideraţie a apariţiei pericolelor şi punctelor vulnerabile noi;
- garanţiei că mijloacele de asigurare a securităţii şi de control funcţionează eficient.

Analiza riscurilor trebuie efectuată la diferite niveluri în profunzime, în funcţie de rezultatele evaluărilor precedente şi de nivelurile ce variază ale riscurilor, al căror nivel este acceptabil pentru conducere.

Evaluările riscurilor trebuie efectuate iniţial la un nivel înalt în calitate de mijloace de stabilire a priorităţilor resurselor în zonele de risc sporit, iar ulterior la un nivel mai detaliat în vederea examinării riscurilor mai specifice.

Importanţa riscului condiţionat de realizarea pericolului trebuie stabilită ca funcţie a probabilităţii de survenire a prejudiciului în privinţa persoanelor fizice sau juridice, proprietăţii de stat, care poate fi cauzat în rezultatul neexecutării funcţiilor atribuite sistemelor de prestare a serviciilor şi al încălcării condiţiilor de exploatare a acestora.

Importanța riscului încălcării securității pentru fiecare resursă concret trebuie determinată ca importanță maximală a riscului pentru toate pericolele examinate ale securității care se referă la aceasta resursa informațională.

În procesul de efectuare a analizei este necesar de îndeplinit un complex de acțiuni, după cum urmează:

- identificarea şi evaluarea resurselor (hardware, software, mijloace de telecomunicații, resurse şi sisteme informaționale, mijloace de asigurare a securității);
- identificarea şi descrierea pericolelor, punctelor vulnerabile şi a mijloacelor de asigurare a securității şi de control. La identificarea pericolelor securității trebuie identificate toate pericolele securității existente şi potențiale de următoarele categorii:

1) obiective şi subiective;
2) interne şi externe;
3) ocazionale şi premeditate.

Descrierea pericolului securității trebuie să includă următoarele:

1) sursa pericolului;
2) mijlocul (metoda) de realizare a pericolului;
3) punctul vulnerabil utilizat;
4) tipul resurselor protejate asupra cărora influențează pericolul;
5) tipul de influență asupra resurselor;
6) caracteristica securității resurselor care este încălcată.

- determinarea probabilității pericolului şi a impactului asupra confidențialității, integrității, disponibilității şi veridicității. La stabilirea probabilității realizării pericolului trebuie de luat în considerație următoarele:

1) motivația, competența sursei pericolului şi resursele utilizate de acesta;
2) puncte vulnerabile existente;
3) existența şi eficiența măsurilor şi mijloacelor de asigurare a securității;

- evaluarea riscurilor, pregătirea recomandărilor privind contracararea acestora. Nivelul prejudiciului condiționat de realizarea pericolului trebuie determinat ca nivel maxim al prejudiciului pentru caracteristicile încălcate, prin realizarea pericolului, ale securității informației procesate în sistemul de prestare a serviciilor;
- elaborarea politicii şi documentației corespunzătoare privind analiza, evaluarea şi managementul riscurilor.

Cerințele privind protecția trebuie identificate pe calea evaluării metodice a riscurilor pentru securitate. Metodele de evaluare a riscurilor pot fi aplicate în privința instituției în totalitate sau a unor secțiuni din cadrul ei, precum şi în privința unor SI separate, componente specifice de sistem sau servicii, atunci cînd acest lucru este practic realizabil sau necesar.

Rezultatele acestei evaluări trebuie să fie utilizate la determinarea sau selectarea direcției acțiunii corespunzătoare de administrare privind asigurarea securității, la stabilirea priorităților protecției informației şi la realizarea mijloacelor de asigurare a securității şi de control;

5.2.3. Selectarea şi implementarea măsurilor şi mijloacelor de minimalizare a riscurilor

5.2.3.1. Selectarea măsurilor şi mijloacelor de minimalizare a riscurilor

După efectuarea analizei şi evaluării riscurilor este necesar de adoptat o decizie privind selectarea măsurilor şi mijloacelor de minimalizare a riscurilor pînă la un nivel admisibil, aprobat de conducere.

La adoptarea deciziei privind selectarea măsurilor şi mijloacelor de asigurare a securității şi controlului este necesar de luat în considerație următorii factori:

- cheltuielile privind implementarea şi mentenanța măsurilor şi mijloacelor de asigurare a

securității;

- politica de management al instituției;
- simplitatea realizării soluțiilor selectate.

Ținîndu-se cont de faptul că securitatea în procesul de prestare a serviciilor poate fi asigurată cu ajutorul diferitor combinații de măsuri şi mijloace organizaționale şi tehnice, ansamblul de măsuri şi mijloace concrete de asigurare a securității trebuie selectat pe baza minimalizării cheltuielilor organizaționale, tehnice şi financiare privind realizarea SI de prestare a serviciilor publice.

Măsurile de minimalizare a riscurilor trebuie să includă:

- diminuarea riscului - riscul este considerat inadmisibil. Pentru diminuarea acestuia este necesar de selectat şi de realizat măsuri şi mijloace corespunzătoare de asigurare a securității şi controlului;
- transferul riscului - riscul este considerat inadmisibil şi în anumite condiții trebuie să fie transferat către o organizație terță (de exemplu, în caz de asigurare sau externalizare);
- acceptarea riscului – riscul în cazul respectiv este considerat admisibil în mod conştient. Instituția cunoaşte şi acceptă eventualele consecințe deoarece costul măsurilor de contracarare depăşeşte în mod considerabil pierderile financiare în caz de realizare a pericolului sau este imposibil de identificat măsuri şi mijloace adecvate de asigurare a securității şi controlului;
- refuzul riscului – refuzul proceselor în cadrul instituției, care constituie cauza riscului sau refuzul serviciilor părților terțe în cazul în care ultimii nu sînt în stare să asigure nivelul acceptabil al riscului aferent serviciilor pe care le prestează.

Măsurile şi mijloacele de asigurare a securității în procesul de prestare a serviciilor publice trebuie selectate în următoarea consecutivitate:

- analiza măsurilor şi mijloacelor de asigurare a securității aplicate;
- suplinirea măsurilor şi mijloacelor de asigurare a securității aplicate cu măsuri şi mijloace necesare pentru îndeplinirea cerințelor stabilite în rezultatul evaluării riscurilor încălcării securității;
- evaluarea riscului încălcării securității pentru ansamblul selectat de măsuri şi mijloace de asigurare a securității;
- precizarea ansamblului selectat de măsuri şi mijloace de asigurare a securității, precum şi, în caz de necesitate, a cerințelor securității, în cazul în care nivelul determinat al riscului nu corespunde nivelului admisibil stabilit al riscului de încălcare a securității.

După stabilirea măsurilor şi mijloacelor necesare privind minimalizarea riscurilor este necesar de îndeplinit un complex de acțiuni, după cum urmează:

- de stabilit condițiile şi metodele de funcționare a mijloacelor de asigurare a securității şi controlului, precum şi ale complexului de hardware şi software;
- de setat configurații mijloacelor de asigurare a securității şi controlului, precum şi complexul de hardware şi software pentru lucru automat sau urmărire de către personal;
- de repartizat responsabilitatea pentru efectuarea verificărilor de control ale funcționării mijloacelor de asigurare a securității şi controlului şi ale complexului de hardware şi software.

Măsurile şi mijloacele de minimalizare a riscurilor trebuie revizuite periodic, cel puțin o dată în an.

5.2.3.2. Implementarea măsurilor şi mijloacelor de minimalizare a riscurilor

Măsurile şi mijloacele de minimalizare a riscurilor trebuie implementate în strictă conformitate cu politica de securitate a informației.

Pentru implementarea măsurilor şi mijloacelor de minimalizare a riscurilor este necesar de:

- stabilit responsabilitatea personală pentru aplicarea măsurilor şi mijloacelor de asigurare a securității în procesul de exploatare a sistemului de prestare a serviciilor publice;
- elaborat documentația organizatorică şi dispoziție privind implementarea măsurilor şi mijloacelor de asigurare a securității, în care să fie determinate:

1) sarcinile personalului şi utilizatorilor privind aplicarea măsurilor şi mijloacelor de asigurare a securităţii;

2) ordinea acţiunilor în caz de survenire a incidentelor de încălcare a securităţii în procesul de prestare a serviciilor;

3) procedura de control al aplicării măsurilor şi mijloacelor de asigurare a securităţii.

Mijloacele de asigurare a securităţi trebuie setate pe baza SI de prestare a serviciilor publice complet desfăşurat şi disponibil de a fi exploatat.

După implementarea măsurilor şi mijloacelor de asigurare a securităţii este necesar de efectuat verificări şi testări de control în vederea stabilirii corectitudinii realizării şi eficienţei acestora în calitate de contracarare a pericolelor securităţii.

Toate deciziile privind selectarea şi implementarea măsurilor şi mijloacelor referitoare la gestionarea riscurilor trebuie să fie înregistrate şi documentate; aceste decizii trebuie să garanteze faptul că riscurile sînt diminuate pînă la nivelul admisibil.

5.2.4. Monitorizarea procesului de management al riscurilor şi a eficienţei activităţilor selectate de minimalizare a riscurilor

Monitorizarea managementului riscurilor presupune analiza rezultatelor activităţilor de reducere a nivelului riscurilor identificate. La această etapă trebuie stabilite mecanismele de evaluare şi control al eficienţei managementului software-ului, proiectelor şi resurselor în limitele deciziilor adoptate în privinţa riscurilor.

În decursul monitorizării procesului de management al riscurilor şi a eficienţei măsurilor de minimalizare a riscurilor este necesar de îndeplinit un complex de acţiuni:

- de creat sistemul de monitorizare a riscurilor identificate şi a activităţilor de diminuare a acestora;
- de verificat eficienţa activităţilor şi lucrărilor de minimalizare a riscurilor;
- de identificat modificările riscurilor pentru instituţie la introducerea modificărilor în legislaţia naţională, apariţia tehnologiilor noi de prestare a serviciilor, modificare a structurii organizaţionale şi a împuternicirilor instituţiei, aplicare a noilor SI şi TI.;
- de edificat un sistem unic de informare despre modificări cu un proces adecvat de gestionare a modificărilor;
- de stabilit nivelul de corespundere a procesului curent de management al riscurilor cu mecanismele existente;
- de determinat mecanismul păstrării informaţiei de lucru examinate în procesul de gestionare a riscurilor.

În calitate de mijloace de monitorizare a procesului de management al riscurilor este necesar de îndeplinit următoarele acţiuni:

- de aplicat măsuri de ordin tehnic – monitorizarea, analiza registrelor de sistem şi a efectuării verificărilor în vederea pregătirii rapoartelor pentru a fi prezentate conducerii;
- de efectuat analiza din partea conducerii;
- de efectuat audit intern independent al securităţii informaţionale.

Auditul sistemului de management al riscurilor reprezintă o etapă indispensabilă a monitorizării riscurilor, în decursul căreia este necesar de examinat următoarele:

- eficienţa mijloacelor de telecomunicaţii din interiorul şi din exteriorul instituţiei;
- eficienţa utilizării mijloacelor alocate pentru activităţile legate de gestionarea riscurilor;
- eficienţa muncii consultanţilor externi şi a părţilor terţe care prestează servicii de externalizare;
- existenţa mecanismelor de reacţionare în caz de situaţii de criză şi eficienţa planului de asigurare a continuităţii activităţii;
- procedurile de manipulare a riscurilor-cheie, existenţa planurilor interne de verificări, elaborate

în vederea identificării noilor riscuri şi pericole.

5.3. Securitate organizațională

Crearea şi implementarea sistemului de asigurare a securității în procesul de prestare a serviciilor publice sînt posibile doar în condițiile determinării clare a responsabilităților şi împuternicirilor privind realizarea procesului de management şi asigurare a securității.

Subdiviziunile şi anumiți colaboratori ai instituției trebuie să-şi îndeplinească obligațiile privind asigurarea securității în conformitate cu documentele organizatorico-dispozitive elaborate şi aprobate de conducere (dispoziții, instrucțiuni, obligațiuni, liste, formulare).

În procesul de stabilire a responsabilităților şi atribuțiilor legate de asigurarea securității procesului de prestare a serviciilor publice, îndeplinirea următoarelor cerințe este obligatorie:

- este necesar de determinat rolurile şi obligațiile specifice privind realizarea şi susținerea măsurilor şi mijloacelor corespunzătoare privind protecția resurselor instituției;
- conducerea trebuie să asigure confirmarea obligațiilor sale privind crearea, implementarea, exploatarea, controlul permanent, analiza, menținerea în stare de lucru şi perfecționarea sistemului de asigurare a securității cu ajutorul unui complex de acțiuni, după cum urmează:

1) elaborarea politicii de securitate, precum şi planurilor de asigurare a securității;

2) aducerea la cunoştința personalului care participă la procesul de prestare a serviciilor publice a faptului privind importanța realizării scopurilor de asigurare a securității în procesul de prestare a serviciilor publice;

3) asigurarea unui volum suficient de resurse pentru crearea, implementarea, exploatarea, controlul permanent, analiza, menținerea în stare de lucru şi perfecționarea sistemului de asigurare a securității;

4) adoptarea deciziei privind criteriile de acceptare a riscului şi nivelurile admisibile ale riscului;

- nivelurile de responsabilități şi atribuții trebuie să fie clar determinate şi documentate;
- este necesar de desemnat o persoană responsabilă de managementul securității, precum şi de implementarea măsurilor şi mijloacelor de asigurare a securității;
- activitatea de protecție a informației trebuie să fie coordonată de către reprezentanți ai diferitelor unități structurale din cadrul instituției, învestiți cu funcții şi obligații de lucru corespunzătoare;
- conducerea trebuie să solicite de la colaboratori şi părțile terțe asigurarea securității procesului de prestare a serviciilor publice în conformitate cu cerințele de securitate stabilite;
- detaliile responsabilității stabilite trebuie să fie fundamentate în documentele organizatorice şi de dispoziție;
- este necesar de stabilit obligațiile privind protecția anumitor resurse şi executarea anumitor procese şi proceduri legate de securitatea procesului de prestare a serviciilor;
- persoana responsabilă de protecția resurselor respective poate să-şi transmită împuternicirile privind asigurarea securității unui alt colaborator al instituției sau unei părți terțe, sub rezerva că împuternicirile transmise se vor realiza în modul corespunzător.

5.4. Clasificarea resurselor şi organizarea mediului de control

Clasificarea resurselor ce urmează să fie supuse protecției constituie un element necesar în organizarea lucrărilor de asigurare a securității informaționale a sistemului de prestare a serviciilor publice.

Scopurile procesului de clasificare a resurselor sînt următoarele:

- determinarea şi menținerea în stare de lucru a unui sistem adecvat şi eficient de protecție a resurselor în procesul de prestare a serviciilor publice;
- asigurarea unui nivel corespunzător de protecție a resurselor şi sistemelor informaționale care participă la procesul de prestare a serviciilor publice.

În procesul de clasificare a resurselor este necesar de îndeplinit următoarele cerințe:

- toate resursele trebuie să fie luate în consideraţie şi atribuite proprietarilor responsabili;
- este necesar de stabilit responsabilitatea proprietarilor de resurse pentru menţinerea măsurilor corespunzătoare de asigurare a securităţii informaţionale;
- fiecare resursă trebuie să fie identificată cu precizie şi clasificată conform criteriilor de securitate;
- proprietarii de resurse trebuie să fie autorizaţi, iar datele despre aceştia trebuie să fie documentate.

Este necesar de efectuat clasificarea resurselor protejate în scopul selectării corecte a măsurilor şi mijloacelor de asigurare a securităţii acestora, prin îndeplinirea următoarelor acţiuni:
- stabilirea gradelor de importanţă la asigurarea protecţiei resurselor;
- atribuirea resurselor concrete la categoriile corespunzătoare.

În calitate de resurse pot fi şi serviciile publice prestate prin intermediul Portalului Guvernamental.

Pentru sistemul de prestare a serviciilor publice trebuie să fie utilizate gradele de secretizare şi categoriile de integritate a resurselor protejate, precum şi gradul de accesibilitate a serviciilor.

Categoriile de protecţie pentru resurse, precum sînt mijloacele de procesare a informaţiei, trebuie stabilite în funcţie de categoriile de secretizare şi integritate a informaţiei păstrate sau procesate. Pentru resursele respective este necesar de stabilit cerinţe concrete privind utilizarea variantelor corespunzătoare de măsuri obligatorii şi setări ale mijloacelor de protecţie a informaţiei.

Toate rezultatele clasificării trebuie examinate şi aprobate de persoanele cu funcţii de răspundere corespunzătoare şi trebuie documentate în materie de asigurare a securităţii SI de prestare a serviciilor publice.

În baza clasificării resurselor urmează să fie organizat mediul de control dotat cu următoarele elemente:
- principiile fundamentale de gestionare a instituţiei;
- structura organizaţională;
- delimitarea responsabilităţilor şi împuternicirilor;
- politica de resurse umane.

Pentru fiecare element este necesar de efectuat proceduri de control, necesare pentru realizarea obiectivelor de corespundere cu cerinţele interne ale instituţiei şi asigurare a securităţii.

5.4.1. Gradele de secretizare a resurselor protejate

Gradele de secretizare a resurselor protejate sînt reglementate cu Legea Republicii Moldova „Cu privire la secretul de stat” nr. 245 din 27.11.2008.

5.4.2. Categoriile de integritate a resurselor protejate

Categoriile de integritate a resurselor protejate sînt următoarele:
- „Cu nivel înalt de cerinţe” - această categorie include resursele a căror modificare sau falsificare nesancţionată poate cauza un prejudiciu direct considerabil instituţiei şi a căror integritate şi autenticitate trebuie să fie asigurate cu ajutorul unor metode garantate (semnătura digitală) în conformitate cu cerinţele obligatorii ale legislaţiei în vigoare;
- „Cu nivel redus de cerinţe” - această categorie include resursele a căror modificare, substituire sau lichidare nesancţionată poate cauza un prejudiciu indirect nesemnificativ instituţiei, utilizatorilor şi colaboratorilor acesteia;
- „Fără cerinţe” - această categorie include resursele pentru care nu sînt înaintate cerinţe faţă de asigurarea integrităţii.

5.4.3. Gradele de disponibilitate a serviciilor

În privinţa sistemului de prestare a serviciilor publice trebuie aplicate următoarele grade de disponibilitate a serviciilor în funcţie de categoria de utilizatori:

- „Disponibilitate liberă” - accesul la serviciu este asigurat în orice moment, serviciul este oferit în permanență, durata reținerii la primirea rezultatului nu depăşeşte cîteva secunde sau minute;
- „Disponibilitate înaltă” - accesul la serviciu este asigurat fără rețineri temporare substanțiale;
- „Disponibilitate medie” - accesul la serviciu poate fi asigurat cu rețineri temporare substanțiale, durata reținerii la primirea rezultatului nu depăşeşte 3 zile;
- „Disponibilitate redusă” – reținerile temporare la accesarea serviciului sînt practic nelimitate, durata admisibilă a reținerii la primirea rezultatului este 7 zile.

5.5. Securitatea personalului

5.5.1. Cerințe esențiale privind securitatea personalului

Asigurarea nivelului necesar de securitate la prestarea serviciilor publice se realizează în baza pregătirii corespunzătoare a specialiştilor şi utilizatorilor care participă la procesul de prestare a serviciilor publice şi a respectării de către aceştia a tuturor regulilor stabilite, orientate spre asigurarea securității.

Cerințele esențiale privind securitatea personalului care participă la procesul de prestare a serviciilor publice trebuie să includă:

- elaborarea, documentarea şi reînnoirea periodică a politicii de asigurare a securității personalului, precum şi procedurile şi măsurile legate de realizarea acestei politici;
- cerințe privind clasificarea personalului:

1) este necesar de desemnat categoriile de personal şi de determinat criteriile corespunzătoare de selectare a personalului din fiecare categorie;

2) categoriile de personal şi criteriile de selectare trebuie să fie periodic analizate şi, în caz de necesitate, ajustate;

- cerințe de securitate la angajarea personalului:

1) este necesar de efectuat verificarea candidaților la funcții, în special la funcțiile care implică accesul la resursele de valoare (existența recomandărilor pozitive, verificarea CV-ului candidatului, confirmarea studiilor şi calificărilor profesionale declarate, verificarea independentă a autenticității actelor de identitate);

2) toți colaboratorii şi reprezentanții organizației terțe care utilizează mijloacele de procesare a informației
trebuie să semneze acorduri de confidențialitate;

- cerințe de securitate la concedierea personalului:

1) la concedierea specialistului trebuie anulat accesul acestuia la resurse;

2) cu specialistul concediat trebuie să fie purtată discuția finală;

3) trebuie să fie asigurată restituirea tuturor atributelor (cheilor, cartelelor de identificare etc.) aflate la specialistul concediat;

4) trebuie să fie asigurată posibilitatea de a accesa informația, creată de specialistul concediat, de către specialiştii împuterniciți din cadrul instituției;

- în cazul transferului specialistului la o altă funcție trebuie reexaminate atributele şi mijloacele specialistului, în baza cărora acestuia i se acordă accesul, (de exemplu, eliberarea repetată a cheilor, cartelelor de identificare, ştergerea înregistrării de evidență învechite şi crearea unei noi înregistrări de evidență);
- determinarea şi aplicarea diferitelor sancțiuni față de specialiştii care nu îndeplinesc cerințele din cadrul politicilor şi procedurile corespunzătoare de asigurare a securității.

5.5.2. Cerințe privind informarea şi instruirea în probleme de asigurare a securității

Pentru asigurarea certitudinii în informarea utilizatorilor despre pericolele şi problemele privind securitatea şi dotarea acestora cu tot necesarul pentru respectarea cerințelor politicii de securitate în procesul de exercitare a obligațiunilor de serviciu este necesar:

- de elaborat, documentat şi periodic de reînnoit politica instruirii în materie de securitate, precum şi procedurile şi măsurile privind realizarea politicii de instruire în materie de securitate;

- de respectat cerințele privind informarea în problemele de securitate:

1) în fişele de post trebuie să fie incluse obligațiile generale privind implementarea şi respectarea politicii de securitate şi aspectele specifice privind protecția unor anumite resurse sau acțiuni referitoare la securitate;

2) este necesar de instruit utilizatorii în materie de proceduri de securitate şi utilizare corectă a mijloacelor de procesare a informației în vederea minimalizării eventualelor riscuri de securitate;

- de respectat cerințele privind instruirea în problemele de securitate:

1) este necesar de identificat persoanele din rîndurile personalului, care îndeplinesc roluri şi dețin obligații esențiale din punct de vedere al influenței asupra securității;

2) este necesar de format grupuri de instruire, în dependență de funcțiile şi obligațiile exercitate;

3) pentru fiecare grup trebuie elaborate materiale educaționale;

4) instruirea specialiştilor trebuie să asigure cunoaşterea de către aceştia a cerințelor securității, a responsabilității în conformitate cu legislația în vigoare, a măsurilor şi mijloacelor de asigurare a securității, precum şi cunoaşterea utilizării corecte a mijloacelor de procesare a informației;

5) persoanele identificate trebuie să fie instruite în probleme de securitate;

- personalul care participă la procesul de prestare a serviciilor publice trebuie să susțină un instructaj privind următoarele aspecte:

1) sistemul de protecție a procesului de prestare a serviciilor publice şi modul de utilizare a acestui sistem;

2) principiile de bază privind structura şi particularitățile mijloacelor moderne de protecție a informației;

3) metodele de protecție a informației.

5.5.3. Cerințe privind reacționarea la incidentele de încălcare a securității

Pentru a minimaliza prejudiciul cauzat în rezultatul incidentelor de încălcare a securității şi deranjamentelor în funcționarea complexului de mijloace hardware şi software, precum şi pentru a efectua monitorizarea şi reacționarea în caz de incidente este necesar:

- de elaborat, documentat şi reînnoit periodic politica de reacționare în caz de incidente de încălcare a securității, precum şi proceduri şi măsuri privind realizarea politicii de reacționare în caz de incidente de încălcare a securității;

- de respectat cerințele privind informarea despre incidentele de încălcare a securității:

1) este necesar, în conformitate cu procedura stabilită, de informat conducerea despre încălcarea securității imediat, dacă este posibil, şi;

2) toți colaboratorii şi organizațiile terțe trebuie să fie informate în privința procedurilor de informare despre diferite tipuri de incidente, precum sînt violarea securității, existența unui pericol potențial şi a unei vulnerabilități, deranjamentele produse în funcționarea mijloacelor software şi hardware, care pot influența negativ asupra securității resurselor instituției;

3) trebuie stabilite măsuri de răspundere disciplinară pentru colaboratorii care încalcă cerințele securității;

- de respectat cerințele privind instruirea despre acțiunile de reacționare la incidentele de încălcare a securității:

1) personalul trebuie să fie instruit periodic privind responsabilitatea şi obligațiile la îndeplinirea acțiunilor de gestionare a reacționării la incidentele de încălcare a securității;

2) în procesul de instruire a personalului trebuie modelate evenimente corespunzătoare, ceea ce va ajuta pe viitor personalul să-şi îndeplinească eficient acțiunile cerute de la acesta în caz de survenire a situațiilor de criză;

3) trebuie utilizate mijloace automatizate în vederea asigurării unui mediu mai complet şi real de instruire;

- de respectat cerințele privind prelucrarea incidentelor:

1) posibilitățile de prelucrare a incidentelor trebuie să includă: depistarea, analiza, prevenirea evoluării, lichidarea incidentelor de încălcare a securității şi restabilirea securității după incidente;

2) trebuie utilizate mijloace automatizate pentru susținerea procesului de prelucrare a incidentelor;

- de respectat cerințele privind verificarea eficienței acțiunilor de reacționare la incidentele de încălcare a securității:

1) trebuie efectuată verificarea periodică a eficienței acțiunilor de reacționare la incidentele de încălcare a securității, cu utilizarea testelor corespunzătoare (succesiunilor acțiunilor de control);

2) trebuie utilizate mijloace automatizate pentru efectuarea unei verificări mai minuțioase a eficienței acțiunilor de reacționare la incidentele de încălcare a securității;

- de respectat cerințele privind monitorizarea incidentelor:

1) este necesar de stabilit procedura de monitorizare şi înregistrare a incidentelor şi deranjamentelor în ce priveşte numărul, tipul şi parametrii acestora;

2) incidentele de încălcare a securității trebuie urmărite şi documentate permanent;

3) trebuie utilizate mijloace automatizate în procesul de urmărire a incidentelor de încălcare a securității, colectare şi analiză a informației despre incidente;

- de respectat cerințele privind prezentarea rapoartelor despre incidente:

1) este necesar de prezentat rapoarte privind incidentele organelor stabilite, în conformitate cu forma şi periodicitatea stabilită;

2) trebuie utilizate mijloace automatizate de susținere a elaborării şi prezentării rapoartelor privind incidentele de încălcare a securității.

5.6. Securitate fizică

Pentru a preveni accesul neautorizat, deteriorarea şi influența asupra încăperilor şi informației instituției, este necesar de asigurat securitatea fizică a mijloacelor de procesare a informației de serviciu cu ajutorul diferitelor bariere de protecție şi mijloacelor de control al intruziunii.

Cerințele privind protecția fizică trebuie să includă:

- elaborarea, documentarea şi reînnoirea periodică a politicii de protecție fizică şi de protecție a mediului SI, precum şi proceduri şi măsuri privind realizarea acestei politici;

- cerințe privind sancționarea accesului fizic:

1) trebuie elaborate listele personalului, căruia îi va fi autorizat accesul la resurse şi emise mandatele corespunzătoare (insigne, cartele de identificare, cartele intelectuale);

2) persoanele cu funcții de răspundere corespunzătoare trebuie să examineze şi să aprobe listele şi mandatele ce permit accesul;

3) listele privind accesul trebuie revizuite în conformitate cu periodicitatea stabilită;

- cerințe privind gestionarea accesului fizic:

1) nivelul de protecție trebuie să fie proporțional riscurilor identificate;

2) trebuie efectuată gestionarea accesului fizic în toate punctele de acces la resurse;

3) este necesar de utilizat zone de securitate clar determinate pentru protejarea încăperilor şi zonelor de amplasare a mijloacelor de procesare a informației;

4) accesul în încăperi şi clădiri trebuie să fie permis doar personalului autorizat;

5) înainte de acordarea accesului fizic la resurse, trebuie îndeplinită procedura de verificare a împuternicirilor de acces;

6) este necesar de analizat şi de revizuit în mod regulat drepturile de acces al colaboratorilor în zonele de securitate;

- cerințe privind monitorizarea accesului fizic:

1) trebuie efectuat controlul permanent al accesului în zonele de intrare în perimetrul clădirii pentru a se asigura de faptul că accesul este permis doar personalului autorizat;

2) în procesul de monitorizare trebuie utilizate dispozitive de supraveghere şi semnalizare a timpului real, precum şi mijloace automatizate care să asigure recunoaşterea încălcărilor şi să iniţieze acţiuni de răspuns;

3) controlul accesului fizic la încăperi trebuie asigurat cu ajutorul celor mai stricte metode de identificare/autentificare;

- cerinţe privind controlul vizitatorilor:

1) trebuie repartizată zona de înregistrare a vizitatorilor sau trebuie să existe alte activităţi de gestionare a accesului fizic în încăperi şi clădiri;

2) trebuie efectuată gestionarea accesului fizic al vizitatorilor la obiecte;

3) trebuie efectuată însoţirea vizitatorilor la obiecte şi controlul asupra acţiunilor acestora;

- cerinţe privind ţinerea registrelor de evidenţă a accesului vizitatorilor:

1) în zonele de securitate vizitatorii trebuie să fie însoţiţi sau să deţină accesul corespunzător;

2) trebuie ţinute registrele de evidenţă a accesului vizitatorilor, în care urmează să fie înregistrate data şi ora intrării şi ieşirii;

3) registrele de evidenţă a accesului vizitatorilor trebuie să fie analizate periodic de către persoanele cu funcţii de răspundere corespunzătoare;

4) trebuie utilizate mijloace automatizate de ţinere a registrelor de evidenţă a accesului vizitatorilor;

- cerinţe privind protecţia echipamentului:

1) echipamentul trebuie să fie amplasat şi protejat astfel încît să fie diminuate riscurile cauzate de influenţele din partea mediului ambiant şi de posibilităţile de acces neautorizat;

2) echipamentul trebuie protejat de deranjamentele în furnizarea energiei electrice şi de alte deranjamente legate de electricitate, de exemplu, existenţa surselor de alimentare de rezervă;

3) echipamentul trebuie protejat de incendii şi alte situaţii excepţionale;

4) trebuie protejate reţelele de telecomunicaţii prin cablu de interceptarea informaţiei dau de deteriorări;

5) trebuie realizată deservirea tehnică corespunzătoare a echipamentului pentru a asigura capacitatea de lucru continuă şi integritatea acestuia.

5.7. Managementul comunicaţiilor şi al activităţii operaţionale a tehnologiilor informaţionale

Pentru a asigura certitudinea în privinţa funcţionării corespunzătoare şi sigure a mijloacelor de procesare a informaţiei este necesar de stabilit obligaţiuni şi proceduri de gestionare şi funcţionare a tuturor mijloacelor de procesare a informaţiei.

Managementul comunicaţiilor şi activităţii operaţionale de funcţionare a TI şi a mijloacelor de procesare a informaţiei trebuie să corespundă următoarelor cerinţe:

- cerinţe privind procedurile operaţionale:

1) procedurile operaţionale trebuie să fie considerate ca fiind documente oficiale, trebuie să fie documentate şi respectate cu strictețe, iar modificările în cadrul acestora trebuie aprobate de către conducere;

2) procedurile trebuie să conţină instrucţiunea detaliată privind executarea unei sarcini concrete şi să includă:

a) procesarea şi gestionarea informaţiei;

b) stabilirea cerinţelor în privinţa graficului de îndeplinire a sarcinilor ce includ interconexiunile între sisteme;

c) ora începerii îndeplinirii sarcinii celei mai timpurii şi ora finalizării ultimei sarcini;

d) procesarea erorilor şi altor situații excepționale care pot surveni în procesul de executare a sarcinilor;

e) restartarea sistemului şi a procedurii de restabilire în caz de deranjamente de sistem;

3) trebuie de asigurat sincronizarea ceasului de sistem pentru executarea corectă a operațiunilor în rețea;

4) trebuie de controlat în permanență modificările configurațiilor în cadrul mijloacelor şi sistemelor de procesare a informației;

5) trebuie stabilite şi implementate roluri, responsabilități şi proceduri de asigurare a controlului tuturor modificărilor în echipament, software sau proceduri;

6) trebuie stabilite obligațiuni şi proceduri de gestionare a incidentelor pentru asigurarea unei reacții rapide, eficiente şi organizate în caz de încălcare a securității;

7) este necesară existența registrelor de înregistrare a erorilor survenite în rezultatul deranjamentelor şi necorespunderilor în procesul de funcționare a sistemului;

- cerințe privind protecția împotriva software-ului dăunător:

1) utilizatorii trebuie informați despre pericolul utilizării software-ului neautorizat sau dăunător;

2) trebuie implementate mijloace speciale de control pentru depistarea şi/sau prevenirea pătrunderii acestui gen de programe;

3) trebuie instalat şi reînnoit în mod regulat software-ul antivirus pentru depistarea şi scanarea calculatoarelor şi purtătorilor de informații;

4) trebuie efectuată inventarierea regulată a software-ului şi a datelor din sistemele care susțin procesele critice ale instituției;

5) trebuie asigurată depistarea tentativelor şi protecția împotriva modificării nesancționate a software-ului şi informației;

- cerințe privind rezervarea şi păstrarea informației:

1) trebuie efectuată în mod regulat copierea de rezervă a informației de serviciu importante şi a software-ului;

2) trebuie asigurat nivelul garantat de protecție fizică şi de protecție împotriva influențelor din partea mediului ambiant pentru copiile de rezervă;

3) trebuie efectuată testarea regulată a echipamentului de rezervă;

4) trebuie actualizate şi testate în mod regulat procedurile de restabilire pentru asigurarea eficienței executării acestora;

5) trebuie efectuat controlul fizic şi păstrarea în siguranță a purtătorilor de informații (de hîrtie sau în format electronic), luîndu-se în considerație categoria maximă de securitate a informației înregistrate pe purtător;

6) pentru păstrarea informației trebuie selectate metode de arhivare a acesteia care să permită restabilirea acestei informații în caz de necesitate, luîndu-se în considerație modificările mijloacelor software şi hardware utilizate;

7) la păstrarea informației trebuie luate în considerație toate aspectele juridice legate de drepturile proprietarului informației utilizate în SI;

8) trebuie identificate locațiile de păstrare de rezervă a informației şi trebuie soluționate aspectele administrative privind păstrarea copiilor de rezervă ale informației;

9) locațiile de păstrare a copiilor de rezervă a informației trebuie să fie delimitate în spațiu (geografic) de locațiile principale de păstrare a informației pentru a nu fi supuse unor pericole identice;

10) locația de păstrare de rezervă a informației trebuie configurată astfel încît să asigure executarea la timp şi eficientă a operațiilor de restabilire;

11) trebuie determinate problemele potențiale ce țin de accesibilitatea locațiilor de păstrare de

rezervă a informației, în caz de deranjament sau accident, şi trebuie stabilite acțiuni concrete privind restabilirea accesibilității;

- cerințe privind securitatea purtătorilor de informație:

1) este necesară existența unor proceduri de utilizare a purtătorilor de informație de schimb (benzi, discuri, casete, precum şi rapoarte imprimate);

2) toate purtătorile de informație trebuie păstrate în locuri sigure;

3) acțiunile de lichidare a informației de pe purtătorile de informație trebuie controlate, documentate şi verificate;

4) este necesar de distrus fizic sau de recopiat într-un mod sigur purtătorile de date ce conțin informații importante, funcțiile standard de lichidare nu urmează a fi utilizate;

5) este necesar de verificat toate componentele echipamentului ce conține purtători de date (de exemplu, hard-discuri incorporate) în materie de lichidare a tuturor datelor importante şi a software-ului licențiat;

6) procedurile de lichidare a informației de pe purtătorile de informație trebuie să fie analizate periodic în materie de corectitudine şi eficiență;

7) trebuie efectuată marcarea tuturor purtătorilor de informație şi trebuie limitat accesul în vederea identificării personalului neautorizat;

8) la purtătorile de informație detaşabile trebuie să fie ataşate mențiuni externe care să conțină informații despre conținutul instalat;

9) trebuie pregătită lista purtătorilor de informație la care au fost ataşate mențiuni externe;

10) trebuie asigurată înregistrarea formalizată a beneficiarilor de date autorizați;

11) în cazul transmiterii purtătorului de informație pentru utilizare repetată, trebuie efectuată procedura de vidare a acestuia pentru a exclude posibilitatea acordării nesancționate a accesului la informația stocată pe purtătorul de informație şi utilizării acesteia de către persoane ce nu sînt învestite cu împuternicirile corespunzătoare;

12) trebuie efectuat controlul transportării purtătorului de informație pentru a asigura recepționarea acestuia doar de către persoana care este învestită cu împuterniciri corespunzătoare;

- cerințe privind accesul la purtătorile de informație secretă – accesul la purtătorile de informație secretă trebuie să fie permis doar persoanelor ce dispun de împuternicirile corespunzătoare, în conformitate cu gradele de secretizare şi în conformitate cu Legea Republicii Moldova „Cu privire la secretul de stat” nr. 245 din 27.11.2008;

- cerințe privind gestionarea serviciilor de rețea:

1) trebuie de repartizat responsabilitățile şi stabilite procedurile şi obligațiunile privind susținerea resurselor de rețea şi a operațiilor de calculator;

2) trebuie implementate mijloace speciale de control pentru asigurarea confidențialității şi integrității datelor care circulă prin rețele de acces comun, precum şi pentru protecția sistemelor cheie;

- cerințe privind schimbul de date:

1) trebuie stabilite procedurile şi măsurile de protecție a informației şi suporturilor în procesul transmiterii acestora;

2) la stabilirea cerințelor de securitate trebuie luat în considerație gradul de importanță a informației ce constituie obiectul schimbului;

3) trebuie asigurată protecția schimbului de date prin intermediul poştei electronice şi a tranzacției în regim on-line prin intermediul rețelelor de acces comun, în special, prin Internet;

4) este necesar de protejat software-ul, datele şi alte informații ce necesită un nivel înalt de integritate şi accesul la care este realizat prin sistemele de acces public, cu ajutorul mijloacelor de protecție criptografică a informației, de exemplu, prin intermediul semnăturii digitale;

5) trebuie asigurată protecția procesului de schimb de informații prin intermediul mijloacelor verbale, de fax şi video de comunicații.

5.8. Controlul accesului

Pentru a asigura accesul sancționat la resursele şi procesele instituției este necesar de efectuat controlul accesului luîndu-se în considerație cerințele interne ale instituției şi cerințele de securitate.

Toate cerințele privind controlul accesului trebuie să fie reflectate în politici cu privire la distribuirea şi autorizarea informației.

5.8.1. Cerințe față de accesul logic

Pentru a asigura accesul la informație doar pentru utilizatorii autorizați este necesar de efectuat controlul accesului logic.

Față de controlul logic sînt înaintate următoarele cerințe:

- regulile privind controlul accesului şi drepturile fiecărui utilizator sau grup de utilizatori trebuie să fie stabilite clar în politica de securitate;
- clasificarea informației în privința diferitor sisteme şi rețele trebuie să fie adusă în concordanță cu politica de control al accesului;
- trebuie determinate profilurile standard de acces al utilizatorilor pentru obligațiunile şi funcțiile tipice;
- stabilirea regulilor trebuie să se bazeze pe premisa „în caz general, totul trebuie să fie interzis, pînă cînd evident nu va fi admis”.

5.8.2. Cerințe privind controlul accesului utilizatorilor

Pentru a preveni accesul neautorizat la resurse este necesar de efectuat controlul acordării drepturilor de acces la resursele instituției.

O abordare riguroasă a acordării accesului utilizatorilor la resursele instituției trebuie să asigure un control strict al accesului şi să permită stabilirea tuturor încălcărilor posibile ale securității.

Controlul accesului utilizatorilor trebuie să includă:

- cerințe privind gestionarea înregistrărilor de evidență:

1) trebuie realizată gestionarea înregistrărilor de evidență, inclusiv crearea, activarea, modificarea, revizuirea în baza unei periodicități stabilite, dezactivarea şi lichidarea înregistrărilor de evidență;

2) trebuie utilizate mijloace automatizate de susținere a gestionării înregistrărilor de evidență;

3) acțiunea înregistrărilor de evidență temporare trebuie să înceteze în mod automat la expirarea perioadei stabilite de timp (pentru fiecare tip de înregistrare de evidență);

4) trebuie efectuată dezactivarea automată a înregistrărilor de evidență inactive după o anumită perioadă de timp;

5) trebuie utilizate mijloace automatizate de înregistrare (audit) şi notificare despre crearea, modificarea, dezactivarea, anularea înregistrării de evidență;

- cerințe privind gestionarea privilegiilor:

1) acordarea privilegiilor trebuie să fie controlată prin intermediul procesului de autorizare;

2) accesul la funcțiile securității realizate în software, hardware şi soft-hardware trebuie să fie permis doar persoanelor învestite cu împuterniciri corespunzătoare, de exemplu administratorilor de securitate;

3) privilegiile trebuie să fie acordate doar colaboratorilor care au nevoie de acestea pentru a executa o lucrare şi doar pe durata executării acesteia;

4) este necesar de asigurat procesul de autorizare şi înregistrare a tuturor privilegiilor acordate;

5) privilegiile nu trebuie să fie acordate înainte de încheierea procesului de autorizare;

6) trebuie realizat periodic procesul formalizat de revizuire a drepturilor de acces al utilizatorilor (se recomandă de realizat o dată în 6 luni sau după fiecare modificare);

- cerințe privind controlul parolelor:

1) toţi utilizatorii trebuie să semneze documentul privind necesitatea de respectare a confidenţialităţii depline a parolelor personale;

2) parolele nu trebuie să fie păstrate niciodată în formă neprotejată.

5.8.3. Cerinţe privind obligaţiile utilizatorilor

Pentru a preveni accesul neautorizat al utilizatorilor la informaţie este necesar de asigurat informarea utilizatorilor despre obligaţiile lor privind utilizarea măsurilor efective de gestionare a accesului.

Obligaţiile utilizatorilor în privinţa controlului de acces sînt:

- utilizatorii trebuie să respecte anumite reguli de asigurare a securităţii în procesul selectării şi utilizării parolelor;
- toţi utilizatorii trebuie să fie informaţi despre necesitatea:

1) de a păstra confidenţialitatea parolelor;

2) de a interzice înregistrarea parolelor pe hîrtie, dacă nu este asigurată păstrarea în siguranţă a acestora;

3) de a modifica parolele ori de cîte ori există un indiciu de compromitere posibilă a sistemului şi parolei;

4) de a selecta parole calitative de lungime minimă formate din şase semne;

5) de a modifica parolele după anumite intervale de timp sau după un anumit număr de accese şi de a exclude utilizarea repetată sau ciclică a parolelor vechi;

6) parolele pentru înregistrările de evidenţă privilegiate trebuie să se schimbe mai frecvent decît parolele obişnuite;

- utilizatorii trebuie să asigure protecţia adecvată a echipamentului lăsat fără supraveghere şi să îndeplinească următoarele cerinţe:

1) şedinţele active la finalizarea lucrării trebuie să fie terminate în cazul în care lipseşte mecanismul de blocare a şedinţei;

2) trebuie limitat numărul de şedinţe paralele pentru fiecare utilizator;

3) trebuie efectuată finalizarea automată a şedinţei după o perioadă stabilită de inactivitate.

5.8.4. Cerinţe privind controlul accesului la reţea

Pentru a asigura protecţia serviciilor de reţea este necesar de efectuat controlul accesului la serviciile de reţea atît interne cît şi externe.

Cerinţele privind controlul accesului la reţea trebuie să includă următoarele:

- este necesar de asigurat accesul utilizatorilor doar la serviciile de care aceştia au nevoie pentru a-şi îndeplini obligaţiile şi pentru care dispun de autorizaţie;
- trebuie de stabilit:

1) reţelele şi serviciile de reţea la care este permis accesul;

2) procedurile de autorizare pentru determinarea cui, la care reţele şi servicii de reţea este permis accesul;

3) măsurile şi procedurile de protecţie împotriva conectării nesancţionate la serviciile de reţea;

- este necesar de limitat variantele de marşrutizare în fiecare punct al reţelei;
- cerinţe privind accesul la distanţă:

1) toate metodele de accesare la distanţă a resurselor (precum sînt legătura prin modem, Internet) trebuie să fie documentate şi supuse monitorizării şi controlului;

2) fiecare metodă de accesare la distanţă utilizată trebuie să fie sancţionată de către persoanele cu funcţii de răspundere corespunzătoare şi permisă doar utilizatorilor care au nevoie de aceasta pentru îndeplinirea sarcinilor stabilite;

3) pentru facilitatea monitorizării şi controlului accesului la distanţă este necesar de utilizat mijloace automatizate corespunzătoare;

4) este necesar de realizat gestionarea centralizată a accesului la distanță la SI;

- cerințe privind gestionarea accesului pentru dispozitivele portabile şi mobile:

1) trebuie stabilite restricții şi elaborate instrucțiuni pentru utilizarea dispozitivelor portabile şi mobile;

2) accesul la SI cu ajutorul dispozitivelor portabile şi mobile trebuie să fie documentat şi supus monitorizării şi controlului;

3) utilizarea dispozitivelor portabile şi mobile trebuie să fie sancționată de persoanele cu funcții de răspundere corespunzătoare;

4) trebuie utilizate hard-discuri de schimb sau alte metode şi mijloace de protecție a informației fixate pe dispozitivele portabile şi mobile;

- cerințe privind limitarea conexiunilor fără cablu:

1) trebuie stabilite restricții şi elaborate instrucțiuni pentru utilizarea tehnologiilor fără cablu;

2) accesul fără cablu la SI trebuie să fie documentat şi supus monitorizării şi controlului;

3) accesul fără cablu la SI trebuie să fie permis doar în cazul aplicării mijloacelor de protecție criptografică a informației;

4) utilizarea tehnologiilor fără cablu trebuie să fie sancționată de către persoanele cu funcții de răspundere corespunzătoare.

5.8.5. Cerințele accesului la sistemele operaționale

Pentru a preveni accesul neautorizat la calculatoare la nivelul sistemului operațional este necesar de utilizat mijloace de asigurare a securității care să asigure următoarele:

- identificarea şi verificarea calculatorului utilizatorului, a terminalului şi locației fiecărui utilizator înregistrat;
- înregistrarea acceselor reuşite şi eşuate la sistem;
- autentificarea nivelului corespunzător.

Cerințele accesului la sistemele operaționale trebuie să includă:

- posibilitatea de a utiliza identificarea automată a terminalului;
- accesul la serviciile informaționale trebuie să fie asigurat cu ajutorul unei proceduri sigure de intrare în sistem;
- accesul la comenzile sistemului operațional trebuie să fie interzis utilizatorilor care nu dispun de drepturi de administrare de sistem;
- trebuie limitat numărul de încercări de acces eşuate permise (se recomandă trei încercări);
- în caz de depăşire a numărului admis de încercări de acces eşuate, trebuie realizată blocarea terminalului şi/sau a înregistrării de evidență pentru o anumită perioadă de timp sau trebuie executate alte acțiuni care să prevină sau să creeze dificultăți substanțiale pentru accesul din partea potențialilor contravenienți;
- informația despre înregistrare trebuie să fie confirmată doar la finalizarea introducerii tuturor datelor de intrare;
- este necesar de limitat timpul maxim şi minim permis pentru procedurile de intrare în sistem;
- informația cu privire la înregistrarea efectuată cu succes trebuie să fie fixată în permanență;
- utilizarea utilităților de sistem trebuie să fie limitată şi controlată în permanență.

5.8.6. Cerințe privind controlul accesului la aplicații

Pentru a preveni accesul neautorizat la datele SI, este necesar de aplicat măsuri de asigurare a securității în vederea limitării accesului la sistemele aplicate.

Cerințele controlului accesului la aplicații trebuie să includă:

- asigurarea accesului utilizatorilor de aplicații la informație şi funcțiile acestor aplicații în conformitate cu politica de control al accesului care se bazează pe cerințele față de anumite aplicații;
- limitarea furnizării către utilizatori a informației despre datele şi funcțiile aplicațiilor pentru care

aceştia nu dispun de autorizația de acces;

- sistemele, ce procesează informații importante, trebuie să fie asigurate cu mediul de calcul separat, cu condiții speciale de exploatare.

5.8.7. Cerințe privind monitorizarea accesului

Pentru a depista acțiunile neautorizate sau devierile de la cerințele politicii de control al accesului este necesar de efectuat monitorizarea sistemului.

Cerințele privind monitorizarea accesului sînt:

- crearea registrelor de audit şi păstrarea lor în decursul perioadei de timp aprobate, în care trebuie să fie ținută evidența incidentelor de încălcare a securității şi a altor evenimente privind securitatea;
- înregistrările de audit trebuie să conțină următoarele:

1) identificatorul utilizatorilor;
2) data şi ora intrării şi ieşirii;
3) identificatorul terminalului sau al locației acestuia;
4) înregistrările încercărilor reuşite şi respinse de acces la sistem;
5) înregistrările încercărilor reuşite şi respinse de acces la date şi la alte resurse;

- stabilirea procedurilor de monitorizare a utilizării mijloacelor de procesare a informației şi de analiză a rezultatelor acestora;
- nivelul de monitorizare a mijloacelor concrete de procesare a informației trebuie să fie determinat în baza evaluării riscurilor.

5.9. Elaborarea şi mentenanța sistemelor informaționale

În procesul de elaborare şi mentenanță a SI este necesar de utilizat metode speciale care iau în considerație criteriile gradului de protecție, flexibilității şi costului şi care asigură următoarele:

- verificarea autenticității – utilizarea metodelor de verificare strictă, a politicilor parolelor, politicilor de blocare a înregistrărilor de evidență şi a cifrării;
- un sistem unic de autorizare – care trebuie să se bazeze pe modelul de permisiuni şi să asigure un grad înalt de detaliere a controlului accesului;
- delimitarea drepturilor de acces – politica ce permite gestionarea accesului la resursele informaționale, sisteme şi operații protejate;
- prevenirea citirii mesajelor de către persoane terțe;
- protecția traficului de date contra analizării acestora de către persoane terțe;
- depistarea modificărilor în fluxurile de mesaje;
- depistarea denaturărilor de date.

Cerințele privind elaborarea şi mentenanța SI includ:

- cerințe privind arhitectura securității:

1) trebuie determinate mijloacele de securitate cu ajutorul cărora se va asigura securitatea serviciilor publice prestate;
2) trebuie de aplicat protocoale de asigurare a autenticității şi confidențialității în două regimuri: regimul de transport (protecția doar a conținutului pachetelor şi a anumitor cîmpuri de titluri) şi regimul de tunelare (protecția întregului pachet);
3) este necesar de utilizat mecanisme de gestionare a mijloacelor de protecție criptografică a informației (algoritmele de cifrare, de control al integrității şi autenticității);

- cerințele de securitate în cadrul sistemelor aplicate:

1) este necesar de efectuat controlul şi de ținut evidența instalării şi înlăturării mijloacelor software, hardware şi soft-hardware ale sistemelor;
2) trebuie efectuată verificarea corectitudinii introducerii datelor în vederea asigurării certitudinii că acestea corespund datelor inițiale;
3) trebuie efectuat controlul asupra procesării datelor în sisteme;

4) pentru aplicațiile în cadrul cărora trebuie de asigurat protecția integrității conținutului mesajelor este necesar de utilizat autentificarea mesajelor;

5) trebuie efectuată testarea de securitate a tuturor sistemelor utilizate;

6) de asemenea, trebuie efectuată verificarea independentă a funcționării sistemelor;

- cerințe privind controlul modificărilor:

1) este necesar de controlat cu strictețe implementarea modificărilor;

2) este necesar de acordat programatorilor responsabili de mentenență accesul doar la porțiunile din sistem care sînt necesare pentru munca lor;

3) trebuie asigurată protocolarea nivelurilor de autorizare aprobate;

4) trebuie efectuat controlul versiunilor pentru toate actualizările software-ului;

5) în registrele de audit trebuie înregistrate toate solicitările de modificare;

6) trebuie efectuată analiza mijloacelor de control al aplicațiilor şi procedurilor de integritate pentru a asigura garanția că acestea nu au fost compromise de modificările din sistemul operațional;

7) trebuie asigurată recepționarea la timp a notificărilor despre modificările din sistemul operațional;

8) trebuie evitată modificarea pachetelor de program;

- cerințe privind aplicarea mijloacelor de protecție criptografică a informației:

1) trebuie stabilite metodele de utilizare a mijloacelor criptografice în cadrul instituției, inclusiv principiile generale şi metodele de restabilire a informației cifrate în caz de pierdere, compromitere sau deteriorare a cheilor;

2) trebuie stabilite nivelurile corespunzătoare de protecție criptografică pentru diferite date;

3) pentru a asigura protecția informației confidențiale sau critice, trebuie aplicată metoda criptografică de cifrare, ținîndu-se cont de tipul şi calitatea algoritmului de cifrare utilizat, precum şi de lungimea cheilor criptografice;

4) pentru a asigura protecția autentificării şi integrității documentelor electronice este necesar de aplicat semnăturile digitale;

5) la utilizarea semnăturilor digitale este necesar de ținut cont de cerințele prevăzute de legislația în vigoare, care stabilesc condițiile în care semnătura digitală obține forță juridică;

6) cheile criptografice trebuie protejate împotriva modificărilor şi distrugerii, iar cheile secrete şi personale trebuie protejate împotriva dezvăluirii neautorizate.

5.10. Managementul continuității activității

Continuitatea activității instituției trebuie asigurată în scopul minimalizării consecințelor negative, cauzate de calamități şi încălcările securității, pînă la un nivel admisibil cu ajutorul unor combinări între activitățile profilactice şi de restabilire ce țin de managementul securității.

Cerințele privind managementul continuității trebuie să includă:

- elaborarea şi documentarea strategiei de asigurare a continuității, precum şi planurilor de asigurare a continuității şi de restabilire a activității;

- utilizarea sistemelor adecvate de rezervare şi restabilire;

- cerințe la planurile de continuitate şi restabilire a activității:

1) planurile trebuie să includă stabilirea persoanelor responsabile şi acțiunilor executate de acestea în caz de restabilire a SI de prestare a serviciilor publice după producerea deranjamentului sau refuzului;

2) planurile trebuie să fie examinate de persoanele cu funcții de răspundere corespunzătoare, aprobate, multiplicate în cantitate necesară şi adresate persoanelor responsabile de acțiunile întreprinse în situațiile neprevăzute;

3) planurile trebuie să fie revizuite şi reînnoite periodic, luîndu-se în considerație modificările sau problemele apărute în rezultatul verificării sau realizării planului;

4) personalul trebuie să fie instruit (reinstruit – cu o periodicitate stabilită) în materie de roluri, responsabilitate şi obligaţii ce îi revin în procesul de executare a acţiunilor în situaţiile neprevăzute;

5) în procesul de instruire a personalului trebuie să se modeleze evenimentele corespunzătoare, ceea ce va ajuta pe viitor personalul să execute în mod eficient acţiunile cerute în caz de survenire a situaţiilor de criză;

6) este necesar de utilizat mijloace automatizate pentru a asigura un mediu de instruire mai complex şi real;

- cerinţe privind verificarea planurilor de continuitate şi restabilire a activităţii:

1) trebuie efectuată testarea periodică a planurilor în scopul evaluării eficienţei acestora şi pregătirii personalului pentru executarea acţiunilor prevăzute în plan;

2) persoanele cu funcţii de răspundere corespunzătoare trebuie să studieze rezultatele testării planurilor şi în caz de necesitate să iniţieze corectarea acestora;

3) trebuie utilizate mijloace automatizate pentru testarea mai minuţioasă şi eficientă a acţiunilor de asigurare a continuităţii şi de restabilire a activităţii;

- cerinţe privind locaţiile de rezervă pentru procesarea informaţiei:

1) trebuie determinate locaţiile de rezervă pentru procesarea informaţiei şi soluţionate aspectele administrative privind procesarea informaţiei pentru sarcinile de importanţă critică pînă la restabilirea posibilităţilor de procesare a informaţiei;

2) locaţiile de rezervă de procesare a informaţiei trebuie să fie delimitate (geografic) în spaţiu de locaţiile de bază pentru procesarea informaţiei pentru a nu fi supuse unor pericole identice;

3) trebuie determinate problemele potenţiale privind accesibilitatea locaţiilor de rezervă pentru procesarea informaţiei în caz de deranjament sau accident şi trebuie stabilite acţiunile concrete în vederea restabilirii accesibilităţii;

4) la utilizarea locaţiilor de rezervă pentru procesarea informaţiei trebuie luate în consideraţie priorităţile de deservire stabilite;

5) locaţia de rezervă pentru procesarea informaţiei trebuie să fie configurată astfel încît să asigure minimumul necesar de posibilităţi exploataţionale;

- cerinţe privind rezervarea serviciilor de telecomunicaţii:

1) este necesar de identificat serviciile de telecomunicaţii de bază şi de rezervă şi de soluţionat aspectele administrative privind utilizarea serviciilor de telecomunicaţii de rezervă pentru sarcinile de importanţă critică pînă la restabilirea accesibilităţii celor de bază;

2) la utilizarea serviciilor de telecomunicaţii de bază şi de rezervă trebuie luate în consideraţie priorităţile de deservire stabilite;

3) furnizorii de servicii de telecomunicaţii de bază şi de rezervă trebuie să fie separaţi între ei în modul corespunzător pentru a nu fi supuşi unora şi aceleaşi pericole identice;

4) furnizorii de servicii de telecomunicaţii de bază şi de rezervă trebuie să dispună de planuri de acţiuni corespunzătoare pentru situaţiile neprevăzute;

- cerinţe privind restabilirea sistemului:

1) trebuie utilizate mecanisme şi proceduri de susţinere a acestora, necesare pentru restabilirea sistemului după deranjament sau refuz;

2) restabilirea sistemului după deranjament sau refuz trebuie să fie utilizată ca o parte componentă a verificării planului de acţiuni pentru situaţii neprevăzute.

5.11. Conformitatea

Pentru a preveni orice încălcare a normelor legislaţiei în vigoare, a prevederilor obligatorii şi a cerinţelor de reglementare sau a obligaţiunilor contractuale, precum şi a cerinţelor securităţii, este necesar de efectuat controlul conformităţii în calitate de monitorizare şi audit al securităţii.

5.11.1. Cerinţe privind monitorizarea securităţii

Monitorizarea securității trebuie să asigure controlul permanent asupra menținerii nivelului necesar de securitate în procesul prestării serviciilor publice.

Monitorizarea securității trebuie să permită depistarea modificării:

- funcțiilor realizate în procesul de prestare a serviciilor – monitorizarea funcțiilor trebuie să fie orientată spre identificarea necesității de modificare a categoriei resurselor în legătură cu modificarea prejudiciului eventual, cauzat prin încălcarea securității;
- resurselor – monitorizarea resurselor trebuie să fie orientată spre depistarea modificărilor în cadrul informației, hardware-ului şi software-ului, care pot servi drept cauză pentru modificarea conținutului punctelor vulnerabile şi pericolelor de încălcare a securității;
- pericolelor şi vulnerabilităților – monitorizarea vulnerabilităților şi pericolelor securității trebuie să fie orientată spre depistarea la timp a vulnerabilităților şi pericolelor care pot spori riscul încălcării securității în procesul de prestare a serviciilor;
- măsurilor şi mijloacelor de asigurare a securității – monitorizarea măsurilor şi mijloacelor de asigurare a securității trebuie să fie orientată spre controlul menținerii eficienței acestora pentru a contracara vulnerabilitățile şi pericolele stabilite şi depistate.

Monitorizarea securității în activitatea de prestare a serviciilor trebuie să includă:

- controlul curent al stării securității – trebuie să asigure certitudinea că măsurile şi mijloacele de asigurare a securității funcționează, nu sînt compromise, iar securitatea sistemului de prestare a serviciilor publice nu a fost încălcată. În acest scop, este necesar de executat următoarele acțiuni:

1) controlul realizării măsurilor permanent active de asigurare a securității;
2) controlul capacității de lucru a mijloacelor de asigurare a securității;
3) controlul integrității resurselor şi sistemelor informaționale;
4) depistarea şi lichidarea invaziilor (încălcarea drepturilor de acces, atacurilor de viruşi, spam).

De asemenea, toate încălcările de securitate identificate în procesul prestării serviciilor publice trebuie să fie fixate, cercetate şi lichidate imediat cu ajutorul diferitor măsuri şi mijloace de protecție a informației.

- evaluarea securității – trebuie să asigure certitudinea că sistemul de prestare a serviciilor este în corespundere cu cerințele securității şi politica de securitate. Evaluarea securității trebuie efectuată periodic, conform termenelor, dar nu mai puțin de o dată în an, precum şi în caz de modificări esențiale în cadrul resurselor, pericolelor securității şi politicii de securitate. La evaluarea securității procesului de prestare a serviciilor publice urmează să fie evaluate:

1) conformitatea măsurilor şi mijloacelor de asigurare a securității cu cerințele stabilite în politica securității;
2) corectitudinea aplicării măsurilor şi mijloacelor de asigurare a securității în conformitate cu politica securității;
3) corectitudinea acțiunilor privind lichidarea consecințelor incidentelor de încălcare a securității şi neutralizarea vulnerabilităților.

Pentru a primi datele despre starea securității sistemului de prestare a serviciilor este necesar de utilizat următoarele:

- analiza documentelor privind evidența aplicării măsurilor şi mijloacelor de asigurare a securității;
- sondaje în rîndurile personalului care participă în procesul de prestare a serviciilor publice;
- analiza eficienței măsurilor şi mijloacelor de asigurare a securității pentru a contracara incidentele de încălcare a securității care s-au produs;
- verificări şi testări ale măsurilor şi mijloacelor de asigurare a securității privind conformitatea cu cerințele securității;
- testări de intruziune privind evaluarea posibilității de utilizare a vulnerabilităților pentru

încălcarea securității;

- mijloace hardware şi software specializate pentru efectuarea controlului stării mijloacelor de asigurare a securității şi depistarea vulnerabilităților;
- datele evaluărilor securității anterioare.

În baza rezultatelor evaluării efectuate, în caz de depistare a deficiențelor în asigurarea securității sistemului de prestare a serviciilor este necesar de îndeplinit următoarele acțiuni, în funcție de importanța deficiențelor:

- precizarea măsurilor şi mijloacelor de asigurare a securității;
- ajustarea politicii de securitate;
- evaluarea riscului şi ajustarea cerințelor securității la prestarea serviciilor.

5.11.2. Cerințe privind auditul securității

Auditul securității reprezintă un proces complex de obținere şi evaluare a unor date obiective despre starea curentă a SI, din punct de vedere al securității, acțiuni şi evenimente ce au loc în cadrul acestuia, proces care stabileşte gradul de conformitate al acestora cu un anumit nivel de securitate.

Scopul auditului securității pentru o instituție ce prestează servicii publice este:

- obținerea unei evaluări cît mai complete şi obiective a protecției;
- localizarea problemelor existente şi elaborarea unui sistem eficient de asigurare a securității instituției.

La efectuarea auditului securității în cadrul unei instituții care prestează servicii publice pot fi utilizate diferite tipuri de audit în domeniul securității informației, care diferă între ele doar prin scop, iar metoda de efectuare este identică:

- cercetarea inițială (auditul primar) – rezultatul este concepția securității instituției, care va permite edificarea unei protecții adecvate a informației;
- cercetarea anteproiect (auditul tehnic) – rezultatul este ansamblul de cerințe față de sistemul de asigurare a securității;
- atestarea obiectului – rezultatul este documentul, certificatul de conformitate, care demonstrează că obiectul este conform cu standardul şi legislația națională în vigoare, sau concluzia expertului;
- examinarea de control – examinarea de control conform planului în vederea verificării respectării regulilor de asigurare a securității.

Procesul de efectuare a auditului securității în cadrul instituției trebuie să includă următoarele etape:

- formularea sarcinilor şi precizarea limitelor lucrărilor – trebuie efectuate o analiză prealabilă şi activități organizaționale de pregătire a efectuării auditului securității;
- colectarea şi analiza informației – trebuie colectată informația şi trebuie evaluate următoarele măsuri şi mijloace: măsurile organizaționale în domeniul securității, mijloacele software şi hardware de protecție a informației, de asigurare a securității fizice;
- efectuarea analizei riscurilor şi evaluării conformității sistemului cu cerințele şi standardele înaintate – trebuie efectuate clasificarea resurselor, analiza vulnerabilităților, crearea modelului răufăcătorului potențial, evaluarea riscurilor încălcării securității;
- elaborarea recomandărilor şi propunerilor cu privire la măsurile de sporire a securității:

1) recomandări privind perfecționarea sistemului de protecție a informației, a căror aplicare va permite minimalizarea riscurilor;
2) aplicații cu lista vulnerabilităților concrete;
3) raportul final ce conține evaluarea nivelului curent al securității;
4) informația despre erorile depistate;
5) analiza riscurilor corespunzătoare şi a recomandărilor privind lichidarea acestora.

Auditul securității în cadrul instituției permite obținerea unei evaluări obiective şi independente a

stării curente a protecției resurselor, estimarea riscurilor care admit probabilitatea realizării pericolelor, precum şi prejudiciul potențial cauzat SI de aceste riscuri.

Cerințele privind auditul securității în procesul de prestare a serviciilor publice trebuie să includă:

- elaborarea, documentarea şi reînnoirea periodică a politicii de audit şi asigurare a raportării (politica înregistrării şi evidenței), precum şi procedurile şi măsurile privind realizarea politicii de audit şi asigurare a raportării;
- trebuie efectuată generarea înregistrărilor de audit pentru evenimentele indicate în lista evenimentelor supuse auditului;
- este necesar de pus la dispoziție mențiuni despre timp pentru generarea înregistrărilor de audit;
- în fiecare înregistrare de audit trebuie indicată următoarea informație: data şi ora evenimentului, tipul evenimentului, identificatorul subiectului şi rezultatul evenimentului (reuşit sau eşuat), precum şi informații suplimentare;
- fiecare eveniment potențial supus auditului trebuie să fie asociat cu identificatorul utilizatorului care a fost inițiatorul evenimentului respectiv;
- administratorul autorizat trebuie să dispună de posibilitatea de a citi toată informația auditului din înregistrările de audit, adică trebuie să existe accesul la registrul de audit;
- accesul la citirea înregistrărilor de audit trebuie să fie interzisă utilizatorilor, cu excepția utilizatorilor cărora accesul evident le este permis;
- trebuie oferită posibilitatea de a efectua căutarea, sortarea şi structurarea datelor auditului bazate pe identificatorul utilizatorului şi destinație;
- trebuie să existe posibilitatea de a include evenimentele ce pot fi supuse în mod potențial auditului în totalitatea de evenimente supuse auditului sau excluderii lor din această totalitate în baza identificatorului utilizatorului sau a destinației;
- înregistrările de audit stocate trebuie să fie protejate contra lichidării nesancționate, trebuie să poată preveni modificarea înregistrărilor de audit;
- trebuie stabilită perioada de timp în decursul căreia datele auditului urmează a fi păstrate pentru a se asigura cercetarea incidentelor de securitate, precum şi respectarea cerințelor normative cu privire la păstrarea datelor auditului;
- este necesar de generat notificări despre pericol către administratorul autorizat în cazul cînd registrul de audit depăşeşte restricțiile stabilite;
- trebuie să existe posibilitatea de a preveni pierderile de evenimente supuse auditării în caz de finisare a registrului;
- cerințe privind volumul de memorie acordat pentru păstrarea datelor auditului:

1) trebuie de acordat volumul de memorie suficient pentru păstrarea datelor auditului;

2) trebuie de efectuat setările necesare astfel încît volumul datelor auditului să nu depăşească volumul memoriei acordat;

- cerințe privind procesarea datelor auditului:

1) în caz de survenire a unui deranjament în cadrul auditului sau în caz de ocupare a întregului volum de memorie acordat pentru păstrarea datelor auditului, este necesar de adresat o notificare către persoanele cu funcții de răspundere corespunzătoare şi de întreprins acțiunile stabilite, precum sînt: finalizarea lucrului sistemului, ignorarea evenimentelor supuse auditării, înregistrarea prin înlăturarea celor mai vechi înregistrări de audit păstrate;

2) în caz de completare a procentului sau volumului stabilit de memorie acordat pentru păstrarea datelor auditului, este necesar de adresat o notificare corespunzătoare;

- cerințe privind monitorizarea, analiza şi generarea rapoartelor despre rezultatele auditului:

1) este necesar de vizualizat şi de analizat în mod regulat înregistrările de audit în scopul depistării unor activități neordinare sau suspecte, de elaborat rapoartele respective pentru persoanele

cu funcții de răspundere şi de efectuat acțiunile stabilite pentru astfel de cazuri;

2) este necesar de utilizat mijloace automatizate care să permită unirea monitorizării, analizei şi generării rapoartelor într-un singur proces de analiză a activităților suspecte şi de reacționare în caz de încălcări potențiale;

- cerințe privind limitarea volumului datelor auditului:

1) trebuie realizate posibilitățile de limitare a volumului datelor auditului şi de generare a rapoartelor corespunzătoare;

2) trebuie realizată posibilitatea procesării automate a înregistrărilor de audit pentru anumite tipuri de evenimente;

- trebuie asigurată protecția datelor auditului şi a mijloacelor de efectuare a auditului contra accesului neautorizat;

- trebuie realizată posibilitatea asigurării negării (de stabilit dacă un anumit utilizator a efectuat acțiunea respectivă).

5.11.3. Cerințe privind controlul de stat

Pe lîngă auditul securității în cadrul instituției care prestează servicii publice este necesar de efectuat controlul de stat asupra respectării cerințelor securității TI, care să fie realizat de către organele abilitate în scopul prevenirii şi depistării încălcărilor cerințelor de securitate. În procesul realizării controlului de stat organele abilitate sînt în drept:

- să solicite de la instituția care prestează servicii publice documentele care demonstrează conformitatea procesului de exploatare a SI cu cerințele de securitate;

- să emită prescripții privind lichidarea încălcărilor cerințelor obligatorii de securitate în termenul stabilit în funcție de natura încălcării;

- în urma deciziei instanței de judecată să adopte decizii motivate cu privire la suspendarea deplină sau parțială a procesului de exploatare a SI de prestare a serviciilor în cazul cînd este imposibil de a lichida încălcarea cerințelor securității cu ajutorul altor măsuri;

- să suspende sau să înceteze acțiunea certificatului de conformitate;

- să întreprindă alte măsuri prevăzute de legislație în scopul neadmiterii încălcării cerințelor de securitate.

Organele abilitate să efectueze controlul de stat sînt obligate:

- în procesul activităților de control de stat să ofere explicații cu privire la aplicarea cerințelor legislației în domeniul securității TI;

- să respecte procedura stabilită pentru protecția informației în funcție de gradul de criticitate şi importanță al acesteia;

- să respecte procedura stabilită pentru realizarea activităților de control de stat şi perfectarea rezultatelor acestor activități;

- în baza rezultatelor activităților de control de stat să întreprindă măsuri de lichidare a consecințelor încălcării cerințelor de securitate şi regulilor de evaluare a conformității.

5.12. Managementul securității informației la atragerea organizațiilor terțe

În procesul prestării serviciilor publice pot fi implicați:

- colaboratorii organizațiilor terțe care deservesc complexul de software şi hardware;

- partenerii care ar putea avea nevoie de schimb de informație sau de acces la resursele instituției.

La atragerea persoanelor terțe este necesar de respectat următoarele cerințe:

- este necesar de identificat riscurile legate de resursele şi procesele care implică persoane terțe;

- înainte de acordarea accesului colaboratorilor organizațiilor terțe la resurse şi procese este necesar de realizat măsuri şi mijloace corespunzătoare de asigurare a securității;

- trebuie controlat accesul organizației terțe la mijloacele de procesare a informației;

- contractele în baza cărora este asigurat accesul organizațiilor terțe trebuie să includă procedura

de stabilire a drepturilor şi condiţiilor de acces ale altor participanţi;

- reprezentanţii organizaţiei terţe trebuie să semneze un acord de respectare a confidenţialităţii înainte de a primi accesul la resursele şi mijloacele de procesare a informaţiei;
- în acordurile de confidenţialitate trebuie stabilită responsabilitatea părţilor, în conformitate cu cerinţele securităţii şi legislaţiei în vigoare;
- în contractul încheiat cu persoana terţă este necesar de acordat atenţie specială următoarelor aspecte:

1) nivelul serviciilor prestate;
2) aspectele juridice, conformitatea cu cerinţele prevăzute de legislaţie (de exemplu asigurarea integrităţii datelor personale);
3) repartizarea răspunderii, incluzînd răspunderea subantreprenorilor persoanei terţe;
4) asigurarea caracterului confidenţial, a integrităţii şi disponibilităţii informaţiei procesate, stocate şi transmise;
5) toate cerinţele de securitate legate de accesul persoanei terţei, inclusiv măsurile şi mijloacele de asigurare a securităţii şi controlului;
6) serviciile şi activităţile care vor fi menţinute în caz de survenire a unor situaţii excepţionale;

- este necesar de garantat faptul că mijloacele de asigurare a securităţii incluse în contractul de prestare a serviciilor organizaţiei terţe sînt realizate, exploatate şi susţinute de către organizaţia terţă în modul corespunzător;
- serviciile, rapoartele şi înregistrările prezentate de organizaţia terţă trebuie să fie controlate şi analizate în permanenţă;
- în procesul de elaborare a software-ului cu implicarea organizaţiei terţe este necesar de aplicat următoarele măsuri de control:

1) controlul existenţei contractelor de licenţă şi al clarităţii în materia dreptului de proprietate asupra software-ului şi respectării drepturilor de proprietate intelectuală;
2) verificarea valabilităţii certificării calităţii şi corectitudinii executării lucrărilor;
3) controlul asupra asigurării drepturilor de acces pentru audit în scopul verificării calităţii şi corectitudinii lucrărilor executate;
4) controlul asupra documentării cerinţelor privind calitatea programelor în formă contractuală;
5) verificarea procesului de testare înainte de instalarea software-ului.

6. Sisteme de asigurare a securităţii

Asigurarea securităţii resurselor instituţiei în procesul de prestare a serviciilor publice este pusă în sarcina sistemului de asigurare a securităţii. Pentru a realiza scopurile şi a soluţiona problemele ce ţin de asigurarea securităţii în procesul de prestare a serviciilor publice este necesar de utilizat cel puţin trei clase de sisteme de asigurare a securităţii:

- sisteme de securitate de bază – sisteme comune care stau la baza realizării multor altor sisteme de securitate;
- sisteme de prevenire a încălcărilor securităţii – sisteme de securitate orientate spre prevenirea diferitor încălcări ale securităţii în procesul de prestare a serviciilor;
- sisteme de depistare a încălcărilor şi de restabilire a securităţii – aceste sisteme trebuie orientate spre soluţionarea problemelor ce ţin de depistarea încălcărilor securităţii în procesul prestării serviciilor publice (înainte şi după realizarea acestora) şi de restabilirea sistemului de prestare a serviciilor în stare de siguranţă.

6.1. Sisteme de securitate de bază

Sistemele de securitate de bază trebuie să reprezinte baza, mediul de legătură pentru edificarea tuturor celorlalte sisteme de securitate. La această clasă sînt atribuite următoarele sisteme de securitate:

- sistemul de identificare – pentru realizarea majorității sistemelor de securitate este necesară identificarea unică a obiectelor şi subiectelor în procesul de prestare a serviciilor publice. Sistemul de identificare trebuie să asigure posibilitatea atribuirii identificatorului unic utilizatorilor, proceselor, SI, resurselor informaționale şi altor resurse din SI;

- sistemul de protecție criptografică – acest sistem este obligatoriu pentru asigurarea securității procesului de prestare a serviciilor publice. Sistemul de protecție criptografică trebuie să includă metodele şi mijloacele speciale (hardware, software şi soft-hardware) de transformare a informației, care sînt utilizate pentru protecția integrității şi confidențialității informației şi a datelor;

- sistemul de management al securității şi de administrare. Sistemul de management al securității include distribuirea şi managementul informației necesare pentru funcționara sistemelor şi mecanismelor de securitate în vederea asigurării securității în procesul de prestare a serviciilor. Sistemul de administrare include procesele de setare a parametrilor instalării şi exploatării software-ului şi hardware-ului din cadrul sistemelor de securitate în procesul de prestare a serviciilor, precum şi evidența modificărilor introduse în echipamentul utilizat.

Este necesar de stabilit obligațiile privind managementul echipamentului de procesare a informației şi exploatarea acestui echipament.

Toate sistemele de securitate de bază asigură protecția sistemului, care reprezintă o totalitate de proprietăți ale sistemului ce permit încrederea în realizarea tehnică a sistemului de asigurare a securității. Exemple de măsuri şi mijloace de protecție a sistemului sînt următoarele:

- protecția informației contra utilizării repetate;
- minimalizarea drepturilor de acces;
- divizarea proceselor;
- divizarea responsabilității;
- modularitatea şi etapele de elaborare;
- minimalizarea cercului de persoane informate.

Este necesar de examinat nu doar calitatea mijloacelor de protecție a sistemului de prestare a serviciilor realizate, dar şi procedurile de elaborare a acestora, metodele de realizare şi soluționare a sarcinilor tehnice.

6.2. Sisteme de prevenire a încălcărilor securității

Sistemele de prevenire a încălcării securității trebuie să asigure securitatea obiectelor protejate contra acțiunilor calificate drept invazie sau încălcare a securității.

La clasa respectivă sînt atribuite următoarele sisteme:

- sistemul de telecomunicații protejate (canale de comunicații). În cadrul sistemului de prestare a serviciilor publice asigurarea unei protecții sigure depinde în mare măsură de protecția canalelor de comunicații. Sistemul de protecție a canalelor de comunicații trebuie să asigure integritatea, confidențialitatea şi accesibilitatea informației în procesul de transmitere a acesteia prin canalele de comunicații. Măsurile şi mijloacele de asigurare a securității trebuie să asigure protecția contra distrugerii, substituirii, modificării şi transmiterii repetate al datelor şi contra altor tipuri de acțiuni premeditate;

- sistemul de autentificare reprezintă cel mai important sistem de securitate, în special în cadrul sistemului de prestare a serviciilor publice. Sistemul de autentificare execută procedura de verificare a autenticității subiectului care permite stabilirea cu certitudine a faptului că subiectul care şi-a prezentat identificatorul este într-adevăr subiectul, al cărui identificator îl utilizează. Metodele de identificare trebuie să fie aplicate pentru utilizatorii de toate categoriile, inclusiv pentru personalul de asistență tehnică, operatori, administratori de rețea, programatori de sistem, administratori de baze de date;

- sistemul de autorizare este orientat spre acordarea (atribuirea) subiecților anumitor împuterniciri

legate de acțiunile executate de aceştia în cadrul SI de prestare a serviciilor publice;

- sistemul de management al accesului este sistemul calificat ca fiind „prevenirea utilizării neautorizate a resurselor, inclusiv prevenirea utilizării resurselor prin metode inadmisibile”. Sistemul trebuie să fie utilizat pentru diverse tipuri de acces la resursele şi sistemele informaționale, de exemplu utilizarea resurselor comunicaționale, citirea, înregistrarea sau lichidarea resurselor informaționale, utilizarea resurselor sistemelor informaționale de procesare a datelor. Politica de management al accesului trebuie să servească drept bază pentru politica de securitate a TI, care trebuie să cuprindă toate etapele de acces al utilizatorilor, începînd cu înregistrarea inițială a noilor utilizatori pînă la anularea finală a înregistrării pentru utilizatorii care nu mai au nevoie de accesul la SI şi la servicii.

Sistemele de prevenire a încălcărilor securității în procesul de prestare a serviciilor publice trebuie să asigure confidențialitatea, integritatea şi accesibilitatea informației, precum şi negarea şi caracterul secret al tranzacțiilor.

Negarea (dovada apartenenței) reprezintă „prevenirea posibilității refuzului unora din participanții reali ai comunicațiilor de faptul participării depline sau parțiale la transmiterea datelor”. Este necesar de utilizat două forme de negare: negarea de la expedierea mesajului (dovada sursei) şi confirmarea (dovada) primirii mesajelor. Negarea este necesară pentru prevenirea şi depistarea încălcărilor securității în cadrul SI de prestare a serviciilor. Măsurile şi mijloacele de asigurare a negării trebuie să prevină posibilitatea refuzului acțiunilor executate.

Caracterul secret al tranzacțiilor în cadrul SI de prestare a serviciilor publice semnifică respectarea cerințelor de asigurare a caracterului secret al persoanei care utilizează resursele şi sistemele informaționale. Caracterul secret reprezintă protecția contra divulgării informației (datelor) despre identitatea utilizatorului care foloseşte resursele şi sistemele informaționale. Caracterul secret al tranzacțiilor trebuie să asigure protecția contra pierderii negării pe calea analizei acțiunilor, operațiilor efectuate de utilizatori în sistemul de prestare a serviciilor publice.

6.3. Sisteme de depistare a încălcărilor şi de restabilire a securității

Sistemele de depistare a încălcărilor şi de restabilire a securității trebuie să includă serviciile de depistare a încălcărilor securității orientate spre consolidarea serviciilor de prevenire, precum şi crearea şi testarea regulată a copiilor de rezervă ale datelor şi software-ului.

Pentru a depista încălcările securității SI de prestare a serviciilor publice este necesar de utilizat următoarele sisteme:

- sistemul de audit al securității, orientat spre depistarea evenimentelor care influențează securitatea SI, asigurarea reacționării sistemului la invaziile depistate, precum şi spre asigurarea formării datelor necesare pentru restabilirea ulterioară a SI în starea de siguranță. În cadrul auditului securității este necesar de examinat diferite sisteme şi mecanisme de securitate care asigură protecția informației în procesul de prestare a serviciilor publice.

Mecanismele de audit trebuie să soluționeze următoarele sarcini:

1) asigurarea subordonării utilizatorilor şi administratorilor, ceea ce reprezintă un mijloc de reținere a tentativelor de încălcare a securității informaționale. Unul din mecanismele importante de securitate pentru asigurarea subordonării sînt mecanismele de identificare şi autentificare, precum şi mecanismele de management al accesului pentru asigurarea caracterului confidențial şi a integrității informației ce urmează să fie raportată;

2) asigurarea posibilității de restabilire a consecutivității evenimentelor, ceea ce permite depistarea aspectelor vulnerabile în protecția informației, identificarea persoanei vinovate de invazie, evaluarea proporțiilor prejudiciului cauzat şi returnarea la regimul normal de activitate;

3) furnizarea informației pentru identificarea şi analiza problemelor prin întocmirea rapoartelor corespunzătoare;

- sistemul de depistare a incidentelor şi politica de reţinere. Sistemul de depistare a incidentelor trebuie să fie orientat spre depistarea atît a tentativelor de încălcare a securităţii, cît şi spre înregistrarea activităţii legitime a utilizatorilor. Depistarea trebuie să fie locală şi/sau la distanţă, şi trebuie să fie realizată prin intermediul semnalizării de alarmă a incidentelor, înregistrarea evenimentelor şi acţiunilor de restabilire. Pentru a reduce consecinţele reale şi potenţiale ale incidentelor, politica de reţinere a incidentelor potenţiale trebuie să includă raportul de incident, contracţiunii de minimalizare a riscurilor şi prioritatea lor;

- sistemul de control al integrităţii componentelor software, hardware şi informaţionale ale SI trebuie să fie orientat spre depistarea la timp a încălcărilor integrităţii;

- sistemul de restabilire a securităţii trebuie să îndeplinească funcţia de reacţie a SI la încălcarea securităţii. Sistemul de restabilire a securităţii trebuie să fie realizat prin executarea acţiunilor, precum sînt: deconectarea imediată sau stoparea funcţionării, refuzul de a acorda acces subiectului, privarea temporară de drepturi a subiectului, introducerea subiectului în „lista neagră”.

7. Cerinţe minime de securitate la prestarea serviciilor publice

La crearea sistemului de asigurare a securităţii este necesar de a se baza pe profilurile de protecţie, ceea ce va permite asigurarea unei protecţii sigure a tuturor resurselor şi proceselor din cadrul instituţiei.

Profilurile de protecţie trebuie să caracterizeze anumite măsuri şi mijloace de asigurare a securităţii, de combinare a unor activităţi similare. În cadrul profilurilor de protecţie trebuie să fie incluse următoarele măsuri şi mijloace de bază de asigurare a securităţii:

- identificarea şi autentificarea;
- managementul accesului;
- protocolarea şi auditul;
- cifrarea;
- controlul integrităţii;
- ecranarea;
- analiza protecţiei;
- asigurarea negării;
- asigurarea restabilirii sigure;
- tunelarea.

La crearea sistemului complex de securitate informaţională în procesul prestării serviciilor publice trebuie să fie utilizate următoarele profiluri de protecţie:

- acces controlat;
- protecţia prin marcare;
- sisteme operaţionale;
- sisteme operaţionale cu un singur nivel;
- sisteme operaţionale cu multe niveluri;
- sisteme de management al bazelor de date.

Toate cerinţele profilurilor de protecţie trebuie să fie divizate în următoarele:

- cerinţe funcţionale ce corespund aspectului activ al protecţiei şi care sînt înaintate faţă de funcţiile de securitate a sistemului de prestare a serviciilor publice şi mecanismele de realizare a acestora;

- cerinţe de încredere, care corespund aspectului pasiv, sînt înaintate faţă de tehnologia şi procesul de elaborare şi exploatare a sistemului de prestare a serviciilor publice.

Cerinţele de încredere a securităţii trebuie să cuprindă tot ciclul de viaţă al prestării serviciilor publice. Cerinţele de încredere presupun îndeplinirea următoarelor acţiuni:

- evaluarea sarcinilor privind securitatea şi a profilurilor de protecţie care au devenit surse ale

cerințelor securității;
- verificarea proceselor şi procedurilor securității, aplicarea acestora;
- analiza documentației;
- verificarea dovezilor prezentate;
- analiza testelor şi rezultatele lor;
- analiza punctelor vulnerabile;
- efectuarea testării independente.

7.1. Profilul de protecție „Acces controlat”

Profilul de protecție „Acces controlat” este destinat pentru formularea cerințelor față de mecanismele de protecție care realizează, în special, principiul discreționar (selectiv) de control al accesului. Profilul de protecție cu acces controlat stabileşte un set de cerințe funcționale şi cerințe de încredere pentru SI de prestare a serviciilor publice. Accesul controlat susține managementul accesului care permite limitarea acțiunii unor anumiți utilizatori şi accesul la resursele şi sistemele informaționale.

Scopurile securității profilului de protecție „Acces controlat” sînt:
- asigurarea accesului la resursele şi sistemele informaționale doar pentru utilizatorii autorizați;
- managementul accesului la resurse pentru a stabili care resurse pot fi accesibile utilizatorilor;
- protocolarea acțiunilor utilizatorilor în SI în procesul prestării serviciilor publice;
- asigurarea nedivulgării oricărei informații conținute în resursa protejată, în procesul de redistribuire a acesteia.

Cerințele de securitate în procesul prestării serviciilor profilului de protecție „Acces controlat” trebuie să fie divizate în cerințe funcționale şi cerințe de încredere, care contribuie la realizarea scopurilor acestui profil al securității.

7.1.1. Cerințe funcționale pentru profilul de protecție „Acces controlat”

7.1.1.1. Cerințe privind protecția datelor utilizatorilor la prestarea serviciilor publice

Cerințele privind protecția datelor utilizatorului la prestarea serviciilor publice sînt:
- trebuie realizată politica managementului discreționar (selectiv) al accesului pentru utilizatori şi al tuturor operațiilor între subiecți şi obiecte (determinarea limitelor managementului);
- cerințe privind managementul accesului, bazat pe atributele securității:

1) trebuie să existe posibilitatea de a compara operațiile permise şi interzise cu identificatorii unui sau mai multor utilizatori;

2) trebuie să existe posibilitatea de a utiliza operații permise şi interzise predefinit;

3) pentru fiecare operație trebuie să fie setate regulile de utilizare predefinit a atributelor de permitere, determinate în atributele de management al accesului la obiect;

4) este necesar de permis sau de refuzat în mod clar accesul subiecților la obiecte în baza regulilor;

- trebuie realizat un pachet de programe-test la lansarea inițială, periodic în timpul funcționării în regim normal sau la solicitarea administratorului autorizat pentru a demonstra corectitudinea îndeplinirii cerințelor de securitate;
- trebuie susținut domeniul securității pentru executare proprie, care să protejeze contra intruziunilor şi denaturărilor din partea subiecților neautorizați;
- trebuie furnizate mențiuni temporale sigure de utilizare proprie, deoarece generarea înregistrărilor de audit depinde de corectitudinea prezentării interne a datei şi orei;
- trebuie asigurată inaccesibilitatea tuturor conținuturilor informaționale anterioare ale resurselor în procesul distribuirii resursei pentru toate obiectele.

7.1.1.2. Cerințe privind managementul securității în procesul prestării serviciilor publice

Cerințele privind managementul securității în procesul prestării serviciilor publice sînt:

- posibilitatea de a modifica drepturile de acces trebuie să fie limitată astfel încît utilizatorul care deține dreptul de acces la obiectul informațional să nu poată modifica aceste drepturi înainte de a primi permisiunea respectivă;

- cerințe privind gestionarea datelor:

1) trebuie să existe posibilitatea creării, distrugerii şi vidării registrului de audit doar de către administratori autorizați;

2) trebuie să existe posibilitatea modificării sau vizualizării multitudinii de evenimente supuse auditării doar de către administratorii autorizați;

3) trebuie să existe posibilitatea inițializării şi modificării atributelor securității utilizatorilor, cu excepția datelor de autentificare, doar de către administratorii autorizați;

4) trebuie să existe posibilitatea inițializării şi modificării datelor autentificării doar de către administratorii autorizați;

- cerințe cu privire la rolurile securității:

1) trebuie susținute următoarele roluri: administrator autorizat; utilizatori împuterniciți prin politica managementului discreționar a accesului de a modifica atributele securității obiectului informațional; utilizatorii împuterniciți de a modifica datele de autentificare personale;

2) trebuie să existe posibilitatea de a asocia utilizatorii cu rolurile.

7.1.2. Cerințe de încredere a securității pentru profilul de protecție „Acces controlat”

7.1.2.1. Cerințe privind documentația şi software

Cerințele privind documentația şi software-ul care asigură prestarea serviciilor publice trebuie să includă următoarele:

- cerințe privind documentația sistemului de prestare a serviciilor publice, care trebuie să:

1) fie actuală, protejată în modul corespunzător şi accesibilă pentru categoriile de personal stabilite;

2) includă documentația în care sînt descrise măsurile şi mijloacele de asigurare a securității în procesul de prestare a serviciilor publice, cu detaliile necesare pentru analiza şi verificarea acestora;

- cerințe privind manualul administratorului, care trebuie să conțină:

1) descrierea funcțiilor de administrare şi a interfețelor accesibile administratorului;

2) descrierea modului inofensiv de management al sistemului de prestare a serviciilor publice;

3) avertizări privind funcțiile şi privilegiile care urmează să fie controlate într-un mediu inofensiv de procesare a informației;

4) descrierea tuturor parametrilor securității controlați de administrator, cu specificarea, în caz de necesitate, a valorilor inofensive ale parametrilor;

5) descrierea tuturor presupunerilor privind comportamentul utilizatorului, care au legătură cu exploatarea inofensivă a sistemului de prestare a serviciilor publice;

6) descrierea evenimentelor posibile legate de securitate şi de exercitarea funcțiilor obligatorii de management;

- cerințe privind manualul utilizatorului, care trebuie să:

1) conțină descrierea funcțiilor şi interfețelor accesibile utilizatorilor;

2) conțină descrierea mijloacelor aplicate de asigurare a securității şi controlului accesibile utilizatorilor, precum şi descrierea modalității de utilizare a acestora;

3) conțină avertizări privind funcțiile şi privilegiile accesibile utilizatorilor;

4) fie expuse într-o manieră exactă toate obligațiile utilizatorilor necesare pentru exploatarea inofensivă a sistemului de prestare a serviciilor publice;

- cerințe privind instalarea software-ului:

1) instituția exploatatoare trebuie să stabilească şi să aplice reguli bine definite privind instalarea software-ului de către utilizatori;

2) trebuie să fie identificate tipurile de software permise şi interzise pentru a fi instalate de către utilizatori;

- cerințe privind utilizarea software-ului:

1) în procesul utilizării software-ului şi a documentației aferente acestuia trebuie să fie respectate acordurile cu producătorii şi cerințele legislației naționale în vigoare cu privire la dreptul de autor;

2) instituția exploatatoare trebuie să dispună de un sistem de control al copierii şi distribuirii software-ului şi a documentației aferente acestuia în conformitate cu licențele obținute.

7.2. Profilul de protecție „Protecție prin marcare"

Profilul de protecție „Protecție prin marcare" este destinat pentru managementul accesului care permite limitarea acțiunilor anumitor utilizatori şi a accesului la resursele şi sistemele informaționale şi stabileşte ansamblul de cerințe funcționale şi cerințe de încredere pentru SI de prestare a serviciilor publice.

În cazul „Protecției prin marcare" trebuie să fie aplicate două clase de mecanisme de management al accesului, care permit utilizatorilor individuali să determine modul de utilizare în comun a resurselor şi sistemelor informaționale (de exemplu, fişiere, cataloage) în condițiile managementului realizat de către aceşti utilizatori, şi care impun restricții privind utilizarea resurselor şi sistemelor în rîndurile utilizatorilor.

Scopurile securității profilului de protecție „Protecție prin marcare" include toate scopurile profilului de protecție „Acces controlat", precum şi următoarele scopuri:

- acordarea tuturor funcțiilor şi posibilităților pentru susținerea administratorilor autorizați care sînt responsabili de managementul securității în procesul de prestare a serviciilor publice;

- proiectarea şi realizarea astfel încît să fie asigurată realizarea politicii de securitate a instituției într-un mediu prestabilit, ținîndu-se cont de cerințele privind securitatea fizică şi de cerințele privind personalul.

Cerințele de securitate la prestarea serviciilor publice ale profilului de securitate „Protecție prin marcare" trebuie să fie divizate în cerințe funcționale şi cerințele de încredere, care contribuie la realizarea scopurilor acestui profil de securitate. Cerințele funcționale ale profilului de protecție „Protecție prin marcare" coincid parțial cu cerințele profilului de protecție „Acces controlat", iar cerințele de încredere coincid cu profilul de protecție „Acces controlat".

7.2.1. Cerințe funcționale pentru profilul de protecție „Protecție prin marcare"

Cerințele funcționale ale profilului de protecție „Protecție prin marcare" coincid cu cerințele profilului de protecție „Acces controlat", care trebuie să fie completate cu următoarele:

- cerințe față de exportul datelor utilizatorului fără atribute de securitate:

1) trebuie realizată politica de management al accesului prin mandat în cazul exportului datelor „nemarcate" ale utilizatorului;

2) dispozitivele utilizate pentru exportul datelor fără atribute de securitate nu trebuie să fie utilizate pentru a exporta date cu atribute de securitate;

- cerințe față de exportul datelor utilizatorului cu atribute de securitate:

1) în cazul de export al datelor utilizatorului peste limite, atributele de securitate trebuie să fie asociate univoc cu datele exportate „marcate" ale utilizatorului;

2) dispozitivele utilizate pentru exportul datelor cu atribute de securitate nu pot fi utilizate pentru exportul datelor fără atribute de securitate;

- trebuie să fie realizată politica de management al accesului prin mandat pentru subiecți şi obiecte şi al tuturor operațiilor între subiecți şi obiecte;

- cerințe privind atributele de securitate ierarhice:

1) trebuie realizată politica de management prin mandat al accesului, bazată pe următoarele tipuri de atribute de securitate a subiecților şi informației: mențiunea privind sensibilitatea subiectului şi

mențiunea privind sensibilitatea obiectului ce conține informații;

2) fluxul informațional dintre subiectul gestionat şi informație trebuie să fie permis: dacă mențiunea privind sensibilitatea subiectului este mai mare decît sau este egală cu mențiunea privind sensibilitatea obiectului, atunci este permis fluxul informațional de la obiect la subiect (operația de citire); dacă mențiunea privind sensibilitatea obiectului este mai mare decît sau este egală cu mențiunea privind sensibilitatea subiectului, atunci este permis fluxul informațional de la subiect la obiect (operația de înregistrare); dacă mențiunea privind sensibilitatea subiectului A este mai mare decît sau este egală cu mențiunea privind sensibilitatea subiectului B, atunci este permis fluxul informațional de la subiectul B la subiectul A;

- cerințe privind anularea drepturilor de acces:

1) trebuie să existe posibilitatea anulării imediate a împuternicirilor importante pentru securitate;

2) drepturile de acces asociate cu obiectul trebuie să fie activate după verificarea accesului;

- pe lîngă rolurile indicate mai sus, este necesar de a susține utilizatorii împuterniciți prin politica de management al accesului prin mandat de a modifica atributele de securitate ale obiectului informațional.

7.3. Profilul de protecție „Sisteme operaționale”

Profilul de protecție „Sisteme operaționale” stabileşte cerințele securității pentru sistemele operaționale de destinație comună în procesul de prestare a serviciilor publice, care conțin de regulă sisteme de fişiere, servicii de imprimare, servicii de rețea, servicii de arhivare a datelor şi alte aplicații asigurate de host (de exemplu, poşta electronică, bazele de date). Sistemele operaționale care corespund cerințelor acestui profil susțin medii în care poate fi procesată informația confidențială. Profilul de protecție „Sisteme operaționale” asigură managementul accesului discreționar, ceea ce înseamnă că subiectul care deține o anumită permisiune de acces are posibilitatea de a transmite această permisiune oricărui alt subiect.

Managementul accesului la toate datele şi resursele informaționale protejate trebuie să fie realizat în baza identificatorului. Pentru toți utilizatorii trebuie să fie desemnați identificatori unici. Acest identificator trebuie să asigure responsabilitatea utilizatorului. Trebuie să fie confirmată autenticitatea identificatorului declarat al utilizatorului înainte de obținerea permisiunii de către utilizator de a executa orice acțiuni.

Particularitățile specifice ale securității, care sînt necesare pentru astfel de sisteme trebuie să includă:

- identificarea şi autentificarea: utilizatorii autorizați trebuie să fie identificați şi autentificați înainte de accesul la informația păstrată în sistemul de prestare a serviciilor publice;

- managementul accesului discreționar oferă utilizatorilor autorizați posibilitatea de a determina protecția pentru fişierele de date pe care aceştia le creează;

- serviciile de audit, care oferă posibilitate administratorilor împuterniciți, trebuie să depisteze şi să analizeze încălcările potențiale ale securității.

Scopurile securității profilului de protecție „Sisteme operaționale” sînt:

- sistemul operațional trebuie să asigure obținerea accesului la ea şi la resursele informaționale pe care le gestionează doar de către utilizatorii autorizați;

- sistemul trebuie să reprezinte informația legată de tentativele anterioare de a stabili o şedință;

- sistemul operațional trebuie să ofere posibilitatea de a depista şi de a înregistra evenimentele semnificative pentru securitate în procesul de prestare a serviciilor publice, asociate cu utilizatorii individuali; trebuie să ofere posibilitatea de a proteja şi de a vizualiza selectiv informația de audit asociată cu utilizatorii individuali;

- sistemul operațional trebuie să gestioneze accesul la resurse în baza identificatorilor utilizatorilor sau ai grupurilor de utilizatori;

- sistemul operațional trebuie să ofere utilizatorilor împuterniciți posibilitatea de a stabili tipul de resurse informaționale şi utilizatorii sau grupurile de utilizatori care pot obține acces;
- sistemul operațional trebuie să fie setat şi instalat prin metoda care susține securitatea sistemului de prestare a serviciilor publice;
- sistemul operațional trebuie să ofere mijloace pentru protecția datelor utilizatorului şi a resurselor;
- nici un utilizator nu trebuie să-i blocheze pe ceilalți utilizatori în caz de apelare la resursele informaționale;
- sistemul operațional trebuie să fie supus unei testări independente care să includă scenarii de testare şi rezultate;
- sistemul operațional trebuie să verifice identificatorul declarat al utilizatorului;
- în sistemul operațional utilizatorii trebuie să se identifice o singură dată.

Cerințele de securitate în procesul de prestare a serviciilor publice ale profilului de protecție „Sisteme operaționale" trebuie să fie divizate în cerințe funcționale şi cerințele de încredere care contribuie la realizarea scopurilor acestui profil de securitate.

7.3.1. Cerințe funcționale pentru profilul de protecție „Sisteme operaționale"

Cerințele funcționale pentru profilul de protecție „Sisteme operaționale" coincid cu anumite cerințe ale profilului de protecție „Protecție prin marcare", care urmează a fi completate cu următoarele:

- trebuie să existe posibilitatea determinării regimului de executare, deconectare, conectare, modificării regimului de executare a funcțiilor privind selectarea evenimentelor supuse auditării;
- trebuie să existe posibilitatea protejării datelor contra revelării şi modificării în procesul de transmitere a lor între porțiunile divizate ale SI;
- trebuie să fie asigurată concordanța datelor la dublarea lor în diverse porțiuni ale SI de prestare a serviciilor publice;
- cerințe privind autotestarea:

1) trebuie să fie realizat un pachet de programe de autotestare la lansare sau la solicitarea administratorului autorizat pentru demonstrarea executării corecte;

2) trebuie să existe posibilitatea la administratorii autorizați de a verifica integritatea datelor şi a codului executat păstrat;

- trebuie să realizeze cotele maxime ale următoarelor procese: procentul de memorie a spațiului de disc şi procentul de memorie de sistem, pe care utilizatorii individuali le pot utiliza în orice timp stabilit;
- trebuie să fie furnizat traseul de comunicații dintre sine şi utilizatorii locali care este diferit din punct de vedere logic de alte trasee de comunicații şi asigură o identificare certă a părților sale terminale, precum şi protecția datelor transmise contra modificării sau revelării.

7.3.2. Cerințe de încredere a securității pentru profilul de protecție „Sisteme operaționale"

Cerințele de încredere a securității profilului de protecție „Sisteme operaționale" coincid cu cerințele de acelaşi gen ale profilului de protecție „Protecție prin marcare", care urmează a fi completate cu următoarele:

- cerințe privind testarea:

1) elaboratorul trebuie să testeze funcțiile SI de prestare a serviciilor publice şi să documenteze rezultatele;

2) documentația de testare trebuie să fie constituită din planuri şi descrieri ale procedurilor de testare, precum şi ale rezultatelor preconizate şi reale ale testării;

3) planurile de testare trebuie să identifice funcțiile verificate ale securității şi să conțină descrierea scopurilor testării;

4) rezultatele testelor executate de elaborator trebuie să demonstreze că fiecare funcție verificată a securității a fost îndeplinită cu succes;

- trebuie să fie identificate toate regimurile posibile de exploatare a sistemului de prestare a serviciilor publice, inclusiv acțiunile de după deranjament sau eroare în funcționare, consecințele şi importanța acestora pentru asigurarea unei exploatări inofensive; documentația trebuie să demonstreze pentru toate punctele vulnerabile identificate faptul că nici unul dintre acestea nu poate fi utilizat în sistemul de prestare a serviciilor.

Exemple de pericole pentru profilul de protecție „Sisteme operaționale" sînt prezentate în anexa nr.1.

7.4. Profilul de protecție „Sisteme operaționale cu un singur nivel"

Sistemele operaționale care corespund cerințelor acestui profil susțin mediile în care pot fi procesate datele cu un singur nivel în procesul de prestare a serviciilor publice. Acest profil trebuie să asigure managementul accesului discreționar şi să furnizeze servicii criptografice. Pentru crearea sistemului de prestare a serviciilor publice pentru acest profil de protecție este necesar de utilizat hardware-ul şi software-ul sau combinarea lor pentru realizarea serviciilor criptografice. Serviciile criptografice trebuie să asigure un nivel corespunzător de posibilități funcționale şi încredere în atingerea scopurilor de asigurare a securității informaționale. Trebuie utilizate mijloacele de protecție criptografică certificate. Profilul „Sisteme operaționale cu un singur nivel" este utilizat pentru sistemele cu destinație comună cu un număr mare de utilizatori, ceea ce convine sistemului de prestare a serviciilor publice.

Scopurile profilului de protecție „Sisteme operaționale cu un singur nivel" includ obiective identice cu cele ale profilului de protecție „Sisteme operaționale", precum şi următoarele scopuri:

- sistemul operațional trebuie să funcționeze susținînd securitatea SI de prestare a serviciilor publice;
- sistemul operațional trebuie să furnizeze mecanisme criptografice de asigurare a integrității datelor în procesul de transmitere a lor către porțiunile îndepărtate ale SI.

Cerințele securității în procesul de prestare a serviciilor ale profilului de protecție „Sisteme operaționale cu un singur nivel" trebuie să fie divizate în cerințe funcționale şi cerințe de încredere, care contribuie la realizarea scopurilor acestui profil de securitate.

7.4.1. Cerințe funcționale pentru profilul de protecție „Sisteme operaționale cu un singur nivel"

Cerințele funcționale pentru profilul de protecție „Sisteme operaționale cu un singur nivel" coincid cu anumite cerințe ale profilului de protecție „Sisteme operaționale", care trebuie să fie completate cu următoarele:

- cerințe privind managementul mijloacelor de protecție criptografică:

1) trebuie generate chei criptografice simetrice şi asimetrice conform algoritmului stabilit de generare a cheilor criptografice;

2) la fiecare cheie simetrică generată trebuie să fie adăugată suma de control a altui algoritm atestat;

3) toate certificatele cheilor publice generate trebuie să corespundă cerințelor legislației naționale în vigoare;

4) cheile criptografice trebuie să fie distribuite în conformitate cu metoda stabilită de distribuire: metoda manuală (fizică), metoda automată (electronică);

5) trebuie să fie asigurată păstrarea cheilor numai în formă cifrată în conformitate cu cerințele legislației naționale în vigoare;

6) cheile criptografice trebuie să fie distruse conform metodei de distrugere a cheilor criptografice care corespunde cerințelor legislației naționale în vigoare, iar lichidarea întregului text public al

cheilor criptografice şi a tuturor altor parametri critici ai securității în limitele dispozitivului trebuie să fie imediată şi totală;

- trebuie efectuate operațiile de cifrare/descifrare a datelor, calculare a semnăturii digitale criptografice, operațiile de hashing, operațiile de schimb de chei criptografice în conformitate cu legislația în vigoare;
- trebuie adăugat rolul de administrator al mijloacelor de protecție criptografică a informației;
- trebuie susținut domenul criptografic, care este separat de cealaltă porțiune şi este protejat contra intruziunilor şi denaturărilor din partea subiecților neautorizați.

7.4.2. Cerințe de încredere a securității pentru profilul de protecție „Sisteme operaționale cu un singur nivel"

Cerințele de încredere a securității pentru profilul de protecție „Sisteme operaționale cu un singur nivel", utilizate în procesul de prestare a serviciilor publice, trebuie să includă analiza punctelor vulnerabile/testul de intruziune, cerințe privind elaborarea şi analiza canalelor secrete pentru criptografie.

Cerințele de încredere a securității pentru profilul de protecție „Sisteme operaționale cu un singur nivel" coincid cu cerințele de acelaşi gen ale profilului de protecție „Sisteme operaționale", care trebuie completate cu următoarele:

- modulul criptografic trebuie să fie proiectat şi structurat astfel încît să fie separat de celelalte procese;
- trebuie stabilite porturile fizice/logice ale modulului criptografic;
- cerințe privind înlăturarea deficiențelor:

1) trebuie stabilită procedura de recepționare şi prelucrare a mesajelor utilizatorilor despre deficiențele securității şi a solicitărilor de remediere;

2) procedurile de înlăturare a deficiențelor trebuie să conțină descrierea procedurilor de monitorizare a tuturor deficiențelor de securitate devenite publice, în procesul de prestare a serviciilor publice;

3) procedurile de înlăturare a deficiențelor trebuie să conțină descrierea naturii şi manifestărilor fiecărei deficiențe de securitate, precum şi a statutului de finalizare a remedierii deficienței respective.

- cerințe privind analiza canalelor secrete ale modulului criptografic:

1) pentru modulul criptografic trebuie efectuată căutarea canalelor secrete de scurgere a parametrilor critici ai securității;

2) documentarea analizei trebuie să identifice canalele secrete din modulul criptografic şi să conțină evaluarea capacității de transmitere;

3) documentația analizei trebuie să conțină descrierea celei mai periculoase variante de scenariu de utilizare a fiecărui canal secret identificat;

4) trebuie să existe confirmarea faptului că rezultatele analizei canalelor secrete demonstrează corespunderea modulului criptografic cu cerințele funcționale.

Exemple de pericole pentru profilul de protecție „Sisteme operaționale cu un singur nivel" sînt prezentate în anexa nr. 2.

7.5. Profilul de protecție „Sisteme operaționale cu multe niveluri"

Sistemele operaționale ce corespund cerințelor acestui profil susțin medii în care pot fi procesate date cu multe niveluri în procesul de prestare a serviciilor publice. Sistemele acestui profil de protecție trebuie să asigure managementul accesului discreționar, managementul accesului prin mandat, managementul integrității prin mandat şi să furnizeze servicii criptografice. Toți utilizatorii trebuie să dețină un nivel asociat de acces, care să determine nivelul maxim al sensibilității resurselor şi sistemelor informaționale la care aceştia pot recurge.

Scopurile sistemului operațional al profilului de protecție „Sisteme operaționale cu multe niveluri” includ scopuri identice cu cele ale profilului de protecție „Sisteme operaționale cu un singur nivel” şi suplimentar scopul: sistemul operațional trebuie să gestioneze accesul la resurse, care este bazat pe nivelul accesului utilizatorilor şi resurselor, precum şi nivelul integrității resurselor şi nivelul drepturilor utilizatorilor la modificarea datelor.

Cerințele securității în procesul de prestare a serviciilor publice ale profilului de protecție „Sisteme operaționale cu multe nivele” trebuie să fie divizate în cerințe funcționale şi cerințe de încredere, care contribuie la realizarea scopurilor acestui profil de protecție. Cerințele de încredere ale securității acestui profil coincid cu cerințele de încredere ale securității profilului „Sisteme operaționale cu un singur nivel”.

7.5.1. Cerințe funcționale pentru profilul de protecție „Sisteme operaționale cu multe niveluri”

Cerințele funcționale pentru profilul de protecție „Sisteme operaționale cu multe niveluri” coincid cu cerințele funcționale ale profilului de protecție „Sisteme operaționale cu un singur nivel”, care urmează să fie completate cu cerințele privind gestionarea totală a fluxurilor informaționale:

- pentru toate operațiile de transmitere a informației gestionate către subiecții gestionați trebuie realizată politica de management a accesului prin mandat;
- dacă mențiunea sensibilității subiectului este mai mare decît sau este egală cu mențiunea privind sensibilitatea obiectului, atunci este permis fluxul de informații de la obiect către subiect (operația de citire);
- dacă mențiunea sensibilității obiectului este mai mare decît sau este egală cu mențiunea privind sensibilitatea subiectului, atunci este permis fluxul de informații de la subiect la obiect (operația înregistrării).

Exemple de pericole pentru profilul de protecție „Sisteme operaționale cu multe niveluri” sînt prezentate în anexa 3.

7.6. Profilul de protecție „Sisteme de management al bazelor de date”

Profilul de protecție „Sisteme de management al bazelor de date” stabileşte cerințele securității pentru sistemele de management al bazelor de date în cadrul instituțiilor care prestează servicii publice, unde există cerințe pentru protecția confidențialității, integrității şi accesibilității informației păstrate în bazele de date. Revelarea, modificarea nesancționată sau refuzul de a deservi o astfel de informație poate avea o influență nefavorabilă asupra procesului de prestare a serviciilor publice şi asupra funcționării însăşi a instituției.

Acest profil de protecție trebuie să stabilească:

- totalitatea cerințelor de bază care trebuie respectate de toate bazele de date;
- totalitatea pachetelor cu datele de autentificare ce reprezintă mijloace de confirmare a autenticității utilizatorului.

Scopurile profilului de protecție „Sisteme de management al bazelor de date” sînt următoarele:

- prevenirea dezvăluirii, introducerii, modificării sau distrugerii neautorizate a datelor şi obiectelor din bazele de date (fişiere, cataloage, inclusiv programe, biblioteci de programe de lucru, fişiere ale bazei de date, fişiere exportate, fişiere ale înregistrării repetate, fişiere gestionate, fişiere cu trasare şi fişiere cu dump), precum şi prevenirea vizualizării bazei de date, gestionării datelor şi a auditului datelor din baza de date;
- acordarea mijloacelor de gestionare utilizînd resursele informaționale ale bazei de date de către utilizatorii autorizați;
- acordarea mijloacelor de identificare/autentificare a utilizatorilor pentru confirmarea sigură a autenticității utilizatorilor;
- acordarea mijloacelor de înregistrare detaliată a evenimentelor semnificative pentru securitate.

Cerințele de securitate în procesul prestării serviciilor publice ale profilului de protecție „Sisteme de management al bazelor de date” trebuie să fie divizate în cerințe funcționale şi cerințe de încredere, care contribuie la realizarea scopurilor acestui profil de securitate.

7.6.1. Cerințe funcționale pentru profilul de protecție „Sisteme de management al bazelor de date”

Cerințele funcționale pentru profilul de protecție „Sisteme de management al bazelor de date” în procesul de prestare a serviciilor publice trebuie să includă:

- fiecare eveniment care poate fi supus auditului bazei de date trebuie să se asocieze cu identificatorul utilizatorului bazei de date, care a fost inițiatorul evenimentului respectiv;
- managementul accesului trebuie să fie realizat pentru subiecți, obiecte şi operațiile bazei de date;
- pentru fiecare utilizator al bazei de date trebuie să se mențină următoarea listă de atribute ale securității: identificatorul utilizatorului bazei de date şi privilegiile de acces la obiectul din baza de date;
- fiecare utilizator al bazei de date trebuie să fie identificat cu succes înainte de permiterea oricărei alte acțiuni în numele utilizatorului respectiv;
- trebuie să existe o limitare a posibilităților de efectuare a operațiilor cu date de către utilizatorii autorizați ai bazelor de date;
- trebuie menținute următoarele roluri: utilizator administrativ al bazei de date şi utilizator al bazei de date;
- trebuie menținut domenul securității pentru executare proprie, care protejează datele contra intruziunilor şi denaturărilor din partea subiecților neautorizați ai bazei de date;
- numărul maxim al şedințelor paralele cu baza de date, acordate aceluiaşi utilizator al bazei de date, trebuie să fie limitat şi stabilit în prealabil.
- trebuie să existe posibilitatea acordării refuzului de a deschide şedința cu baza de date utilizatorului, bazîndu-se pe drepturile lui;
- cerințe privind autentificarea cu mijloacele bazei de date:

1) trebuie depistate tentativele eşuate de autentificare cu ajutorul mijloacelor bazei de date;
2) parolele bazei de date trebuie să corespundă cerințelor legislației în vigoare.

7.6.2. Cerințe de încredere a securității pentru profilul de protecție „Sisteme de management al bazelor de date”

Cerințele de încredere a securității pentru profilul de protecție „Sisteme de management al bazelor de date” trebuie să includă cerințele de bază:

- sistemul trebuie să identifice şi să autentifice utilizatorii înainte de acordarea accesului la orice resurse, sisteme şi mijloace informaționale;
- sistemul trebuie să furnizeze mecanisme de management al accesului pentru realizarea scopurilor fixate;
- sistemul trebuie să furnizeze mecanisme de audit şi mijloace instrumentale de gestionare a auditului în vederea susținerii SI de prestare a serviciilor;
- sistemul trebuie să furnizeze o copie de rezervă, să asigure capacitatea de returnare la starea de lucru şi alte mecanisme sigure de restabilire.

Exemple de pericole pentru profilul de protecție „Sisteme de management al bazelor de date” sînt prezentate în anexa nr. 4.

Anexa nr.1

Pericolele securității

ale profilului de protecție „Sisteme operaționale”

Pericolele securității
1. Erori în proiectul sistemelor operaționale
2. Erori în realizarea sistemelor operaționale
3. Erori de documentare
4. Acțiuni eronate ale administratorului, care încalcă politica de securitate a informației a sistemelor operaționale
5. Acțiuni eronate ale utilizatorului, care duc la încălcarea politicii de securitate a informației a sistemelor operaționale
6. Deficiență (refuz) a (al) sistemelor operaționale

Anexa nr. 2

Pericolele securității
ale profilului de protecție „Sisteme operaționale
cu un singur nivel”

Pericolele securității
1. Administrarea incorectă poate duce la încălcarea proprietăților caracteristice ale securității.
2. Deteriorarea sau pierderea datelor auditului
3. Deteriorarea sau pierderea datelor configurației sau a altor date încredințate.
4. Atacuri care conduc la refuzul de deservire.
5. Accesul neautorizat al utilizatorului neautorizat sau autorizat la datele aflate în tranzit, care sunt transmise sau recepționate de sistemul operațional
6. Instalarea incorectă a sistemului operațional, ceea ce poate duce la încălcarea securității
7. Restartarea poate conduce la o stare periculoasă a sistemului operațional.
8. Sistemele nu pot transmuta în mod adecvat datele din obiecte, care sunt utilizate în comun de diferiți utilizatori, în procesul de eliberare şi utilizare ulterioară a resurselor.
9. Erorile ocazionale sau premeditate în specificațiile cerințelor, în proiect sau în procesul elaborării sistemului operațional
10. Erorile ocazionale sau premeditate în procesul realizării proiectului sistemului operațional
11. Comportamentul incorect al sistemului poate fi rezultatul incapacității de a stabili faptul că toate funcțiile şi interacțiunile sistemului operațional sunt corecte.
12. Intrusul poate primi accesul repetând informația de autentificare
13. Utilizatorii autorizați pot considera în mod greşit că mențin legătura cu sistemul operațional, pe când aceştia de fapt mențin legătura cu o entitate nocivă care pretinde că reprezintă un sistem operațional
14. Accesul ilegal al intrusului la înregistrarea de evidență a administratorului sau la înregistrarea de evidență a altei persoane din rândurile personalului împuternicit
15. La şedința rămasă fără supraveghere poate fi obținut un acces neautorizat
16. Accesul neautorizat al utilizatorilor neautorizați şi autorizați la datele

sistemului informațional
17. Modificarea sau utilizarea neautorizată a atributelor sistemului operațional şi ale resurselor
18. Deficiența sistemului operațional în caz de depistare şi înregistrare a acțiunilor neautorizate
19. Refuzul sistemului la tentativele administratorului de a identifica acțiunile neautorizate şi de acționa asupra lor
20. După deranjamentul sistemului operațional starea securității poate fi necunoscută.
21. Pierderea sau deteriorarea datelor utilizatorului de către alți utilizatori

Anexa nr. 3

Pericolele securității
ale profilului de securitate „Sisteme operaționale
cu multe niveluri”

Pericolele securității includ pericolele securității ale profilului de protecție „Sisteme operaționale cu un singur nivel” şi pericolele securității indicate în tabel.

Pericolele securității
1. Entitatea, care operează la un calculator în rețea, poate să-şi schimbe aparența în această rețea, preluând aparența unei entități care operează la un alt calculator
2. Accesul neautorizat al utilizatorilor la datele „marcate” deoarece sistemele nu pot diviza în mod adecvat datele în baza mențiunilor pe care acestea le comportă

Anexa 4

Pericolele securității
ale profilului de securitate „Sisteme de management
a bazelor de date”

Pericolele securității
1. Accesul neautorizat la baza de date
2. Accesul neautorizat la informația din baza de date
3. Utilizarea excesivă a resurselor bazei de date
4. Utilizarea incorectă a privilegiilor utilizatorilor bazei de date
5. Pierderea sau distrugerea datelor de management a bazei de date sau a datelor auditului în rezultatul întreruperilor inopinate în procesul funcționării obiectelor din sistem

Anexa nr. 4
la Ordinul nr. 94
din 17 09 2009

REGLEMENTARE TEHNICĂ
Determinarea costului de elaborare şi implementare
a sistemelor informaționale automatizate.
Normativele şi estimarea cheltuielilor de lucru

1 Domeniu de aplicare

Prezenta reglementare stabileşte principiile generale pentru determinarea costului de elaborare şi implementare a sistemelor informaţionale automatizate (în continuare - sisteme informaţionale (SI)). În prezenta reglementare sînt stabilite procesele, lucrările şi sarcinile care sînt folosite la determinarea costului de elaborare şi implementare a SI, fără stabilirea detaliilor privind realizarea sau îndeplinirea lucrărilor şi sarcinilor.

Prezenta reglementare propune metodologia de formare a costului SI, descrie componentele de bază ale costului SI, propune o metodă de determinare a costului componentelor SI, inclusiv de elaborare şi implementare a SI.

Prezenta reglementare este folosită pentru formarea sau estimarea costului SI. Reglementarea este destinată: clienţilor SI, produselor şi serviciilor software; furnizorilor, elaboratorilor şi administratorilor SI; managerilor de proiecte; managerilor responsabili de calitate şi utilizatorilor produselor software.

În prezenta reglementare este stabilit setul de procese, lucrări şi sarcini destinate adaptării la condiţiile unor proiecte concrete în domeniul de implementare a SI.

2 Baza normativ-legislativă

Prezenta reglementare este alcătuită în baza prevederilor următoarelor acte legislative ale Republicii Moldova:

1) Legea Republicii Moldova privind accesul la informaţie nr. 982-XIV din 11.05.2000;

2) Legea Republicii Moldova cu privire la informatizare şi resursele informaţionale de stat nr. 467–XV din 21.11.2003;

3) Legea Republicii Moldova cu privire la documentul electronic şi semnătura digitală nr. 264-XV din 15.07.2004;

4) Legea Republicii Moldova privind comerţul electronic nr. 284-XV din 22.07.2004;

5) Legea Republicii Moldova privind activitatea de reglementare tehnică nr.420-XVI din 22.12.2006;

6) Legea Republicii Moldova cu privire la protecţia datelor cu caracter personal nr. 17-XVI din 15.02.2007;

7) Legea Republicii Moldova cu privire la registre nr. 71-XVI din 22.03.2007;

8) Legea Republicii Moldova privind achiziţiile publice nr. 96 din 13.04.2007.

3 Terminologie

Componenta produsului de program — parte identificabilă şi cuprinzătoare a produsului de program, de exemplu, procedură de program, compartiment sau alineat al documentului, documentul integral.

Divizarea structurală a lucrărilor — structurarea ierarhică a lucrărilor proiectului, orientată spre rezultatele de bază ale proiectului, care îi determină domeniul de obiect. Fiecare nivel inferior al structurii constituie o detaliere a elementului nivelului superior al proiectului. Element al proiectului poate fi un produs, serviciu, precum şi un pachet de lucrări sau o lucrare.

Hardware — echipamentul folosit pentru introducerea, procesarea şi extragerea datelor din sistemele informaționale.

Modelul ciclului de viață — structură compusă din procesele, lucrările şi sarcinile implicate în elaborarea, exploatarea şi mentenanța produsului de program care cuprinde viața sistemului de program începînd cu stabilirea cerințelor față de acesta pînă la încetarea utilizării sale.

Monitorizare — procesul de colectare, analiză a datelor, prezentare a rapoartelor privind executarea lucrărilor.

Sarcină tehnică — document folosit de client în calitate de mijloc pentru descrierea şi fixarea sarcinilor executate la realizarea contractului.

Tehnologie comunicațională — echipamentul şi software-ul care servesc pentru legătura dintre elementele separate ale sistemelor informaționale şi transmiterea „fizică” a datelor.

4 Conținutul sistemului informațional

SI reprezintă o totalitate organizatoric-aranjată de resurse informaționale, tehnologii informaționale, echipament şi mijloace de comunicare ce permite colectarea, păstrarea, procesarea şi utilizarea informației.

SI constă din următoarele componente de bază:

1) software reprezintă totalitatea informației, datelor şi programelor ce sînt procesate de sistemele computerizate;

2) asigurarea informațională reprezintă asigurarea cu date faptice ale structurilor de administrare, utilizarea datelor informaționale pentru sistemele automatizate de administrare, folosirea informației pentru asigurarea activității diferiților consumatori;

3) hardware reprezintă un complex de dispozitive electronice, electrice şi mecanice ce fac parte din sistem sau rețea;

4) personalul de deservire.

4.1. Software

Software reprezintă totalitatea de programe ale sistemelor de procesarea informației şi documentelor de program, necesare pentru exploatarea programelor acesteia, clasificîndu-se în următoarele:

1) software de sistem – un set de programe care gestionează componentele SI, cum sînt procesorul, dispozitivele comunicaționale şi periferice, precum şi programele destinate asigurării

funcționării şi capacității de funcționare a întregului sistem:

- sistemele operaționale cu destinație generală, de timp real, de rețea, incorporabile;

- încărcătorul sistemului operațional;

- driver-ele dispozitivelor;

- programele capabile să realizeze transformarea fluxului de date sau a semnalului;

- utilite;

2) mijloacele software de protecție - includ programe pentru identificarea utilizatorilor, controlul accesului, criptarea informației, ştergerea informației reziduale (de lucru) de tipul fişierelor temporare, controlul de testare a sistemului de protecție. Mijloacele software de protecție sînt:

- gateway criptice;

- mijloacele de autentificare;

- mijloacele de monitorizare şi audit;

- scanerele gradului de protecție;

- mijloacele de delimitare a accesului;

- sistemele de protecție criptografică, criptare şi semnătură electronică digitală;

- programele antivirus şi antispam;

- ecrane între rețele;

3) software instrumental – programele destinate utilizării în procesul de proiectare, elaborare şi mentenanță a SI. Include mijloacele de elaborare a software, sisteme de gestionare a bazelor de date, compilatoare, translatoare, generatoare;

4) software aplicativ include:

- aplicațiile de birou: redactori de text, procesoare de text, procesoare de tabele, redactori de prezentări;

- SI corporative: programe de contabilitate, sisteme MRP (Material Requirement Planning), sisteme MRP II, sisteme ERP (Enterprise Resource Planning System), sisteme CRM (Customer relationship management), sisteme SCM (Supply Chain Management), sisteme de gestionare a proiectelor, sisteme de automatizare a circuitului documentelor, sisteme de gestionare a arhivelor documentelor, portalul corporativ;

- sisteme de proiectare şi producere: sisteme de proiectare automatizată (sisteme CAD Computer-Aided Design), sisteme CAE (Computer-aided engineering), sisteme CAM (Computer-aided

manufacturing), sisteme PDM (Product Data Management), sisteme PLM (Product Lifecycle Management), sisteme automatizate de gestionare a procesului tehnologic;

- sisteme de suport logistic al produselor: sisteme de analiză a suportului logistic şi sisteme organizatorico-tehnice;

-sisteme de prelucrare şi păstrare a informației medicale;

- software-ul ştiințific;

- sisteme geoinformaționale;

- sisteme de susținere a luării deciziilor;

- clienţi pentru acces la serviciile Internet: poşta electronică, resursele Web, transmiterea momentană a mesajelor, canalele chat, telefonia IP, schimbul de fişiere P2P, difuzarea în torente, client-bancă;

- multimedia.

4.2. Asigurarea informațională

Infrastructura SI include subsisteme organizatorice şi tehnologice, precum şi un complex de resurse de furnizare, cu ajutorul cărora sînt realizate atît sarcinile interne, cît şi cele externe de administrare şi organizare, în conformitate cu funcțiile stabilite de legislație.

SI asigură legătura subsistemelor în cadrul unei logici unice, a standardelor, „interfețelor” şi utilizării în comun a resurselor informaționale.

Resursele informaționale includ:

1) bazele de date şi banca de date;

2) documentația de sistem;

3) ghidul utilizatorului;

4) materialele educaționale;

5) procedurile operaționale şi procedurile de suport;

6) planurile de asigurare a funcționării neîntrerupte a organizației;

7) procedurile de trecere la regimul de avarie.

În dependență de utilizare, resursele informaționale de stat se împart în:

1) resurse informaționale de stat de bază;

2) resurse informaționale de stat departamentale;

3) resurse informaționale de stat teritoriale.

Resursele informaționale de stat de bază sînt resursele informaționale destinate utilizării comune de către toate autoritățile administrației publice, persoanele juridice şi fizice, în limitele împuternicirilor acordate.

Resursele informaționale de stat departamentale se formează şi sînt folosite de organele de specialitate ale administrației publice, deținătoare ale acestor resurse. Resursele informaționale departamentale conțin informația necesară pentru îndeplinirea de către organele menționate a funcțiilor acestora, cu excepția datelor destinate includerii în resursele informaționale de bază.

Resursele informaționale teritoriale se formează şi sînt utilizate de autoritățile administrației publice locale, deținătoare ale acestor resurse. Resursele informaționale teritoriale conțin date despre toate tipurile de obiecte geografice naturale şi artificiale, inclusiv potențialul de resurse pe teritoriile administrate.

4.3. Hardware

Hardware sînt folosite în scop de instalare, menținere şi stopare a conexiunii, precum şi în scop de asigurare a prelucrării semnalelor între echipamentul de date definitiv şi canalul de acces comun, şi includ:

1) calculatoare şi dispozitive logice;

2) dispozitive externe şi aparataj de diagnosticare;

3) resurse comunicaționale;

4) dispozitive energetice;

5) baterii;

6) acumulatoare.

Resursele comunicaționale sînt destinate gestionării proceselor de transmitere a informației între alte sisteme şi includ:

1) comutatoare;

2) concentratoare;

3) routere;

4) ecrane între rețele;

5) adaptoare;

6) sisteme de cablare;

7) dispozitive de repetare, poduri.

Resursele comunicaționale constituie un multiprocesor complex specializat, care trebuie să fie configurat, optimizat şi administrat.

5. Metodele de determinare a costului sistemelor informaționale

La baza metodelor de determinare a costului SI se află modelul constructiv de cost (Constructive Cost Model – COCOMO), elaborat de către Barry Boehm şi aplicat pentru determinarea costului SI comerciale şi de stat. COCOMO II este adaptat la metodologiile moderne de elaborare a software-ului şi se potriveşte pentru toate modelele ciclului de viață al software-ului.

Modelul prezentat reprezintă unul din cele mai populare, deschise şi bine documentate modele matematice de evaluare a costului şi volumului de lucru pentru elaborarea software-ului. Pentru prelucrarea datelor statistice este folosită analiza lui Bayes, care oferă cele mai bune rezultate pentru proiectele de program incomplete şi ambigue.

Analiza lui Bayes constituie o abordare, care ia în considerație distribuirea probabilităților, bazată fie pe opinia subiectivă, fie pe astfel de date obiective precum rezultatele cercetării anterioare; poate fi folosită pentru cercetări unice şi pentru meta-analiză. Analiza lui Bayes utilizează teorema lui Bayes şi permite reevaluarea distribuirii cu luarea în considerație a rezultatelor cercetării, oferind următoarea distribuire, pe care se bazează concluziile statistice (evaluări punctiforme, intervale de încredere).

Modelul se bazează pe indicatori real măsurabili. Pentru evaluarea volumului de lucru şi costului proiectului, aceste date inițiale trebuie să fie detaliate. La calcularea indicatorilor, modelul ia în considerație nivelul de maturitate a procesului de elaborare.

În prezentul document se prezintă abordarea formării costului SI la fiecare etapă a ciclului de viață. Abordarea este prezentată sub forma executării pe etape a lucrărilor, cu respectarea şirului de cerințe enumerate mai jos.

6. Etapele de determinare a costului sistemelor informaționale

Înainte de începerea etapelor de determinare a costului de elaborare şi implementare a SI, este necesar a parcurge etapa lucrărilor de anteproiect. Etapa lucrărilor de anteproiect începe de la conştientizarea inițială a necesității de creare a unui SI nou sau de modificare a unui SI existent.

Această etapă reprezintă o perioadă de examinare inițială, colectare de fapte şi analiză, examinare a legislației în vigoare şi a structurii organizaționale existente, examinare a SI analogice existente. Rezultatele etapei lucrărilor de anteproiect sînt concepția sistemului şi propunere-business, care permit luarea deciziei – de a continua sau de a înceta realizarea SI.

Totuşi, în cazul în care este necesară introducerea unor sarcini suplimentare, trebuie să fie evaluată oportunitatea îndeplinirii lor.

În scop de determinare a costului elaborării şi implementării SI, este necesar de urmat consecutiv cîteva etape:

1) analiza şi specificarea cerinţelor faţă de SI - analiza cerinţelor funcţionale şi nefuncţionale, a cerinţelor faţă de interfeţele externe ale SI, faţă de hardware-ul, faţă de asigurarea securităţii informaţionale, determinarea arhitecturii hardware-ului, proiectarea software-ului, identificarea obiectelor şi ierarhia acestora;

2) determinarea unităţilor structurale şi a costului de livrare a software-ului şi a hardware-ului - determinarea livrărilor şi arendării hardware-ului şi software-ului;

3) estimarea mărimii segmentului de programare al SI - determinarea mărimii segmentului de programare al SI şi alcătuirea documentaţiei privind evaluarea volumului segmentului de programare;

4) estimarea volumului lucrărilor - identificarea riscurilor, a Divizării structurale a lucrărilor, calculul şi corectarea volumului de lucrări şi de cheltuieli de lucru pentru elaborarea software-ului;

5) cheltuielile de lucru pentru codificare şi testare - calcularea volumului de lucrări şi a cheltuielilor pentru codificare şi testare, calcularea duratei codificării şi testării, elaborarea planului de lucru pentru elaborarea SI şi a scenariilor de testare;

6) determinarea caracteristicilor calităţii SI - determinarea caracteristicilor cantitative, calitative, interne şi externe ale calităţii şi evaluarea calităţii SI;

7) calcularea costului SI - aprecierea costului total al proiectului;

8) determinarea influenţei riscurilor - evaluarea influenţei riscurilor, reglarea acesteia, precum şi reglarea cheltuielilor bazate pe evaluarea riscului;

9) confirmarea şi corectarea estimării costului riscurilor - evaluarea riscurilor efectuată de un grup independent de experţi, analiza datelor statistice, compararea evaluărilor riscurilor şi corectarea acestora;

10) implementarea SI - elaborarea planului şi sarcinilor de implementare, realizarea implementării depline a SI.

6.1. Analiza şi specificarea cerinţelor faţă de sistemul informaţional

Scopul analizei cerinţelor faţă de SI constă în elaborarea şi confirmarea cerinţelor funcţionale, nefuncţionale, a cerinţelor faţă de interfeţele externe şi securitatea sistemului, identificarea restricţiilor tehnice şi de program, care permit cea mai exactă estimare a costului SI.

Procesul de colectare şi analiză a cerinţelor constă din următoarele:

11) analiza şi modelarea detaliată a cerinţelor de program;

12) determinarea arhitecturii SI;

13) determinarea limitelor de realizare a SI;

14) determinarea arhitecturii hardware-ului, comunicaţiilor.

6.1.1. Analiza şi modelarea detaliată a cerințelor de program

6.1.1.1. Cerințele funcționale

Cerințele funcționale descriu acțiunile pentru realizarea cărora este destinată aplicația şi pot fi exprimate sub formă de servicii, sarcini sau funcții pe care aplicația trebuie să le îndeplinească.

Modelul cerințelor determină un complex orientat de interacțiuni între participanții externi şi sistemul examinat. Participanții externi sînt părțile din afara sistemului, care interacționează cu sistemul. Participant extern poate fi clasa utilizatorilor, rolurile îndeplinite de către utilizatori sau alte sisteme.

Scopul principal al modelării cerințelor funcționale constă în stabilirea limitelor funcționării aplicației şi a întregului complex de posibilități funcționale, oferite utilizatorului final.

Cerințele funcționale trebuie să includă cel puțin următoarele:

1) cerințele, coordonate de către toți reprezentații subdiviziunilor de afaceri interesați, care includ:

- caracteristica SI;

- scopurile de bază ale creării şi destinația;

- dezvoltarea planificată;

- cerințele față de SI în întregime;

- cerințele față de structura datelor SI;

- cerințele față de funcționalitatea SI;

- cerințele față de interfața utilizatorului şi rapoarte;

- cerințele față de mijloacele de administrare;

- cerințele față de mijloacele de elaborare;

- cerințele față de interacțiunea cu alte produse software;

- cerințele față de documentare;

- cerințele față de software şi hardware;

- descrierea specificației SI în care se aplică aplicația respectivă;

- documentarea formatelor datelor de intrare şi de ieşire;

- metodele de realizare a controalelor pregătirii, introducerii datelor şi prelucrării erorilor de introducere a datelor, care permit depistarea, indicarea şi corectarea erorilor;

- metodele de realizare a controalelor verificării datelor tranzacțiilor, introduse pentru prelucrare (manual sau de către sistem) pentru exactitate, integritate şi veridicitate;

- metodele de identificare şi eliminare a tranzacțiilor eronate concomitent cu prelucrarea acestora;

- mijloacele ce susțin imposibilitatea de refuz al tranzacțiilor;

2) cerințele formalizate, coordonate de către toți reprezentanții subdiviziunilor de afaceri interesați, care includ:

- descrierea specificațiilor detaliate ale software în privința funcționalității sistemului;

- cerințele față de elaborarea şi documentarea interfețelor cu sisteme interne;

- cerințele față de elaborarea şi documentarea algoritmelor de procesare a datelor;

- cerințele de asigurare a securității, integrității şi accesibilității (inclusiv în situații excepționale).

6.1.1.2. Cerințele față de interfețele externe

Cerințele față de interfețele externe, în dependență de necesitate, trebuie să includă următoarele puncte:

1) prioritatea pe care SI trebuie să o atribuie interfeței;

2) cerințele față de tipul interfeței (funcționarea în regim de timp real, transmiterea datelor, păstrarea şi extragerea datelor), care trebuie să fie asigurate;

3) caracteristicile necesare ale elementelor individuale ale datelor, pe care trebuie să le ofere SI pentru a asigura păstrarea, transmiterea, accesul, primirea datelor:

- numele/identificatorii;

- tipul datelor (cifre-litere, integru);

- dimensiunea şi formatul (lungimea şi punctuația rîndului de simboluri);

- unitățile de măsură (volumului, costului, timpului);

- intervalul sau enumerarea valorilor posibile (de exemplu, 0–99);

- acuratețea (pe cît de corect este) şi exactitatea (numărul categoriilor semnificative);

- prioritatea, cronometrajul, frecvența, volumul, ordinea şi alte restricții pentru actualizarea elementului datelor şi regulile aplicabile de afaceri;

- restricțiile de securitate;

- sursele (obiectele care creează / expediază datele) şi destinatarii (obiectele care utilizează / primesc datele);

4) caracteristicile necesare ale totalităţilor elementelor datelor (înregistrări, mesaje, fişiere, matrice, rapoarte), pe care SI trebuie să le ofere, păstreze, transmită, primească şi la care trebuie să asigure accesul:

- numele/identificatorii;

- elementele datelor care fac parte din structura lor (numărul, ordinea, gruparea);

- mediile (cum sînt discurile) şi structurile datelor / elementelor în mediu;

- caracteristicile audiovizuale ale mesajelor şi altor ieşiri;

- relaţiile dintre grupuri, caracteristicile sortării / accesului;

- prioritatea, cronometrajul, frecvenţa, volumul, ordinea şi alte restricţii;

- timpul de reacţionare la interpelare;

- restricţiile de securitate;

- sursele şi destinatarii;

5) caracteristicile necesare pentru metodele de comunicare, pe care trebuie să le folosească SI pentru interfaţă:

- identificatorii unici de proiect;

- comunicaţiile, conexiunile/benzile de transmitere/frecvenţele/mediile şi caracteristicile acestora;

- formatul mesajelor;

- controlul fluxurilor;

- vitezele de transmitere, periodicitatea, intervalul între transmiteri;

- marşrutizarea, adresarea şi spaţiul denumirilor;

- serviciile de transmitere, inclusiv priorităţile şi evaluările;

- consideraţiile de securitate/confidenţialitate, cum sînt criptarea, autentificarea utilizatorilor, efectuarea auditului;

6) cerinţele faţă de caracteristicile de care trebuie să dispună protocoalele SI pentru interacţiune:

- identificatorul unic de proiect;

- prioritatea/nivelul protocolului;

- divizarea pe pachete, inclusiv fragmentarea, asamblarea repetată, marşrutizarea şi adresarea;

- verificările legalității, controlul erorilor şi procedurile de restabilire;

- sincronizarea, inclusiv instalarea conexiunii, menținerea, încetarea;

- starea, identificarea şi toate posibilitățile rapoartelor;

7) alte caracteristici necesare, compatibilitatea fizică a obiectelor resurselor informaționale, care interacționează (dimensiuni, intervale, încărcări).

6.1.1.3. Cerințele nefuncționale

Cerințele nefuncționale trebuie să fie utilizate pentru determinarea cerințelor şi restricțiilor SI. Cerințele trebuie să fie folosite ca bază pentru sistemul inițial de măsurare şi evaluare a viabilității SI elaborat.

Cerințele nefuncționale includ:

1) restricții de mediu şi realizare;

2) productivitatea (viteza, capacitatea de trecere, timpul de reacție, memoria folosită);

3) dependența de platformă;

4) expansivitatea;

5) fiabilitatea (utilitatea, exactitatea, timpul mediu de funcționare pînă la refuz, cantitatea erorilor la o mie de rînduri de program, cantitatea erorilor pe o clasă).

În cadrul elaborării cerințelor nefuncționale trebuie să fie folosite următoarele categorii de atribute ale calității:

1) caracter dirijabil;

2) rentabilitatea;

3) eficacitatea;

4) posibilitatea interacțiunii cu alte aplicații şi servicii;

5) accesibilitatea şi fiabilitatea;

6) capacitatea şi productivitatea;

7) posibilitatea introducerii corectărilor;

8) posibilitatea instalării;

9) testabilitatea;

10) capacitatea de menținere;

11) comoditatea folosirii;

12) securitatea.

Cerințele nefuncționale trebuie să fie folosite pentru prescripția atributelor calitative ale aplicației elaborate. Atributele calitative respective trebuie să fie folosite pentru alcătuirea planurilor de testare a aplicațiilor în conformitate cu cerințele nefuncționale (a se vedea 6.5).

6.1.1.4. Cerințele principale față de SI ale autorităților administrației publice

SI ale autorităților administrației publice trebuie să asigure:

1) accesul garantat şi sigur la resursele informaționale de stat accesibile;

2) posibilitatea căutării, colectării, prelucrării şi păstrării resurselor informaționale de stat;

3) posibilitatea acordării accesului la resursele informaționale globale şi locale autorităților administrației publice;

4) fiabilitatea funcționării şi stabilitatea în cazul defectelor software-ului sau hardware-ului, inclusiv în cazurile de acțiuni incorecte ale utilizatorilor;

5) schimbul operativ şi sigur de date între utilizatori;

6) posibilitatea extinderii ulterioare prin intermediul modernizării hardware-ului şi software-ului, adăugării componentelor noi la sistem;

7) alte funcții legate de direcția principală de activitate a autorităților administrației publice.

Cerințele față de SI ale autorităților administrației publice trebuie să fie documentate şi necesar de a verifica corespunderea lucrărilor în baza următoarelor categorii de sisteme:

1) sisteme tranzacționale şi de evidență care asigură susținerea îndeplinirii de către autoritățile administrației publice a sarcinilor şi funcțiilor de bază ale acestora;

2) sisteme de interacțiune informațională interdepartamentală între SI ale autorităților administrației publice;

3) sisteme de gestionare a resurselor, care asigură susținerea proceselor de afaceri şi a regulamentelor administrative în activitatea autorităților administrației publice;

4) sisteme informațional-analitice, care asigură colectarea, prelucrarea, păstrarea şi analiza datelor cu privire la rezultatele îndeplinirii sarcinilor şi funcțiilor de bază ale autorităților administrației publice de către acestea;

5) sisteme de circuit electronic al documentelor;

6) sisteme de gestionare a arhivelor electronice de documente;

7) sisteme de gestionare a exploatării (inclusiv sistemele de gestionare a componentelor de infrastructură);

8) sisteme de interacțiune cu persoanele fizice sau juridice, care asigură acordarea informației şi a serviciilor de informare, inclusiv portalurile şi centrele de deservire telefonică, de către autoritățile administrației publice prin Internet sau prin alte canale de legătură;

9) sisteme de asigurare a securității informaționale;

10) sisteme de birou, folosite de către colaboratorii autorităților administrației publice în activitatea lor zilnică pentru pregătirea documentelor şi schimbul de informație.

SI ale autorităților administrației publice trebuie să fie create în baza următoarelor principii:

1) accesibilitatea, veridicitatea, completitudinea şi oportunitatea acordării informației;

2) confidențialitatea — asigurarea delimitării accesului la resursele informaționale ale SI în limitele împuternicirilor acordate utilizatorilor;

3) deschiderea — posibilitatea integrării cu alte SI şi cu SI național;

4) capacitatea de dezvoltare a proporțiilor — posibilitatea extinderii ulterioare a posibilităților funcționale ale SI prin adăugarea de software şi hardware în componența lor, prin modernizare;

5) protecția — asigurarea integrității resurselor informaționale care fac parte din SI;

6) fiabilitatea funcționării şi stabilitatea SI.

6.1.1.5. Cerințele față de asigurarea securității informaționale a sistemelor informaționale ale autorităților administrație publice

Securitatea informațională în SI ale autorităților administrație publice trebuie să fie asigurată de un sistem, care include un complex de măsuri organizatorico-tehnice, precum şi software şi hardware pentru protecția informației.

Software-ul şi hardware-ul pentru protecția informației utilizate în SI ale autorităților administrației publice trebuie să fie licențiate, certificate şi să asigure:

1) identificarea resurselor informaționale protejate;

2) autentificarea utilizatorilor SI;

3) confidențialitatea informației care circulă în sistem;

4) schimbul autentificat de date;

5) integritatea datelor la formarea, transmiterea, utilizarea, prelucrarea şi păstrarea informației;

6) accesibilitatea autorizată a tuturor resurselor sistemului în condiții de exploatare normală;

7) delimitarea accesului utilizatorilor la resursele Sl;

8) administrarea (desemnarea drepturilor de acces la resursele SI, prelucrarea informației din jurnalele de înregistrare, instalarea şi dezinstalarea sistemului de protecție);

9) înregistrarea acțiunilor de intrare şi ieşire ale utilizatorilor, precum şi a încălcărilor drepturilor de acces la resursele SI;

10) controlul integrității şi capacității de lucru a sistemului de asigurare a securității informaționale;

11) securitatea şi funcționarea neîntreruptă a sistemului în situații excepționale.

6.1.2. Determinarea arhitecturii sistemului informațional

La această etapă este necesar a efectua analiza şi precizarea ierarhiei arhitecturii fizice a SI rezultante, a segmentelor de program şi a realizării construcției segmentelor. Datele inițiale pentru această etapă le constituie pachetul de cerințe de afaceri, care includ cerințele funcționale, nefuncționale şi de asigurare a securității SI.

La etapa determinării arhitecturii SI, trebuie să fie elaborate modelele detaliate ale rezultatelor atinse la etapa elaborării propunerii-business. Modelele elaborate includ modele arhitecturale în care este necesar a determina metoda de transformare a diferitelor componente funcționale în componente fizice (adică masa de lucru, serverul, baza de date, rețeaua).

La această etapă trebuie să fie elaborate planurile de testare pentru diferitele niveluri de testare (a se vedea capitolul 6.5):

1) testarea în bloc;

2) testarea modulului;

3) testarea sistemului (posibilitățile de integrare a sistemelor);

4) testarea interfețelor între sisteme;

5) testarea fişierelor de încărcare;

6) testarea de încărcare;

7) testarea securității;

8) testarea copierii de rezervă.

6.1.3. Determinarea limitelor realizării SI

La această etapă este necesar a efectua analiza proiectului şi planului de elaborare a SI. Trebuie să fie identificate restricțiile şi cerințele de program, inclusiv resursele ajutătoare, specificațiile, stabilirea deciziilor cu privire la procurarea sau elaborarea internă a componentelor necesare ale

aplicației.

Este determinat setul complet al elementelor sistemice viabile din punct de vedere tehnic şi comercial, din care este configurat SI.

Este necesar a examina arhitectura SI şi schema structurală a acesteia cu asocieri dintre elemente, de a determina interfețele cele externe în raport cu sistemul şi între componentele sistemului.

Este descris mediul de program al SI elaborat. Dacă SI elaborat constituie o extindere a unui SI existent deja, atunci sînt descrise, în primul rînd, caracteristicile suplimentare ale acesteia. Este prezentată lista software-ului şi hardware-ului necesare pentru funcționarea SI.

Este necesar a examina cîteva aspecte de compatibilitate: neuniformitatea mediului de program, limbajele de programare, formatele datelor şi ale mesajelor, formatele rapoartelor, formatele listing-urilor. Trebuie să fie discutată în special compatibilitatea cu software-urile diferite.

6.1.4. Analiza arhitecturii hardware-ului, comunicațiilor

La această etapă este necesar a verifica capacitatea hardware-ului ale SI a face față cerințelor noi şi în schimbare ce țin de organizarea afacerilor din partea unor astfel de componente ale infrastructurii precum rețelele, telecomunicațiile şi alte aplicații de software.

La etapa de proiectare sînt determinate atît arhitectura hardware-ului, cît şi cerințele nivelului inferior. Elaborarea arhitecturii constă în luarea unui şir de decizii succesive şi interconexe cu privire la structura hardware-ului SI. Elaborarea cerințelor de nivel inferior față de SI – formarea cerințelor față de anumite module de program.

Arhitectura SI include descrierea:

1) entităților fizice din care constă sistemul (nodurile rețelei, rețele);

2) fluxurilor informaționale între entitățile fizice în sistem;

3) specificațiilor canalelor de transmitere a informației în sistem;

4) alegerii platformei (platformelor) şi a sistemului operațional (sistemelor operaționale);

5) alegerii arhitecturii “fişier–server” sau “client–server”;

6) alegerii arhitecturii din 3 niveluri cu următoarele straturi: server, software-ul stratului intermediar (serverul de aplicații), software-ul clientului;

7) alegerii bazei de date centralizate sau distribuite.

Confirmarea cerințelor față de capacitatea, productivitatea şi accesibilitatea SI se referă la acțiunile de bază care sînt realizate la această etapă.

Rezultatele etapei:

1) determinarea cerințelor şi restricțiilor aplicate hardware-ului şi software-ului;

2) determinarea cerințelor funcționale, nefuncționale şi față de securitatea SI;

3) crearea ierarhiei arhitecturii de program a segmentelor şi funcțiilor aferente;

4) crearea arhitecturii echipamentului.

La această etapă, costul SI va include componentele cheltuielilor, indicate în tabelul 1.

Tabelul 1. Costul sistemului informațional la etapa „Colectarea şi analiza cerințelor față de sistemului informațional”

Nr. d/o	Componentele cheltuielilor	Costul lucrărilor organizațiilor externe	Costul lucrărilor personalului propriu	Costul cursurilor de instruire şi al certificării
1	Elaborarea documentației privind cerințele funcționale			
2	Elaborarea documentației privind cerințele față de interfețele externe			
3	Elaborarea documentației privind cerințele nefuncționale			
4	Elaborarea specificației cerințelor față de SI			
5	Elaborarea documentației privind cerințele față de software			
6	Verificarea şi validarea, definirea restricțiilor pentru SI			
7	Determinarea arhitecturii SI			
8	Determinarea restricțiilor de realizare a SI			
9	Planificarea administrării configurației software-ului			
10	Controlul configurației			
11	Alcătuirea rapoartelor privind configurație			
12	Determinarea arhitecturii hardware-ului			
13	Stabilirea cerințelor față de hardware			
14	Elaborarea modelului critic de			

	SI			
15	Stabilirea cerințelor cu privire la asigurarea securității informaționale			
16	Proiectarea software-ului			
17	Cheltuielile administrative legate de colectarea şi analiza cerințelor față de SI			
Total:				
Totalul pentru etapă:				

6.2. Determinarea unităților structurale şi a costurilor de livrare a software-ului şi hardware-ului

Scopul prezentei etape constă în determinarea unităților structurale şi a costului de livrare a software-ului şi hardware-ului, care vor fi incluse în costul SI.

Urmează să fie aplicat principiul Divizării structurale a lucrărilor pentru planificarea unităților structurale ale proiectului, pentru care este necesară estimarea costului.

Unitățile structurale şi livrările de software şi hardware, care trebuie să fie analizate la această etapă, includ următoarele:

1) gestionarea software-ului presupune rezolvarea unui spectru larg de sarcini:

- urmărirea defecțiunilor în calculatoarele gestionate, înlăturarea automată a cauzelor acestor defecțiuni, corectarea consecințelor lor şi acțiunile de prevenire a lor;

- gestionarea productivității calculatoarelor şi aplicațiilor;

- configurarea automată a calculatoarelor şi dispozitivelor de rețea;

- configurarea şi actualizarea software-ului;

2) proiectarea SI este definită ca un proces iterativ de obținere a modelului logic al SI împreună cu scopurile clar formulate, care sînt fixate pentru SI respectiv, precum şi cu elaborarea specificațiilor sistemului fizic, care să corespundă acestor cerințe;

3) elaborarea software-ului reprezintă specificarea destul de detaliată a cerințelor clientului şi a deciziei de proiect şi transformarea acestora în unul sau mai multe software-uri viabile;

4) testarea software-ului constituie una din etapele principale de verificare a calității software-ului elaborat;

5) mediul de elaborare a software-ului reprezintă un sistem de mijloace de program folosit de către programatori pentru elaborarea software-ului. Mediul de elaborare include:

- redactorul de texte;

- compilatorul şi/sau interpretatorul;

- mijloacele de automatizare a asamblării şi reglementatorul;

- sistemul de gestionare a versiunilor;

- instrumentele pentru simplificarea construirii interfeței grafice a utilizatorului;

- browser-ul claselor, inspectorul obiectelor şi diagrama ierarhiei claselor;

6) nivelul sistemic de susținere a testării include testarea software-ului elaborat, testarea nivelului sistemic al software-ului, susținerea asamblării, testările şi procedurile de dare a software-ului în exploatare;

7) asamblarea, testarea şi procedura de dare a software-ului în exploatare – software-ul pregătit este transmis clientului, sînt efectuate testările de predare-primire, este realizată instruirea utilizatorilor şi exploatarea experimentală, după care software-ul este pus pe mentenanță şi începe exploatarea productivă a software-ului;

8) sistemul de asigurare a calității este orientat spre asigurarea nivelului necesar de obiectivitate şi veridicitate a rezultatelor elaborării şi implementării software-ului, precum şi spre asigurarea calității necesare a producției produse şi/sau serviciilor prestate ale organizației;

9) verificarea independentă şi confirmarea potrivirii SI.

Aceste categorii de Divizare structurală a lucrărilor includ procesele ciclului de viață a elaborării SI.

Rezultatele etapei:

1) determinarea livrărilor de software şi hardware;

2) determinarea unităților structurale ale SI.

La această etapă, în costul SI vor fi incluse componentele cheltuielilor, indicate în tabelul 2.

Tabelul 2. Costul sistemului informațional la etapa „Determinarea unităților structurale şi a costului de livrare a software-ului şi hardware-ului”

Nr. d/o	Componentele cheltuielilor	Costul de achiziție	Costul de organizare a tenderelor	Costul lucrărilor adiționale pentru punerea în exploatare
1	Determinarea componentelor software-			

	ului şi hardware-ului			
2	Mediul de elaborare a software-ului			
3	Instrumentele de gestionare a bazei de date			
4	Instrumentele de monitorizare a sistemului			
5	Instrumentele de evidență a sistemului			
6	Instrumentele de generare a rapoartelor			
7	Cheltuielile pentru monitorizarea sistemului			
8	Instrumentele de diagnosticare a hardware-ului şi software-ului			
9	Instrumentele de analiză şi proiectare			
10	Instrumentele de testare			
11	Stațiile de lucru şi accesoriile			
12	Imprimante, scannere, xeroxe			
13	Dispozitive de păstrare a datelor			
14	Servere			
15	Echipament pentru încăperea de servere			
16	Instrumentele de asigurare a securității informaționale			
17	Costul pentru închirierea hardware-ului şi software-ului			
18	Echipament de rețea			
19	Suportul de mentenanță			
20	Sisteme de operare			
21	Actualizarea software-ului			
22	Licențe			
23	Servicii de comunicații			
24	Programe pentru comunicații			
25	Instruirea, reciclarea, instructajul personalului			
26	Cheltuielile administrative			

	legate de definirea unităţilor structurale şi livrările de software şi hardware			
Total:				
Total pentru etapă:				

6.3. Estimarea mărimii segmentului de programare al sistemului informaţional

Scopul prezentei etape constă în determinarea mărimii segmentului de programare al SI.

Unitatea industrială de măsurare a mărimii software-ului este cantitatea rîndurilor iniţiale ale codului — Source Lines of Code (SLOC). Prin rîndurile codului SLOC se subînţeleg rîndurile logice ale codului, şi anume: rîndurile în înţelegerea limbajului de programare folosit, fără a lua în consideraţie comentariile.

Evaluarea mărimii software-ului SI are loc în felul următor:

1) divizarea şi gruparea cerinţelor funcţionale de program şi cerinţelor faţă de SI ale autorităţilor administraţiei publice în categorii ale moştenirii de program.

Categorii ale moştenirii de program includ:

- proiect nou şi cod nou;
- proiect analogic şi cod nou;
- proiect analogic şi cod utilizat de multe ori;
- proiect analogic şi cod extins utilizat de multe ori.

Cerinţele nefuncţionale şi cerinţele faţă de interfeţe sînt utilizate pentru alcătuirea planurilor de testare la testarea software-ului şi a aplicaţiilor.

Ulterior, categoriile moştenirii de program vor fi folosite în calitate de multiplicatori pentru corectarea volumului de lucrări pentru moştenirea de program (a se vedea punctul 6.4.2.2, formula (3), tabelul 6);

2) evaluarea dimensiunii fiecărei funcţii de program în conformitate cu coeficienţii prezentaţi în tabelul 3.

Tabelul 3. Estimarea KSLOC a dimensiunilor de bază a software-ului pentru modelul COCOMO II

Dimensiunea SI	KSLOC	Unitatea de măsură
Mic	2	mii rânduri ale codului
Nu prea mare	8	mii rânduri ale codului
Mediu	32	mii rânduri ale codului
Mare	128	mii rânduri ale codului
Foarte mare	512	mii rânduri ale codului

Pentru calcularea KSLOC, este necesar a folosi formula:

$$KSLOC = \frac{(SLOCP \times K_p + SLOCI \times K_i + SLOCR \times K_r)}{1000}, \quad (1)$$

unde:

- KSLOC - numărul miilor de rînduri ale codului;

- SLOCP - codul care asigură o anumită logică a funcționării sistemului. De obicei, acestea sînt clasele care descriu caracteristicile obiectelor sistemului, legătura dintre funcțiile-business;

- SLOCI - codul care prelucrează elementele interfeței şi o unește cu alte părți ale sistemului. De obicei, acestea sînt clasele de prelucrare a erorilor de introducere a datelor, de înregistrare a datelor în baza de date:

- SLOCR - codul care descrie interfața sistemului. De obicei, acesta este codul care descrie interfața însăşi. Pentru componentele care funcționează în mediul Internet acesta este codul HTML;

- Kp - factorul modificării logicii funcționării sistemului;

- Ki - factorul modificării prelucrării elementelor de interfață ale sistemului;

- Kr - factorul modificării interfeței sistemului.

Factorii K sînt selectați pe cale experimentală şi sînt măsurați de la 0,01 — 0,6 şi mai sus de 0,6 la crearea unui sistem nou. Pentru determinarea factorilor K este folosită abordarea statistică, care ajută la modificarea evaluărilor apriorice cu luarea în considerație a datelor cercetărilor noi;

3) calcularea mărimii totale a segmentului de programare al SI în KSLOC, sumînd datele obținute în punctul 2 pentru fiecare funcție de program.

Metodele alternative de evaluare a segmentului de programare al SI sînt prezentate în anexa nr. 1.

Rezultatele etapei:

1) mărimea software este evaluată pentru fiecare categorie funcțională a moştenirii KSLOC;

2) evaluarea totală de program a dimensiunii KSLOC.

La această etapă costul SI va include componentele cheltuielilor, indicate în tabelul 4.

Tabelul 4. Costul sistemului informațional la etapa „Aprecierea mărimii segmentului de programare al sistemului informațional”

Nr. d/o	**Componentele cheltuielilor**	**Costul lucrărilor organizațiilor externe**	**Costul lucrărilor personalului propriu**	**Costul cursurilor de instruire şi al certificării**
1	Elaborarea documentației de apreciere a mărimii segmentului de programare al SI			
2	Determinarea mărimii segmentului de programare al			

	SI			
3	Analiza datelor statistice din domeniul dat			
4	Cheltuielile administrative legate de aprecierea mărimii segmentului de programare al SI			
Total:				
Totalul pentru etapă:				

6.4 Estimarea volumului lucrărilor

Pentru estimarea resurselor umane (în persoane pe lună), a duratei (în zile calendaristice) şi a costului (în unități monetare) este necesar a se baza pe statistica din experiența anterioară. În cazul absenței datelor istorice sau dacă se lucrează asupra unui proiect nou, este necesar a aplica metodici speciale, care permit evaluarea prealabilă a cheltuielilor pentru proiectul planificat.

6.4.1. Identificarea categoriilor Divizării structurale a lucrărilor, atributele cărora vor influența asupra dimensiunii şi volumului lucrărilor

Este necesar de identificat categoriile Divizării structurale a lucrărilor, atributele cărora vor influența asupra dimensiunii şi volumului lucrărilor conform devizului de cheltuieli al proiectului, din punctul de vedere al moştenirii şi riscului. Categoriile de bază ale riscurilor vor fi următoarele:

1) noile tehnologii: codul, limbajul de programare sau metoda de proiectare. Alegerea limbajului de programare mai poate avea şi o influență substanțială asupra securității SI. Cele mai bune limbaje de programare sînt cele în care toate acțiunile sînt determinate şi întemeiate, sînt susținute funcțiile care reduc numărul erorilor, este efectuat controlul asupra distribuirii memoriei şi utilizării indicatorilor. Acest grup de riscuri cuprinde riscurile legate de tehnologiile folosite, incompatibilitatea limbajelor de programare, necorespunderea metodelor de proiectare;

2) nivelul redus de pregătire a tehnologiilor – expirarea termenului de valabilitate a licenței, învechirea morală a tehnologiilor, apariția unei tehnologii principial noi, care face imediat unele produse şi servicii neactuale;

3) presupunerile optimiste, legate de moştenirea elementelor SI;

4) posibilitatea utilizării multiple a codului — sporirea numărului de erori în legătură cu alcătuirea incorectă a codului de program, folosit de multe ori;

5) riscul legat de furnizorii de software şi hardware — este necesar a crea nişte proceduri formale de gestionare a riscurilor legate de furnizori. La această categorie de riscuri se mai referă şi riscurile formării prețurilor, legate de imprecizia indicatorilor economici ai proiectelor, riscurile valutare;

6) riscul protecției insuficiente a proprietății intelectuale: posibilitatea încălcării patentelor şi furtului de proprietate intelectuală pe piețele în dezvoltare;

7) riscurile legate de servicii şi de deservirea tehnică: lipsa unor servicii inginereşti specializate, a forţei de muncă calificate şi a echipamentului substutuit;

8) elaborarea în paralel a dispozitivelor;

9) cantitatea interfeţelor între numeroasele subdiviziuni ale elaboratorilor;

10) riscurile de infrastructură – probleme de conectare la reţea şi lipsa accesului la sistemele de emitere şi distribuire;

11) distribuirea geografică a numeroaselor subdiviziuni ale elaboratorilor;

12) gradul înalt de complexitate a elementelor SI;

13) abilităţile profesionale şi experienţa personalului – această categorie de riscuri necesită o atenţie deosebită. Conducătorul proiectului trebuie să aprecieze riscurile şi să organizeze instruirea pînă la începutul proiectului pentru a nu pierde în viitor timpul cu erori;

14) cerinţele nedeterminate sau incomplete – procesul de elaborare a SI începe cu determinarea cerinţelor şi variantelor de utilizare a sistemului. Problema principală constă în faptul că unele cerinţe-cheie pot fi omise, alte cerinţe pot să nu fie înţelese corect de către elaboratori. O altă categorie de riscuri legată de cerinţe este realizarea cerinţelor auxiliare şi amînarea cerinţelor de bază;

15) riscurile legate de outsourcing;

16) riscurile politice – riscuri legate de politica corporativă a părţilor care interacţionează, precum şi de caracteristicile organizaţiilor şi activitatea subdiviziunilor componente.

Pentru fiecare categorie de riscuri, coeficientul mediu ponderat al influenţei asupra mărimii şi volumului lucrărilor este determinat conform abordări statistice, care contribuie la modificarea evaluărilor apriorice cu luarea în consideraţie a datelor cercetărilor noi.

6.4.2. Transformarea mărimii software-ului în volumul lucrărilor

Scopul constă în transformarea mărimii software-ului, obţinute în conformitate cu subcapitolul 6.3 (formula (1)), în volumul lucrărilor. Elaborarea software-ului include inginerii de program, tehnicienii de sistem, testatorii, programatorii, precum şi: elaborarea şi analiza cerinţelor de integrare şi testare a software-ului. Volumul lucrărilor şi costul altor categorii ale Divizării structurale a lucrărilor sînt calculate în punctele următoare cu utilizarea altor metode.

Calcularea volumului lucrărilor se efectuează în luni lucrătoare (LL) pentru următoarele categorii ale Divizării structurale a lucrărilor: ”Proiectarea SI”, “Elaborarea software” şi “Testarea software”.

6.4.2.1. Evaluarea cheltuielilor de lucru şi a volumului lucrărilor pentru proiectarea sistemului informaţional

Analiza şi proiectarea sînt determinante la construirea SI. Se evidenţiază trei faze de analiză şi proiectare a SI:

1) examinarea şi analiza sistemică a SI existent şi identificarea neajunsurilor acestuia;

2) generalizarea rezultatelor analizei sistemice şi crearea concepției provizorii a SI nou sau modernizat;

3) elaborarea proiectului sistemic al complexului de programe şi baze de date, care determină metodele şi mijloacele proiectării detaliate ulterioare şi ale întregului ciclu de viață al SI şi al bazei de date.

Analiza sistemică este importantă pentru proiectarea reuşită a SI, de aceea poate fi examinată ca unul din factorii de risc. Pentru realizarea lucrărilor de proiectare a SI pot fi implicate organizațiile specializate, care posedă experiență de proiectare a unor astfel de proiecte, sau structurile analitice proprii, care cunosc procesele-business ale organizației. Lucrările de proiectare a SI sînt îndeplinite cel mai eficient de către un grup de proiect combinat.

La realizarea analizei sistemice sînt obținute următoarele rezultate:

1) descrierea proceselor-business şi informaționale, care s-au stabilit în organizație;

2) locurile înguste în procesele-business şi modalitățile de lichidare a acestora;

3) modelul informațional şi funcțional al SI;

4) lista cerințelor față de SI nou sau modernizat;

5) metodele şi mijloacele de proiectare şi realizare a SI;

6) planul provizoriu mărit de proiectare a SI;

7) fundamentarea tehnico-economică.

Cheltuielile de lucru pentru proiectarea SI includ plata pentru lucrul specialiştilor organizațiilor terțe, conform condițiilor contractului semnat, precum şi plata pentru lucrul structurilor analitice proprii.

Volumul lucrărilor pentru proiectarea SI este determinat conform contractului încheiat cu specialiştii organizațiilor terțe în care se indică volumul lucrărilor îndeplinite şi termenele de îndeplinire a acestora, precum şi conform instrucțiunilor de funcție ale personalului propriu.

Volumul lucrărilor pentru proiectarea SI la secțiunea descompunerii categoriilor de bază ale Divizării structurale a lucrărilor în raport procentual este determinat conform metodicii şi analizei statistice SEER–SEM (a se vedea punctul 6.4.3(2), tabelul 11) sau conform metodei statistice (Anexa 1).

Proiectarea SI cuprinde trei domenii principale:

1) proiectarea obiectelor de date, care vor fi realizate în baza de date;

2) proiectarea programelor, formelor de ecran, rapoartelor care vor asigura efectuarea

interpelărilor la date;

3) evidența mediului concret sau a tehnologiei concrete, şi anume: a topologiei rețelei, configurației hardware-ului, prelucrării paralele, prelucrării distribuite a datelor.

6.4.2.2. Transformarea mărimii fiecărei funcții de program în volumul lucrărilor pentru elaborarea software-ului

Transformarea mărimii fiecărei funcții de program în volumul lucrărilor pentru elaborarea software-ului se calculează in felul următor:

1) calcularea volumului lucrărilor pentru elaborare - conform formulei (2).

$$\text{Volumul lucrarilor pentru elaborarea software} = \frac{Marimea_obtinuta}{Productivitatea_de_program}, \quad (2)$$

unde
- *Volumul lucrărilor pentru elaborarea software* - măsurat în luni lucrătoare (LL);
- *Productivitatea de program* - măsurată în SLOC/PM;
- *Mărimea obținută* – măsurată în SLOC.

Pentru determinarea productivității de program se folosesc datele din proiectul analogic de program. Dacă datele proiectului analogic sînt inaccesibile, se foloseşte tabelul 3. Indicatorii productivității, prezentați în tabelul 5, reflectă procesul de elaborare a software-ului.

Tabelul 5. Productivitatea elaborării de program pentru proiectele industriale medii

Caracteristica	Productivitatea elaborării de program (SLOC/PM)
Indicatori clasici	130–195
Metodele în dezvoltare	244–325
Software nou incorporat	17–105

2) corectarea volumului lucrărilor pentru evaluarea fiecărei categorii a Divizării structurale a lucrărilor se efectuează conform formulei (3), folosind multiplicatorii volumului lucrărilor pentru moştenirea de program, prezentați în tabelul 6.

*Volumul_lucrărilor_corectat=Volumul_lucrărilor * Multiplicatorul_volumului_lucrărilor,* (3)

unde
- *Volumul_lucrărilor_corectat* - măsurat în luni lucrătoare (LL);
- *Volumul_lucrărilor* - măsurat în luni lucrătoare (LL);
- *Multiplicatorul_volumului_lucrărilor* – este indicat în tabelul 4.

Tabelul 6. Multiplicatorii volumului lucrărilor pentru moştenirea de program

Categoria moştenirii de program	Multiplicatorul volumului lucrărilor
Proiect nou şi cod nou	1,2
Proiect analogic şi cod nou	1,0
Proiect analogic şi cod, care este folosit de	0,8

multe ori	
Proiect analogic şi cod extins, care este folosit de multe ori	0,6

3) adunarea volumului corectat al lucrărilor pentru fiecare categorie funcțională şi de program a moştenirii pentru a ajunge la volumul total al lucrărilor.

6.4.2.3. Estimarea cheltuielilor de lucru pentru elaborarea software-ului

Cheltuielile de lucru pentru elaborarea software-ului pot include plata pentru lucrul specialiştilor organizațiilor terțe conform condițiilor contractului semnat, precum şi plata pentru lucrul personalului propriu.

6.4.2.3.1. Cheltuielile de lucru pentru outsourcing la elaborarea software-ului

Outsourcing este definit ca refuzul de elaborare a software-ului de către personalul propriu şi procurarea serviciilor de elaborare a acestuia de la alte organizații.

Outsourcing-ul la elaborarea software-ului poate include următoarele tipuri de servicii:

1) elaborarea software-ului;
2) susținerea software-ului;
3) refactoring-ul şi reengineering-ul aplicațiilor;
4) implementarea software-ului elaborat;
5) documentarea software-ului;
6) instruirea personalului clientului;
7) consultanță în domeniul de TI.

La luarea deciziei privind utilizarea outsourcing-ului pentru elaborarea software-ului trebuie să fie luați în considerație următorii factori:

1) costul propriilor elaborări în raport cu costul serviciilor de outsourcing;
2) riscurile de încălcare a regimului securității informaționale;
3) riscurile întreruperii relațiilor cu compania de outsourcing şi dezvoltarea ulterioară a aplicației create;
4) particularitățile organizării şi gestionării proceselor de elaborare în cadrul companiei;
5) gradul de încredințare de către organizația terță a unor secrete ale sale.

Outsourcing-ul permite utilizarea experienței profesioniştilor, reducerea riscurilor şi a cheltuielilor, sporind randamentul mijloacelor investite.

Cheltuielile de lucru pentru elaborarea software-ului de către specialiştii organizațiilor terțe includ plata lucrărilor de acordare a serviciilor pentru elaborarea software-ului, conform condițiilor contractului încheiat.

6.4.2.3.2. Cheltuielile de lucru pentru elaborarea software-ului de către personalul propriu

Estimarea cheltuielilor de lucru pentru elaborarea software-ului se determină în baza numărului de rînduri ale codului. Formula de bază pentru estimarea cheltuielilor de lucru prin utilizarea modelului COCOMO II:

$$E = a \times KSLOC^{b} \times EAF \ , \quad (4)$$

unde:

- *E* - cheltuielile de lucru exprimate în luni lucrătoare;

- *a, b* - constantele care depind de regimul utilizării modelului (a se vedea tabelele 4, 5);

- *KSLOC* - numărul miilor de rînduri ale codului;

- *EAF* - factorul corectării cheltuielilor de lucru.

Sînt prevăzute trei regimuri de utilizare a modelului COCOMO II în funcție de mărimea echipei şi a proiectului (tabelul 7).

Tabelul 7. Regimurile modelului COCOMO II

Denumirea regimului	Mărimea proiectului	Descrierea
Organic	Până la 50 KSLOC	Proiectul nu prea mare este elaborat de o echipă nu prea mare, căreia nu-i sunt caracteristice inovațiile, iar mediul rămâne stabil
Blocat	50–300 KSLOC	O echipă relativ nu prea mare se ocupă de un proiect de proporții medii, în procesul elaborării sunt necesare anumite inovații, mediul este caracterizat prin instabilitate nesemnificativă
Implementat	Mai mult de 300 KSLOC	O echipă mare de elaboratori lucrează asupra unui proiect mare, este necesar un volum considerabil de inovații, mediul constă din numeroase elemente, care nu sunt caracterizate prin stabilitate

Valorile de bază ale coeficienților modelului COCOMO II în funcție de regim sînt prezentate în tabelul 8.

Tabelul 8. Valorile de bază ale coeficienților modelului COCOMO II în funcție de regim

Denumirea regimului	Valoarea coeficientului ***a***	Valoarea coeficientului ***b***
Organic	2,4	1,05
Blocat	3,0	1,12
Implementat	3,6	1,20

Factorul corectării cheltuielilor de lucru EAF sporeşte sau reduce cheltuielile de lucru în funcție de factorii mediului de elaborare. Calcularea factorului corectării cheltuielilor de lucru se efectuează după formula (5):

$$EAF = \prod_{i=0}^{n} C_i \quad , \quad (5)$$

unde:

- Ci - este unul din factorii mediului de elaborare.

Determinarea factorilor corectării cheltuielilor de lucru EAF:

1) Factorul Evidenței Tehnologiei de Elaborare (FETE). În cadrul acestui factor se duce evidența creşterii volumului cheltuielilor de lucru în urma implicării unui număr diferit de angajați.

Următoarele categorii de angajați sînt implicate în acest proces:

- categoria “A”: managerul proiectului; managerul elaborării sistemului de program; managerul implementării software-ului; managerul exploatării; managerul mentenanței software-ului; analistul proceselor-business; proiectantul business; analistul de sistem; tehnologul proceselor-business;

- categoria “B”: programatorul; proiectantul sistemului de program; proiectantul interfeței utilizatorului; integratorul; scriitorul tehnic; administratorul de sistem; administratorul bazelor de date; specialistul în gestionarea configurației;

- categoria “C”: testatorul; testatorul serviciului de mentenanță; elaboratorul testelor; analistul serviciului de mentenanță.

Durata testării este o valoare ce depinde de durata codificării şi se determină cu coeficientul Ktest, care se calculează după formula (6):

$$\frac{ltest}{l} = Ktest \quad , \ (6)$$

unde:

- *l* - durata procesului de codificare exprimată în luni lucrătoare;

- *ltest* - durata procesului de testare exprimată în luni lucrătoare.

Calcularea Factorului Evidenței Tehnologiei de Elaborare exprimată în luni lucrătoare se efectuează după formula (7):

$$FETE = \frac{A \times (1 + Ktest) + C \times Ktest}{B} + 1 + Ktest \quad , \ (7)$$

unde:

- *A, B, C* — numărul angajaților din categoriile respective.

Calcularea duratei elaborării exprimată în luni lucrătoare se efectuează după formula (8):

$$L = l \times (1 + Ktest) \quad , (8)$$

2) Factorul Evidenței Complexității şi Experienței de Elaborare (FECEE) este determinat în mod empiric şi este alcătuit din valorile prezentate în tabelul 9.

Tabelul 9. Valorile de bază ale coeficienților Factorului Evidenței Complexității şi Experienței de Elaborare

Factorul evidenței complexității şi experienței de elaborare	Valoarea
Trebuie să corectăm ceea ce este	1,00
S-a făcut mai înainte, există experiență	1,10
Există experiență şi nu se văd dificultăți	1,30

Experienţă nu este, dar există asistenţă	2,00
Nu există nici experienţă, nici asistenţă	4,00

Această metodă de evaluare este folosită la etapa incipientă a proiectului pentru evaluarea întregului proiect. Aplicarea acesteia este dificilă pentru proiectele mici şi pentru volumele mici de lucrări.

6.4.3 Finalizarea estimării volumului lucrărilor

Scopul pasului dat constă în extinderea evaluării pentru a acoperi toate categoriile Divizării structurale a lucrărilor. Pînă la acest pas sînt evaluate următoarele categorii ale Divizării structurale a lucrărilor: ”Proiectarea SI”, “Elaborarea software” şi “Testarea software”. Volumul lucrărilor, cum sînt “Gestionarea volumului de program al lucrărilor” şi “Sistemul de asigurare a calităţii” este suplimentar la volumul lucrărilor pentru elaborarea software-ului.

1) În scopul obţinerii estimării costului lucrărilor pentru toate categoriile enumerate este necesar a adăuga volumul suplimentar al lucrărilor de elaborare a software-ului la volumul lucrărilor evaluat anterior. Volumul suplimentar al lucrărilor de elaborare a software-ului este procentul volumului de lucrări de elaborare a software-ului pentru activitate suplimentară, din volumul total al lucrărilor, pentru toate elementele de lucru ale Divizării structurale a lucrărilor. Volumul suplimentar al lucrărilor de elaborare a software-ului este prezentat în tabelul 10.

Tabelul 10. Volumul suplimentar al lucrărilor de elaborarea software-ului

Categoria Divizării structurale a lucrărilor	Volumul suplimentar al lucrărilor de elaborarea software-ului, %
Gestionarea software	Adăugaţi 6–27%
Nivelul sistemic de susţinere a testării	Adăugaţi 34–112%
Sistemul de asigurare a calităţii	Adăugaţi 6–11%
Verificarea independentă	Adăugaţi 9–45%
Activitatea suplimentară:	
gestionarea configuraţiei proiectelor	Adăugaţi 3–6%
gestionarea proiectelor	Adăugaţi 8–11%
gestionarea livrărilor de software şi hardware	Adăugaţi 11–22%
finisarea	Adăugaţi 17–22%
Exploatarea, primii cinci ani	Adăugaţi 22% din volumul lucrărilor pentru elaborarea software-ului în decursul unui an de exploatare

2) Adunaţi volumul total al lucrărilor pentru fiecare categorie a Divizării structurale a lucrărilor care nu se referă la elaborarea software-ului pentru a obţine volumul total de lucrări. Descompunerea volumului lucrărilor categoriilor principale ale Divizării structurale a lucrărilor conform metodicii şi analizei statistice SEER–SEM este prezentată în tabelul 11.

Tabelul 11. Descompunerea elaborării software-ului

Categoria Divizării structurale a lucrărilor	% din volumul lucrărilor pentru elaborarea software-ului
Elaborarea software-ului:	100%
Analiza cerinţelor software-ului	12%
Elaborarea codului software-ului	55%

Implementarea software-ului	13%
Integrarea şi testarea de program	20%

SEER–SEM este un sistem de determinare şi evaluare a resurselor software, folosit pe larg şi creat în baza combinării matematicii şi statisticii.

Descompunerea volumului lucrărilor poate fi efectuată conform metodei statistice (Anexa 1).

Rezultatele etapei:

1) volumul lucrărilor de elaborare a software-ului pentru toate categoriile Divizării structurale a lucrărilor (în luni lucrătoare);

2) volumul total al lucrărilor pentru elaborarea software-ului.

La această etapă, costul SI va include componentele cheltuielilor indicate în tabelul 12.

Tabelul 12. Costul sistemului informaţional la etapa „Evaluarea volumului lucrărilor”

Nr. d/o	**Componentele cheltuielilor**	**Costul lucrărilor organizaţiilor externe**	**Costul lucrărilor personalului propriu**	**Costul cursurilor de instruire şi al certificării**
1	Identificarea Divizării structurale a lucrărilor			
2	Identificarea riscurilor			
3	Calcularea volumului lucrărilor de elaborare a software-ului			
4	Corectarea volumului lucrărilor de elaborare a software-ului			
5	Estimarea cheltuielilor de lucru pentru elaborarea software-ului			
6	Calcularea factorului de corectare a cheltuielilor de lucru			
7	Determinarea lucrărilor suplimentare de elaborare a software-ului			
8	Determinarea volumului de lucrări suplimentare pentru elaborarea software-ului			
9	Descompunerea elaborării a software-ului			
10	Cheltuielile administrative legate de evaluarea volumului de lucrări			
Total:				
Totalul pentru etapă:				

6.5. Cheltuielile de lucru pentru codificare şi testare

Scopul prezentei etape este de a determina perioada de timp şi a calcula cheltuielile de lucru

pentru codificare şi testare, necesare pentru finalizarea proiectului de program şi perioadele de executare a elementelor de lucru ale Divizării structurale a lucrărilor.

6.5.1. Volumul lucrărilor pentru codificare şi testare

Ca bază pentru estimarea cheltuielilor de lucru pentru elaborarea componentei de program vom lua estimarea cheltuielilor de lucru după numărul rîndurilor codului, conform formulelor (4), (5). Vom evalua fiecare cerință funcțională în parte şi vom presupune că valoarea constantei b este egală cu 1, deoarece cerința funcțională este parte componentă a proiectului. Volumul lucrărilor depinde de tipul lucrului, iar timpul pentru îndeplinirea acestuia depinde de productivitatea de program necesară pentru îndeplinirea sa. Productivitatea de program este o valoare egală cu proporția dintre volumul lucrului efectuat şi timpul în care a fost efectuat. Formula (4) se transformă în forma prezentată în formula (9):

$$E = \sum_i \sum_j \left(\frac{KSLOC(_{i,j})}{W_j} \times EAF\right) \quad , (9)$$

unde:

- W_j - productivitatea de program necesară pentru îndeplinirea tipului j de lucru;

- $KSLOC(_{i,j})$ - numărul rîndurilor codului la tipul de lucru j pentru realizarea cerinței i.

Productivitatea W se determină pe cale experimentală, reieşind din experiența de lucru asupra componentelor anterioare.

6.5.2. Determinarea duratei codificării şi testării

Codificarea este scrierea unui program proiectat deja, într-un anumit limbaj formal de programare. În procesul codificării sînt verificate anumite cerințe față de SI. Apoi începe testarea integrală a sistemului ca un tot întreg, care începe încă în procesul de codificare. Testarea este însoțită de verificarea codului inițial, căutarea erorilor după manifestările acestora în procesul îndeplinirii programului.

Durata codificării şi testării este exprimată în luni lucrătoare şi calculată după formula (10):

$$T = \sum_i \sum_j \left(\frac{KSLOC(_{i,j})}{W_i} \times FECEE(_i)\right) \times \frac{1}{P} \times (1 + Ktest) \quad , (10)$$

A se distribui timpul pentru fiecare categorie a Divizării structurale a lucrărilor şi a se determina încărcătura permisă de lucru. După alcătuirea planului de activități, a se verifica distribuirea lucrărilor conform experienței analogice, folosind tabelul 13 şi tabelul 14. Numerele din tabelul 13 şi tabelul 14 reprezintă orarul mediu, de bază. Deviațiile semnificative de la aceste date vor duce la creşterea riscului şi a costului.

Tabelul 13. Distribuirea timpului pe faze de elaborare a

software-ului, în baza datelor industriale

Faza	Datele (mijloacele) industriale
Analiza cerințelor	18%
Elaborarea software-ului	22%
Implementarea software-ului	36%
Integrarea şi testarea de program	24%

Tabelul 14. Distribuirea volumului lucrărilor pentru software-ului nou, modificat sau transformat în baza datelor industriale

Faza	Software-ul nou	Software-ul modificat existent	Software-ul transformat
Analiza cerințelor proiectului	20%	15%	5%
Proiectul de lucru, codul şi testul	57%	10%	5%
Integrarea şi testarea software-ului	23%	40%	30%
Volumul relativ al lucrărilor	100%	65%	40%

6.5.3. Cheltuielile de lucru pentru codificare şi testare

Cheltuielile de lucru pentru estimarea costului codificării şi testării exprimate în luni lucrătoare sînt calculate cu ajutorul formulei (11):

$$E = \sum_i \sum_j \left(\frac{KSLOC(_{i,j})}{W_j} \times FECEE(_i)\right) \times FETE \quad , (11)$$

La determinarea cheltuielilor de lucru pentru testare este important a lua în considerație cheltuielile de lucru pentru personalul din categoria “C” (a se vedea punctul 5.4.2.3) la alcătuirea planurilor de testare (a se vedea punctul 5.1.2).

Unul din elementele-cheie pentru asigurarea calității este testarea. Procesul de testare se efectuează în cîteva etape, care diferă după tipurile lucrărilor îndeplinite şi ale resurselor implicate.

Prima etapă de testare este testarea internă, în cadrul căreia este verificată completitudinea funcțională a SI, corespunderea documentației de proiect, corectitudinea deciziilor de proiect, precum şi corespunderea cu legislația.

Următoarea etapă este testarea externă, în cadrul căreia are loc concentrarea eforturilor experților cu experiență, care folosesc diferite metodologii şi abordări față de funcționarea SI.

Atît în cadrul testării interne, cît şi al celei externe, se efectuează permanent analiza statistică a numărului erorilor depistate şi corectate, în baza rezultatelor căreia se ia decizia de a trece la următoarea etapă.

La testarea finală este verificată realizarea cantității maxime a proceselor de afaceri şi sînt corectate erorile de la etapele anterioare.

Pentru această etapă de testare este necesar a acorda mai mult timp şi resurse de lucru pentru a garanta un grad înalt de fiabilitate a SI. Nivelul înalt al asigurării metodice, tehnice, organizaționale a testării la toate etapele determină calitatea înaltă a SI. Urmează exploatarea experimentală, care permite depistarea tuturor nuanțelor ce nu au fost identificate la etapele anterioare de testare.

Testarea este un proces ce implică tehnologii înalte şi cheltuieli de lucru mari. Acest proces necesită de la organizație disponibilitatea unei multitudini de resurse de echipament, program şi umane. În unele cazuri, este oportun a utiliza outsourcing-ul pentru testare.

Outsourcing-ul testării reprezintă transmiterea funcțiilor de evaluare a calității SI unei părți terțe, care se ocupă în mod profesional de testare. Pentru a asigura nivelul cuvenit al testării efectuate, este necesar a asigura calificarea suficientă a testatorilor, instrumente moderne de automatizare a testării, dotarea cu utilaj, care permite imitarea situației de exploatare reală a SI.

Încredințînd testarea SI unei părți terțe, este necesar a asigura garanția verificării şi evaluării anume a aspectelor care au nevoie de aceasta. În acest scop, este elaborat un plan şi un scenariu de testare, care descriu în detalii ce, în ce ordine, cu ce priorități, cu ce grad de meticulozitate, în ce mod, cu ajutorul căror instrumente şi în ce mediu va fi testat.

Procesul de testare trebuie să fie numaidecît documentat, şi anume: sînt necesare rapoartele şi protocoalele testării, care arată rezultatele şi dinamica evaluării efectuate.

Rezultatele etapei:

1) determinarea cheltuielilor de lucru pentru codificare şi testare;

2) distribuirea termenelor de îndeplinire a lucrărilor categoriilor Divizării structurale a lucrărilor.

La această etapă, costul SI va include componentele cheltuielilor, indicate în tabelul 15.

Tabelul 15. Costul sistemului informațional la etapa „Cheltuielile de lucru pentru codificare şi testare”

Nr. d/o	**Componentele cheltuielilor**	**Costul lucrărilor organizațiilor externe**	**Costul lucrărilor personalului propriu**	**Costul cursurilor de instruire şi al certificării**
1	Determinarea volumului lucrărilor de codificare			
2	Determinarea volumului lucrărilor de testare			
3	Determinarea factorului de mediu EAF			
4	Calcularea Factorului de Evidență a Tehnologiei de Elaborare			
5	Calcularea Factorului de Evidență a Complexității şi Experienței de Elaborare			

6	Calcularea duratei de codificare şi testare			
7	Calcularea cheltuielilor de lucru pentru codificare şi testare			
8	Distribuirea timpului după faze de elaborare a software-ului			
9	Crearea planului de elaborare a SI			
10	Elaborarea planurilor şi scenariilor de testare			
11	Cheltuielile administrative legate de estimarea cheltuielilor de lucru pentru codificare şi testare			
Total:				
Totalul pentru etapă:				

6.6. Determinarea caracteristicilor calității sistemului informațional

Scopul prezentei etape este de a determina caracteristicile interne şi externe ale calității, metodologia de analizare a calității, indicatorii calității şi de a determina lucrările necesare pentru îmbunătățirea calității SI, care necesită asigurare organizațională, tehnică şi metodologică.

Pentru a descrie caracteristicile calității SI sînt evidențiate următoarele procese:

1) selectarea şi argumentarea setului de date inițiale care reflectă particularitățile generale şi etapele ciclului de viață al SI, care influențează anumite caracteristici ale calității SI;

2) selectarea, stabilirea şi confirmarea parametrilor concreți şi a scărilor de măsurare a caracteristicilor şi atributelor calității SI pentru estimarea lor ulterioară şi compararea cerințelor specificațiilor în procesul testărilor de calificare sau al certificării la anumite etape ale ciclului de viață a SI.

6.6.1. Parametrii calității

La etapele inițiale ale ciclului de viață se stabilesc detaliat cerințele față de SI (a se vedea punctul 6.1.1). Cerințele detaliate necesare pentru funcționarea SI sînt stabilite de caracteristicile calității care precizează şi concretizează cerințele date față de conținutul şi realizarea lor.

La selectarea parametrilor calității, indicatorii principali sînt: potrivirea perfectă a parametrilor scopurilor calității, transparența şi claritatea interpretării şi eficacitatea economică de obținere a rezultatului.

Parametrii calității:

1) adaptabilitatea - măsură de flexibilitate a sistemului, estimează capacitatea SI de a se adapta la modificarea cerințelor sau la reproiectarea SI, sau la integrarea aplicațiilor;

2) complexitatea interfețelor şi integrării - parametru ce măsoară nivelul de complexitate al interfeței sau volumul suplimentar de lucrări de programare necesare pentru integrarea componentelor în SI, necesare pentru testare, corectare şi mentenanță;

3) aria de testare indică nivelul de completitudine al diverselor tipuri de testare;

4) fiabilitatea - parametru care determină probabilitatea funcționării SI fără refuzuri;

5) profilurile erorilor - parametru care măsoară numărul cumulativ al erorilor identificate.

Din punctul de vedere al posibilității şi exactității, caracteristicile, subcaracteristicile şi atributele calității SI se divizează în tipurile:

1) categoric – descriptiv, care reflectă setul de proprietăți şi caracteristici generale ale obiectului. La tipul dat se atribuie proprietățile software-ului şi ale setului de date, care cuprind scopul şi funcțiile SI. Utilitatea funcțională este cea mai importantă şi dominantă caracteristică a SI;

2) cantitativ - este reprezentat de o mulțime de puncte numerice ordonate care pot fi măsurate obiectiv şi contrapuse numeric cerințelor. Valorile caracteristicilor de acest tip influențează posibilitățile funcționale ale SI. Astfel de caracteristici sînt fiabilitatea şi eficacitatea software-ului. Fiabilitatea este reflectată de durata de lucru pînă la refuz, durata medie de restabilire şi coeficientul de pregătire. Caracteristicile cantitative ale calității sînt prezentate în tabelul 16;

3) calitativ – care conține cîteva valori ordonate sau separate care se caracterizează prin scara de ordin sau punctiformă, se stabilesc, se selectează şi se estimează subiectiv şi de către experți. Caracteristicile calitative ale calității SI sînt prezentate în tabelul 17.

Tabelul 16. Caracteristicile cantitative ale calității SI

Caracteristicile calității	Unitate de măsură	Intervalul valorilor
Fiabilitatea		
Nivelul de completare:		
durata de lucru până la refuz în lipsa restartării	oră	10–1000
Durabilitatea:		
durata de lucru până la refuz cu restartare	oră	10–1000
resursele relative pentru asigurarea fiabilităşii şi restartării	%	10–90
Capacitatea de restabilire:		
durata restabilirii	minut	10–2 – 10
Accesibilitatea-pregătirea:		
timpul relativ de funcționare SI cu menținerea capacității de lucru	probabilitatea	0,7–0,99
Eficacitatea		
Eficacitatea temporară:		
perioada de reacționare – primirea rezultatelor pentru sarcina tipică	secundă	1–1000
capacitatea de trecere - numărul sarcinilor tipice efectuate într-o unitate de timp	numere per minut	1–1000
Gradul de utilizare a resurselor:		
valoarea relativă a utilizării resurselor la funcționarea normală a software-ului	probabilitatea	0,7–0,99

Tabelul 17. Caracteristicile calitative ale calității SI

Caracteristicile calității	Unitate de măsură	Intervalul valorilor
Utilitatea		
Claritatea:		

exactitatea conceptului de SI	-	Excelentă; bună; satisfăcătoare; nesatisfăcătoare
capacitățile de demonstrare		
claritatea şi completitudinea documentației		
Simplitatea utilizării:		
simplitatea administrării funcțiilor	-	Excelentă; bună; satisfăcătoare; nesatisfăcătoare
confortul exploatării		
timpul mediu de introducere a sarcinilor	-	1 – 1000
timpul mediu de reacționare la sarcină		
Studierea		
dificultatea studierii aplicațiilor SI	om-oră	1 – 1000
durata studierii	oră	1 – 1000
volumul documentației de exploatare	pagini	1 – 1000
volumul manualelor electronice	kilobait	1 – 1000
Atractivitatea:		
estimări subiective sau ale experților	-	Excelentă; bună; satisfăcătoare; nesatisfăcătoare
Mentenabilitatea	-	Excelentă; bună; satisfăcătoare; nesatisfăcătoare
Comoditatea analizării:		
organizarea arhitecturii programelor	om-oră	1–1000
unificarea interfețelor	oră	1–1000
completitudinea şi corectitudinea documentației	-	Excelentă; bună; satisfăcătoare; nesatisfăcătoare
Modificabilitatea:		
volumul de lucru pentru pregătirea modificărilor	om-oră	1–1000
durata de pregătire a modificărilor	oră	1–1000
Stabilitatea:		
rezistența la manifestările negative apărute în urma modificărilor	-	Excelentă; bună; satisfăcătoare; nesatisfăcătoare
Testabilitatea:		
volumul de lucru pentru testarea modificărilor	om-oră	1–1000
durata testării modificărilor	oră	1–1000
Mobilitatea		
Adaptabilitatea:		

volumul de lucru necesar pentru adaptare	om-oră	1–100
durata adaptării	oră	1–100
Simplitatea instalării:		
volumul de lucru necesar pentru instalare	om-oră	1–100
durata instalării	oră	1–100
Coexistența-corespunderea:		
standardizarea interfeței cu mediul operațional şi echipamentul	-	Excelentă; bună; satisfăcătoare; nesatisfăcătoare
Substituibilitatea:		
volumul de lucru necesar pentru substituirea componentelor	om-oră	1–100
durata substituirii componentelor	oră	1–100

6.6.2. Caracteristicile interne şi externe ale calității sistemului informațional

Calitatea SI trebuie să fie conform caracteristicilor interne şi externe care sînt compuse din şase grupuri de indicatori de bază, fiecare dintre care este detaliat prin cîteva subcaracteristici normative:

1) utilitatea funcțională a SI:
- utilitatea pentru aplicare;
- corectitudinea (precizia, exactitatea);
- capacitatea de interacțiune;
- protecția;

2) fiabilitate SI:
- nivelul de completare (lipsa erorilor);
- rezistența la defecte;
- capacitatea de restabilire;
- accesibilitatea-pregătirea;

3) eficacitatea SI:
- eficacitatea temporară;
- gradul de utilizare a resurselor;

4) aplicabilitatea (caracterul practic) SI:
- claritatea;
- simplitatea utilizării;
- posibilitatea de studiere;
- atractivitatea;

5) mentenabilitatea SI:
- comoditatea analizării;
- modificabilitatea;
- stabilitatea;
- testabilitatea;

6) transferabilitatea (mobilitatea) SI:
- adaptabilitatea;
- simplitatea instalării;

- coexistenţa –corespunderea;
- substituibilitatea.

Fiecare caracteristică trebuie să fie însoţită suplimentar de o subcaracteristică „conformitatea”, care reflectă lipsa contradicţiilor cu documentele normative.

6.6.3. Caracteristicile calităţii software-ului în utilizare

Caracteristicile interne şi externe ale calităţii se referă nemijlocit la SI, iar caracteristicile calităţii în utilizare se manifestă prin efectul utilizării acestuia şi depind de mediul extern. Între caracteristicile calităţii există interdependenţă de sus în jos şi dependenţă de jos în sus, adică mărirea unei caracteristici poate duce la scăderea altei caracteristici şi invers.

Caracteristicile de bază ale calităţii software-ului în utilizare sînt:

1) eficacitatea de sistem a aplicării software-ului potrivit scopului său;

2) productivitatea - randamentul la soluţionarea sarcinilor de bază ale SI, obţinut cu resurse limitate într-un mediu extern concret de aplicare;

3) securitatea - fiabilitatea funcţionării complexului de software şi riscul ce poate decurge din aplicarea sa pentru oameni, afaceri şi mediul extern;

4) satisfacerea cerinţelor şi cheltuielilor utilizatorilor în conformitate cu scopurile utilizării SI.

6.6.2. Metodologia de apreciere a calităţii sistemului informaţional

Pentru a asigura completitudinea măsurării calităţii SI este necesară elaborarea parametrilor structurali ai calităţii la etapele iniţiale ale ciclului de viaţă al SI.

Măsurarea calităţii SI constă în calcularea devierii caracteristicilor reale ale SI de la normative.

Metodologia creării parametrilor calităţii SI constă din următorii paşi:

1) stabilirea nivelului nontehnic, destinat managerilor, utilizatorilor, clientului:
- formarea cerinţelor de calitate;
- selectarea proprietăţilor calităţii, stabilirea priorităţilor şi legăturii cu cerinţele;
- stabilirea pasajelor admisibile pentru valorile calităţii;

2) determinarea nivelului tehnic, destinat analiticilor, designerilor, elaboratorilor:
- realizarea descompunerii factorilor calităţii în caracteristici de software măsurabile;

3) determinarea nivelului inferior al ierarhiei – nivelul regulilor şi normelor elaborate, cărora va trebui să se conformeze SI pentru realizarea factorilor calităţii.

Estimarea metodologică a calităţii SI efectuată minuţios şi în conformitate cu scopurile elaborării SI creează baza pentru planificarea corectă şi controlul cheltuielilor referitoare la calitate, pentru realizarea indicilor necesari şi eficacitatea activităţii SI. Cheltuielile pentru estimarea calităţii SI includ remunerarea specialiştilor din propria organizaţie.

Rezultatele etapei:

1) determinarea caracteristicilor calităţii;

2) costul cheltuielilor de estimare a calităţii SI.

La etapa dată în costul SI vor fi incluse componentele cheltuielilor indicate în tabelul 18.

Tabelul 18. Costul sistemului informaţional la etapa „Determinarea caracteristicilor calităţii sistemului informaţional”

Nr. d/o	Componentele cheltuielilor	Costul lucrărilor organizaţiilor externe	Costul lucrărilor personalului propriu	Costul cursurilor de instruire şi al certificării
1	Determinarea caracteristicilor cantitative ale calităţii SI			
2	Determinarea caracteristicilor			

	calitative ale calității SI			
3	Determinarea caracteristicilor interne şi externe ale calității SI			
4	Evaluarea calității SI			
Total:				
Total pentru etapă:				

6.7. Calcularea costului sistemului informațional

Scopul - de a efectua estimarea costului total al proiectului pentru elaborarea SI, incluzînd livrările de software şi hardware şi Divizarea structurală a lucrărilor.

În costul total al SI sînt incluse:

1) cheltuielile capitale;

2) cheltuielile operaționale.

6.7.1. Cheltuielile capitale

Cheltuielile capitale sînt cheltuielile pentru achiziționarea noilor şi schimbarea vechilor active materiale şi nemateriale de lungă durată, utilizate în procesul de creare a SI.

Cheltuielile capitale includ şi costul livrărilor de:

1) hardware:

- costul echipamentului (prețul total al echipamentului, fără includerea amortizării);
- cheltuielile de amortizare (perioada de amortizare se calculează în funcție de tipul tehnicii);
- upgrade (include toate actualizările şi schimbările în configurația echipamentului, acestea sînt: schimbarea discurilor fixe, instalarea dispozitivelor suplimentare. Într-o subcategorie separată sînt incluse upgrade-urile de procesoare);
- memoria (cheltuielile pentru majorarea volumului memoriei atît pentru locurile clienților cît şi pentru celelalte dispozitive ce conțin module de memorie);
- dispozitive de păstrare a informației (disc drivere, discuri fixe, plăci de memorie, drive optic, sisteme de păstrare, streamere, dispozitive de stocare a datelor, flash carduri);
- periferice (imprimante, scanere, plottere);
- echipament de rețea (concentratoare, comutatoare, plăci de rețea (cu excepția celor încorporate în computerele clienților), routere, poduri şi altele);

2) software:

- sisteme operaționale;
- prețul licențelor;
- aplicații (pe lîngă aplicațiile de birou standard acestea includ şi software-ul specializat, elaborat de compania dată, precum şi de organizații terțe);
- programe de deservire (de diagnosticare, de corectare, programe defragmentatoare, criptografice, antivirus şi altele);
- programe pentru comunicații: diverse browsere, protocoale FTP de transfer al fişierelor, programe de e-mail, mijloacele de acces la distanța şi altele.
- determinarea costului cheltuielilor de transport legate de SI.

6.7.2. Cheltuielile operaționale

Cheltuielile operaționale sînt cheltuielile şi plățile legate de efectuarea într-o anumită perioadă de timp a operațiunilor financiare, de producere, administrative ce țin de procesul de susținere a SI. Cheltuielile operaționale includ cheltuielile pentru producerea şi realizarea produselor şi / sau oferirea serviciilor, cheltuielile administrative şi financiare.

La cheltuielile operaționale se referă:

1) plățile - plata pentru închirierea hardware-ului şi software-ului şi alte cheltuieli pentru echipament de computer, care nu sînt incluse în nici una din categoriile menționate;

2) administrarea:

- administrarea rețelei;
- diagnosticul şi reparația;
- gestionarea şi planificarea traficului;
- optimizarea productivității (se efectuează de către administratorul de sistem şi include identificarea zonelor înguste din rețea şi luarea măsurilor corespunzătoare);
- administrarea utilizatorilor (adăugarea, excluderea, modificarea drepturilor);
- suportul sistemelor operaționale;
- lucrările regulamentare curente (profilaxia);
- alte lucrări de administrare a rețelei;

3) administrarea sistemului:

- studierea şi planificarea dezvoltării sistemului;
- determinarea costului şi procurarea echipamentului;
- licențierea şi distribuirea software-ului;
- gestionarea bunurilor (echipamentului);
- administrarea aplicațiilor;
- controlul securității şi protecția contra viruşilor;
- configurarea şi resetarea echipamentului;
- instalarea echipamentului;
- alte sarcini de administrare a sistemului;
- administrarea dispozitivelor de păstrare a datelor;
- administrarea discurilor şi fişierelor;
- planificarea capacității dispozitivelor de păstrare a datelor;
- administrarea accesului la date;
- arhivarea şi copierea de rezervă;
- pronosticul defecțiunilor şi restabilirea;
- administrarea repository-ului;
- alte tipuri de administrare;

4) susținerea:

- activitatea operativă;
- ajutorul personalului administrativ;
- instruirea neregulată (personalul administrativ);
- susținerea producătorului;
- susținerea realizată de organizații externe (outsourcing);
- instruirea personalului administrativ;
- instruirea utilizatorului final;
- cheltuieli pentru deplasare;
- achiziții;
- alte cheltuieli pentru lucrul operativ;
- contracte de livrare;
- contracte de susținere;
- cursuri de instruire şi certificarea;

5) stabilirea nivelului profesional şi a remunerării personalului.

Rezultatele etapei:

1) costul livrărilor de software şi hardware;
2) stabilirea costului categoriilor de Divizare structurală a lucrărilor;
3) costul estimativ total al SI.

La etapa dată în costul SI vor fi incluse componentele cheltuielilor, indicate în tabelul 19.

Tabelul 19. Costul sistemului informațional la etapa „Calcularea costului sistemului informațional”

Nr. d/o	Componentele cheltuielilor	Costul lucrărilor organizațiilor externe	Costul lucrărilor personalului propriu	Costul cursurilor de instruire şi al certificării
1	Estimarea costului total al proiectului pentru elaborarea SI			
2	Realizarea lucrărilor curente regulamentare			
3	Studierea şi planificarea dezvoltării SI			
4	Cheltuielile administrative legate de calcularea costului SI			
Total:				
Total pentru etapă:				

6.8. Determinarea influenței riscurilor

Scopul prezentei etape de a determina riscurile proiectului pentru a estima influența lor asupra costului de elaborare.

6.8.1. Evaluarea influenței riscurilor asupra costului SI

Riscurile se evaluează în modul următor:

1) în baza listei inițiale a riscurilor (a se vedea punctul 5.4.1) de identificat riscul de bază care are cea mai mare influență asupra evaluării SI;

2) de evaluat influența generală a riscurilor (a se vedea tabelele 20, 21). De calculat influența generală a riscurilor prin înmulțirea valorilor evaluării influenței a riscurilor la costul tuturor cauzelor riscurilor. Evaluarea influenței a riscurilor asupra costului este prezentat în tabelul 21;

Tabelul 20. Evaluarea cauzelor riscurilor

Tipurile de riscuri	Evaluarea cauzelor riscurilor	
	Reduce riscul	Sporeşte riscul
Experiență şi abilități de lucru în echipă	Experiența de participare la elaborarea de software; Experiența de planificare şi de luare a deciziilor; Integrarea hardware-ului şi software-ului ale grupurilor	Lipsa experienței de elaborare a software-ului; Lipsa experienței de planificare; Hardware-ul şi software-ul ale grupului nu sunt integrate
Planificare	Planul detaliat şi revizuit; Suficient timp pentru	Lacune în planificare; La planificarea proiectului nu au

	elaborarea tuturor modulelor principale ale proiectului; Destinația corespunzătoare a rezervelor; Moştenirea software-ului se bazează într-un mod clar pe analiză	luat parte toate părțile interesate; O abordare simplificată a repartizării rezervelor; Presupuneri optimiste, neverificate, cu privire la moştenirea software-ului
Proiectare	Arhitectura de sistem şi de program completă, precum şi reguli clare care divizează sistemul în module; Decizii de sistem integrate se bazează atât pe hardware cât şi pe software; Procesul de elaborare a software-ului este proiectat ținând cont de creşterea ulterioară a funcționalității	Arhitectură de sistem şi de program cu o descriere neclară a bazelor de divizare funcțională a hardware-ul şi software-ul; Deciziile de sistem sunt luate fără a ține cont de influența lor asupra software; Presupunerea că nu va fi necesară modificarea şi dezvoltarea software-ului până la sfîrşitul ciclului de viață
Resursele umane	Nivel redus de fluctuație a cadrelor; Angajarea la timp a personalului pentru elaborarea software-ului; Păstrarea grupului de elaborare a programelor până la emiterea produsului	Nivel înalt de fluctuație a cadrelor; Completarea slabă cu personal; Planificarea de eliberare a grupului de elaboratori înainte de asamblarea, testarea şi procedura de dare în exploatare a software-ului
Testare	Standurile de testare sunt pregătite până la începutul elaborării; Un grup separat de testatori; Elaborarea la timp a planului de testare	Insuficiență de standuri de testare sau lipsa lor; Se planifică de a transforma grupul de elaboratori în grupul de testatori la finele elaborării; Lipsa planului de testare
Instrumente	Sistemul de gestionare corespunde mijloacelor de testare şi cerințelor proiectului; Mijloace de proiectare verificate	Lipsa sau insuficiența compatibilității sistemului de gestionare cu instrumentele de analiză a testării; Mijloace de proiectare nepotrivite

Tabelul 21. Evaluarea influenței riscurilor asupra costului

Cauzele riscului	Evaluarea influenței asupra costului		
	Înaltă	**Foarte înaltă**	**Cea mai înaltă**
Experiență şi abilități de lucru în echipă	1,02	1,05	1,08
Planificare	1,10	1,17	1,25
Proiectare	1,05	1,13	1,2
Resurse umane	1,02	1,05	1,13
Testare	1,05	1,08	1,15
Instrumente	1,02	1,03	1,1
Influența maximă pronosticată	1,3	1,6	2,32

3) de determinat influența riscurilor asupra costului SI după formula (12):

*Influența_riscului_asupra_costului=Costul_SI **

Influența_generală_a_riscurilor (12)

Costul total al SI se stabileşte în subcapitolul 6.7;

4) de reglat evaluarea riscului prin adăugarea factorului general al riscului la cost după formula (13):

$$\sum_{i=1}^{n}\left[\left(Influenta_i\right)*\left(Probabilitatea_cazului_i\right)\right], \quad (13)$$

unde

- *Influență* – influența riscurilor asupra costului SI;
- *Probabilitatea cazului* se stabileşte în mod experimental utilizînd abordarea statistică care ajută la modificarea evaluării apriorice ținînd cont de datele noilor cercetări.

6.8.2. Influența securității informaționale asupra funcționării sistemului informațional

Pentru minimalizarea influenței riscurilor de funcționare a SI este necesară respectarea şi controlul cerințelor de asigurare a securității informaționale a SI.

Cerințele de asigurare a securității informaționale a SI sînt:

1) planificarea asigurării securității informaționale – planul de asigurare a securității şi regulile de conduită a angajaților;

2) reacționarea la incidentele legate de încălcarea securității informaționale;

3) activități de asigurare a securității informaționale în situații imprevizibile – planul de acțiuni în situații imprevizibile, rezervarea serviciilor de telecomunicații, copierea de rezervă şi păstrarea informației, restabilirea datelor;

4) cerințe față de evaluarea riscurilor şi vulnerabilităților;

5) cerințe față de protejarea suporturilor de informație – marcarea, păstrarea, transportarea, curățarea, transmiterea şi distrugerea suporturilor de informație;
6) cerințe față de asigurarea integrității informației;
7) cerințe față de protejarea fizică a SI;
8) cerințe față de securitatea personalului de exploatare, precum şi față de informarea şi instruirea acestuia în probleme de securitate;
9) cerințe de identificare şi autentificare;
10) cerințe față de gestionarea accesului.

Asigurarea securității informaționale include cheltuielile pentru mijloacele de protejare a hardware-ului şi software-ului, cheltuielile pentru remunerarea specialiştilor în securitate informațională atît a organizațiilor externe, cît şi a personalului propriu.

Rezultatele etapei:
1) lista detaliată a riscurilor SI:
2) determinarea cerințelor de asigurare a securității informaționale;
3) sînt reevaluate: mărimea, volumul, planul lucrărilor, costul proiectului, ținînd cont de riscuri.

La etapa dată în costul SI vor fi incluse componentele cheltuielilor indicate în tabelul 22.

Tabelul 22. Costul sistemului informațional la etapa „Determinarea influenței riscurilor”

Nr. d/o	**Componentele cheltuielilor**	**Costul lucrărilor organizațiilor externe**	**Costul lucrărilor personalului propriu**	**Costul cursurilor de instruire şi al certificării**
1	Evaluarea influenței riscurilor asupra costului			
2	Reglarea evaluării riscului			
3	Reglarea cheltuielilor bazate pe evaluarea riscului			
4	Cheltuieli administrative legate de determinarea influenței riscului asupra costului			
5	Asigurarea securității informaționale			
Total:				
Total pentru etapă:				

6.9. Confirmarea şi corectarea estimării costului riscurilor

Scopul etapei – de a confirma şi corecta estimarea costului riscurilor.

Lista inițială a riscurilor (a se vedea punctul 5.4.1) se completează cu o listă suplimentară a riscurilor utilizînd:

1) evaluarea alternativă: atragerea unui individ sau a unui grup cu experiență corespunzătoare pentru obține o estimare a experților independenți;

2) analoguri istorice: folosind experiența precedentă, evaluarea se compară în conformitate cu următorii parametri:
- mărimea, volumul lucrărilor şi costul unui SI analogic;
- raportul dintre mărime şi scopul SI;
- raportul dintre mărime şi volumul lucrărilor şi cost (productivitatea elaborării);

- raportul dintre tehnologia utilizată la elaborare şi volumul de lucrări şi preț.

Pentru realizarea sarcinii date este necesar a compara lista inițială de riscuri (a se vedea punctul 5.4.1) cu riscurile suplimentare obținute în punctul precedent, a stabili diferența şi a elabora o listă nouă a riscurilor pentru obținerea indicatorilor mai exacți.

În continuare este necesară gestionarea şi corectarea listei de riscuri obținute.

Realizarea procesului de gestionare cuprinde:

1) evaluarea riscurilor pe parcursul ciclului de viață al SI;
2) determinarea şi clasificarea riscurilor;
3) determinarea cantitativă a influențelor nefavorabile ale riscurilor;
4) determinarea măsurilor de prevenire a riscurilor;
5) determinarea strategiei de gestionare a fiecărui risc identificat;
6) întocmirea raporturilor cu privire la riscuri şi starea lor.

Rezultatele etapei:

1) confirmarea corectitudinii evaluării;
2) sînt confirmate şi corectate: volumul lucrărilor, termenele de realizare, cheltuielile de deviz obținute cu o exactitate mai mare.

La etapa dată în costul SI vor fi incluse componentele cheltuielilor indicate în tabelul 23.

Tabelul 23. Costul sistemului informațional la etapa „Confirmarea şi corectarea estimării costului riscurilor”

Nr. d/o	**Componentele cheltuielilor**	**Costul lucrărilor organizațiilor externe**	**Costul lucrărilor personalului propriu**	**Costul cursurilor de instruire şi al certificării**
1	Evaluarea riscurilor efectuată de către un grup independent de experți			
2	Analiza datelor statistice din domeniul dat			
3	Compararea evaluărilor riscurilor			
4	Reglarea evaluării riscurilor			
5	Cheltuieli administrative legate de confirmarea şi corectarea estimării costului riscurilor			
Total:				
Total pentru etapă:				

6.10. Implementarea sistemului informațional

Scopul etapei este:

1) de a spori productivitatea muncii personalului;
2) de a reduce volumul de muncă necesar pentru realizarea proceselor concrete din contul spațiului informațional unic;
3) de a reduce erorile din contul creşterii posibilităților de analiză şi verificare a informației în cadrul SI.

Etapa de implementare se începe cu următoarele:

1) obținerea permisiunii pentru instalarea SI la locurile de funcționare;
2) pregătirea infrastructurii utilizatorului şi echipamentului încăperii în care va funcționa SI;
3) verificarea capacității de funcționare a SI în condiții reale de exploatare;
4) organizarea instruirii personalului lucrului cu SI sau componentele acestuia.

Sarcinile de implementare a SI sînt complexe, deoarece soluționarea lor presupune realizarea unui şir de acțiuni care include:

1) concentrarea resurselor umane şi financiare pentru soluționarea sarcinilor de implementare a SI;
2) elaborarea concepției de creare a unui SI unitar;
3) instruirea utilizatorilor;
4) instruirea administratorilor şi specialiştilor de profil îngust;
5) adaptarea SI la specificul proceselor din organizație;
6) realizarea proiectului-pilot al SI;
7) elaborarea bazei normative pentru activitatea în cadrul noilor tehnologii;
8) implementarea completă a SI în activitatea practică a organizației.

Pentru realizarea sarcinilor de implementare a SI este necesar a elabora planul de implementare a SI.

Planul-standard de implementare a SI cuprinde următoarele etape:

1) planificarea implementării – desemnarea managerului de proiect, asigurarea informării angajaților, recrutarea angajaților în grupul de implementare a SI;
2) instalarea sistemului – instalarea, testarea şi verificarea corectitudinii setărilor SI;
3) lansarea proiectului-pilot – instruirea utilizatorilor, transferul utilizatorilor la noul SI, colectarea opiniilor utilizatorilor şi finisarea SI în caz de necesitate, desemnarea unui grup de persoane responsabile de suportul SI (managerul responsabil de procesul de implementare);
4) implementarea deplină a SI în activitatea organizației.

Rezultatele etapei:

1) instruirea utilizatorilor;
2) elaborarea documentației de implementare;
3) realizarea proiectului-pilot al SI şi ulterior implementarea deplină a SI.

La etapa dată în costul SI vor fi incluse componentele cheltuielilor indicate în tabelul 24.

Tabelul 24. Costul sistemului informațional la etapa „Implementarea sistemului informațional”

Nr. d/o	**Componentele cheltuielilor**	**Costul lucrărilor organizațiilor externe**	**Costul lucrărilor personalului propriu**
1	Elaborarea planului de implementare		
2	Instruirea utilizatorilor		
3	Instalarea SI		
4	Adaptarea SI la specificul proceselor organizației		
5	Realizarea proiectului pilot al SI		
6	Realizarea implementării depline a SI		
Total:			

Total pentru etapă:	

Calculul total al sistemului informațional la toate etapele este indicat în tabelul 25.

Tabelul 25. Calculul total al sistemului informațional

Nr. d/o	Denumirea etapei	Costul
1	Colectarea şi analiza cerințelor față de SI	
2	Determinarea unităților structurale şi a costului de livrare a software-ului şi hardware-ului	
3	Aprecierea mărimii segmentului de programare al SI	
4	Evaluarea volumului lucrărilor	
5	Cheltuielile de lucru pentru codificare şi testare	
6	Determinarea caracteristicilor calității SI	
7	Calcularea costului SI	
8	Determinarea influenței riscurilor	
9	Confirmarea şi corectarea estimării costului riscurilor	
10	Implementarea SI	
Costul total al SI:		

7. Metodologia de analiză a costului, bugetului şi termenelor de realizare a lucrărilor în cadrul proiectului de durată

7.1. Revizuirea costului, bugetului şi termenelor de realizare a lucrărilor proiectului de durată

Scopul – revizuirea costului aprobat, bugetului proiectului şi a termenelor de realizare a lucrărilor pentru determinarea diferențelor.

Este necesar a efectua următoare lucrări:

1) stabilirea limitelor bugetului SI în expresie procentuală după formula (14):

$$\text{Limitele_bugetului} = \frac{\text{Cheltuielile_de deviz - Costul_proiectului_SI}}{\text{Cheltuielile_de_deviz}} * 100\% \qquad (14)$$

În mod similar calculăm şi limitele termenelor de realizare a lucrărilor;

2) compararea costului proiectului, termenelor de realizare a lucrărilor şi limitelor bugetare ale proiectului pentru a le coordona;

3) dacă evaluarea este mult mai înaltă de valoarea planificată, de stabilit şi eliminat diferențele. Pentru aceasta trebuie:

- de detaliat maximal funcționalitatea şi limitele necesare, analizînd şi stabilind prioritățile funcțiilor pentru a identifica funcțiile care pot fi excluse. Trebuie de ținut cont de interconexiunea funcțiilor;
- de încetat livrările care nu sînt necesare;

- de verificat termenele de realizare a lucrărilor, costul de deviz şi riscurile care influenţează costul de bază. De micşorat riscul şi cheltuielile din contul reducerii funcționalității şi volumului de livrări;

- de repetat acest proces pînă cînd funcționalitatea şi livrările nu vor intra în limitele permise în baza bugetului şi termenelor de realizare a lucrărilor;

- de coordonat reducerea funcționalității, a volumului de livrări şi cheltuielile revizuite corespunzător pentru a ajunge la un acord. De corectat Divizarea structurală a lucrărilor potrivit funcționalității revizuite.

7.2. Documentarea şi evidența estimării efectuate a costului sistemului informațiomal

Scopul - verificarea exactității estimării costului SI şi asigurarea unei analize similare a viitoarelor proiecte de programe.

În cadrul ciclului de viață al SI, fiecărui proces-business îi este atribuită documentația care este prezentată la intrare sau este primită la ieşirea din acest proces.

Trebuie de analizat evaluarea pentru a determina termenele şi motivele care ar putea cauza depăşirea limitelor de cheltuieli planificate pentru proiect, ca urmare este necesar:

1) de modificat documentația în procesul de stabilire a costului SI. Documentația este rezultatul înregistrării informației primite pe durata acțiunilor sau proceselor ciclului de viață al sistemului de program;

2) pentru a îmbunătăți indicii de evaluare şi planificare de corectat evaluarea la fiecare etapă.

Este necesar a documenta:

1) informația de bază despre proiect:

- denumirea proiectului;
- organizația-elaborator;
- platforma;
- limbajul de programare;
- metoda de evaluare;
- data de aprobare a costului proiectului;

2) mărimea estimată şi reală, volumul lucrărilor, costul software-ului şi hardware-ului;

3) datele planificate şi reale ale etapelor de bază;

4) identificarea riscurilor şi influența lor presupusă şi reală.

În procesul de proiectare, elaborare şi implementare a SI se elaborează următoarele documente în conformitate cu RT 38370656-002:2006:

1) plan de administrare a proiectului;
2) plan calendaristic de realizare a proiectului;
3) concepția SI;
4) propunere-business;
5) sarcina tehnică;
6) proiect tehnic;
7) instrucțiune de exploatare a SI;
8) instrucțiunea administratorului;
9) plan de testare;
10) proces-verbal de testare;
11) act de transmitere în exploatarea experimentală;
12) act de finisare a elaborării;
13) plan calendaristic al procesului de trecere;
14) act de predare în exploatare;
15) act de punere în exploatare;

16) propunere de modificare;
17) mesaj despre problemă;
18) jurnal de înregistrare a adresărilor.

Documentaţia conţine date de referinţă despre proiectul SI şi despre contractele încheiate în procesul de proiectare, elaborare şi implementare.

Anexa nr. 1

Metode alternative de evaluare a segmentului de programare a sistemului informaţional

În calitate de metode de evaluare a segmentului de programare a SI pot fi utilizate:

Metoda Analogiei — se foloseşte la utilizarea repetată sau pentru funcţiile modificabile. Metoda analogiei se foloseşte pe larg ca model analog al obiectului, cercetat prin intermediul modelării. Se utilizează analogia deciziei experţilor sau analogia datelor istorice. Decizia experţilor se bazează pe experienţa cu o funcţie analogică, pe cînd analogia datelor istorice se bazează pe proiectele precedente, asemănarea şi diferenţele dintre cerinţele funcţionale.

Metoda statistică (PERT). Se utilizează pentru funcţiile analogice sau noi, unde experienţa şi datele istorice sînt limitate, sau pentru proiectele cu cerinţe incomplete sau ambigue. Evaluarea segmentului de programare a SI se efectuează în modul următor:

1) primul expert independent stabileşte mărimea minimă admisibilă a segmentului de programare a SI (Least);
2) al doilea expert independent stabileşte mărimea maximă admisibilă a segmentului de programare a SI (Most);
3) al treilea expert independent, folosind şi datele istorice, stabileşte mărimea maximal-posibilă a segmentului de programare a SI (Likely);
4) se calculează mărimea segmentului de programare a SI (Mean):

$$Mean = (Least + 4*Likely + Most)/6.$$

Această metodă este compensată de faptul că evaluarea tinde spre limita inferioară, şi nu spre cea superioară.

În cazul în care mărimea evaluării este întemeiată pe bazele istorice de date, ce au utilizat rînduri fizice ale codului sau analogii în proiecte, trebuie de transformat rîndurile fizice ale evaluării de cod a mărimii în rînduri logice, folosind Tabelul 1.1.

Tabelul 1.1 Transformarea mărimii evaluării

Limbajul de programare	SLOC logice
Assembly şi Fortran	SLOC fizice = SLOC logice
Limbaje de programare de generaţia a treia (C, Cobol, Pascal, Ada 83)	Reducerea SLOC fizice cu 25%
Limbaje de programare de generaţia a patra (SQL, Perl, Oracle)	Reducerea SLOC fizice cu 40%
Limbaje de programare orientate-obiect (Ada 95, C++, Java, Python)	Reducerea SLOC fizice cu 30%

Deoarece productivitatea elaborării codului autogenerat este mult mai înaltă decît productivitatea elaborării unui alt cod, acest fapt ar trebui luat în considerație la transformare. Este necesar de utilizat tabelul 1.2 pentru transformarea codului autogenerat în SLOC logice:

Tabelul 1.2.Tabelul de transformare a codului autogenerat în SLOC logice

Limbajul de programare	**Transformarea codului auto-generat în SLOC logice după:**		
	Least	**Likely**	**Most**
De generația a doua	-	1	-
De generația a treia	0,22	0,25	0,4
De generația a patra	0,04	0,06	0,13
Orientate-obiect	-	0,09	0,17