**Universitatea Tehnică a Moldovei**



**Aplicație web de gestionare a riscurilor informaționale**

**Web application for managing information risks**

**Student:**

**Ciubotaru Radu**

**Conducător:**

**lector superior Bulai Rodica**

**Chişinău 2017**

**Ministerul Educaţiei al Republicii Moldova**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare Informatică şi Microelectronică**

**Departamentul Ingineria Software şi Automatică**

**Admis la susţinere**

**Şef departament: dr.conf.univ. Ciorbă D.**

**„\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017**

**Aplicație web de gestionare a riscurilor informaționale**

**Proiect de licenţă**

**Student:** (R. Ciubotaru)

**Conducător:** (R.Bulai )

**Consultanţi:** (R.Bulai)

( G.Covdii)

**Chişinău 2017**

**Universitatea Tehnică a Moldovei**

**Facultatea Calculatoare, Informatică şi Microelectronică**

**Departamentul Ingineria Software şi Automatică**

**Specialitatea** **Securitate Informaţională**

**Aprob**

**dr.conf.univ. Dumitru Ciorbă**

**şef departament**

**„\_\_”\_\_\_\_\_\_\_\_\_\_\_\_\_ 2017**

**CAIET DE SARCINI**

**pentru proiectul de licenţă al studentului**

*Ciubotaru Radu*

**1. Tema proiectului de licenţă**: Aplicație web de gestionare a riscurilor informaționale

**confirmată prin hotărârea Consiliului facultăţii de la** „ *24*” *octombrie*  *2016*

**2. Termenul limită de prezentare a proiectului** *31.05.2017*

**3. Date iniţiale pentru elaborarea proiectului** *Sarcina pentru elaborarea proiectului de diplomă*

**4. Conţinutul memoriului explicativ**

*Introducere*

*1. Analiza domeniului de studiu*

*2. Proiectarea sistemului*

*3. Realizarea sistemului*

*4. Documentarea produsului realizat*

*5. Argumentarea economică*

*Concluzii*

**5. Conţinutul părţii grafice a proiectului**

Diagrame Use-Case, Interfața principală a programului

**6. Lista consultanţilor:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Consultant** | **Capitol** | Confirmarea realizării activităţii | |
| Semnătura consultantului (data) | Semnătura studentului (data) |
| *G.Covdii* | *Argumentarea economică* |  |  |
| *R.Bulai* | *Controlul calităţii*  *Standarde tehnologice* |  |  |

**7. Data înmânării caietului de sarcini** *01.09.2016*

**Conducător**

*semnătura*

**Sarcina a fost luată pentru a fi executată**

**de către studentul** *01.09.2016*

*semnătura, data*

**PLAN CALENDARISTIC**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr. crt.** | **Denumirea etapelor de proiectare** | **Termenul de realizare a etapelor** | **Nota** |
| *1* | *Elaborarea sarcinii, primirea datelor pentru sarcină* | *01.09.16– 30.09.16* | *10%* |
| *2* | *Studierea literaturii de domeniu* | *01.10.16– 30.11.16* | *20%* |
| *3* | *Alegerea şi pregătirea de lucru a softului* | *01.12.16 – 25.12.16* | *20%* |
| *4* | *Realizarea programului* | *16.01.17 – 30.04.17* | *25%* |
| *5* | *Descrierea programului, diagramele UML* | *01.05.17 – 15.05.17* | *10%* |
| *6* | *Testarea aplicaţiei* | *16.05.17– 28.05.17* | *10%* |
| *7* | *Finisarea proiectului* | *29.05.17– 31.05.17* | *5%* |

**Student**  *Ciubotaru Radu ( )*

**Conducător de proiect** *Bulai Rodica ( )*

| Cuprins  [Introducere 9](#_Toc421613450)  [1 Managementul Riscurilor Informaţionale 11](#_Toc421613451)  [1.1 Noţiuni Şi Concepte Privind Securitatea Informaţională 11](#_Toc421613452)  [1.2 Sistemul De Management Al Riscurilor Informaţionale 11](#_Toc421613453)  [1.3 Evaluarea Şi Analiza Riscurilor Informaţionale 11](#_Toc421613454)  [1.4 Identificarea, Gruparea Şi Ierarhizarea Resurselor Informaţionale 11](#_Toc421613455)  [1.5 Identificarea Şi Clasificarea Riscurilor 11](#_Toc421613456)  [1.6 Metodologii Şi Instrumente De Management Al Riscurilor Informaţionale 11](#_Toc421613457)  [2 Proiectarea Sistemului 11](#_Toc421613458)  [2.1 Denumirea Completă A Sistemului Şi Abrevierea 11](#_Toc421613459)  [2.2 Dispoziţii Generale 11](#_Toc421613460)  [2.3 Cerinţele Faţă De Sistem 11](#_Toc421613461)  [2.4 Proiectarea Sistemului În Uml 11](#_Toc421613462) |
| --- |

# Introducere

Dezvoltarea managementului securităţi informaţionale din ultimul deceniu a focalizat preocupările pentru eficacitatea şi optimizarea activităţilor de conducere în domeniul analizei şi evaluării riscului în activităţile economice, sociale sau politice. Acest demers implică o concepţie şi o abordare multidisciplinară, în care sunt utilizate cunoştinţe din cele mai diferite domenii de activitate. Astfel, economiştii şi inginerii definesc modelele deterministe ale fenomenelor economice sau industriale, matematicienii şi statisticienii construiesc modelele probabiliste ale acestor fenomene,iar informaticienii dezvoltă programele de simulare şi de prelucrare a datelor ale acestor modele. Managementul riscului informaţional devine astfel, din ce în ce mai mult, un domeniu distinct şi bine conturat al managementului de vîrf, o componentă esenţială şi indispensabilă a fiecărui proiect tehnic, economic sau de altă natură.

Desigur, complexitatea problemelor legate de tratarea riscurilor este deosebit de ridicată, prin faptul că este necesară o bună cunoaştere a fenomenelor analizate şi a activităţilor desfăşurate,dar şi o bază de cunoştinţe din domeniul managementului în general, al metodelor şi instrumentelor de analiză a riscurilor informaţionale.

Analiza riscului la adresa securităţii informaţilor este un instrument puternic pe care managerii îl au la îndemână în procesul de adoptare a deciziilor cu privire la implementarea unor sisteme eficiente de management al informaţiilor şi, în ultimă instanţă, în îndeplinirea misiunii organizaţiei. Ca parte a procesului de management al riscului, analiza riscului reprezintă implementarea sistematică a metodelor, tehnicilor şi practicilor de management pentru evaluarea contextului, identificarea şi analiza riscurilor, găsirea variantelor de răspuns care maximizează impactul pozitiv si minimizează impactul negativ al acestora, tratarea, monitorizarea şi comunicarea riscurilor la adresa securităţii informaţiilor şi a sistemelor prin intermediul cărora acestea sunt procesate, stocate sau transmise.

Natura fluidă a mediului tehnologic impune, totodată, necesitatea de a revizui rezultatele analizei riscului la adresa securităţii informaţiilor, prin reluarea periodică a acestui proces. În această direcţie, au fost dezvoltate diferite metode calitative şi cantitative de analiză a riscului, al căror scop este acela de a analiza în mod cât mai corect riscurile la care sunt expuse, la un moment dat, informaţiile organizaţiei.

1. MANAGEMENTUL RISCURILOR INFORMAŢIONALE

1.1 Noţiuni şi concepte privind securitatea informaţională

Societatea îmbrăţişează din ce în ce mai mult tehnologia informaţiei. Informaţia care până nu demult avea la bază hârtia, îmbracă acum forma electronică. Adoptarea semnăturii electronice deschide perspectiva digitizării complete a documentelor, din punct de vedere funcţional,dar odată cu adoptarea acestei perspective duce la majorarea nivelului de securitate. Indiferent de forma pe care o îmbracă, mijloacele prin care este memorată, transmisă sau distribuită, informaţia trebuie protejată.

*Securitatea informaţiei -* este un concept mai larg care se referă la asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei. Dinamica tehnologiei informaţiei induce noi riscuri pentru care organizaţiile trebuie să implementeze noi măsuri de control.

Cele trei componente ale securităţii informaţiei sunt:

* *confidenţialitate* asigurarea că informaţia este accesibilă numai persoanelor autorizate;
* *integritate* menţinerea exactităţii şi fiabilităţii informaţiilor şi a metodelor de prelucrare a datelor;
* *disponibilitate* garantarea că utilizatorii autorizaţi au acces la informaţii şi la infrastructura asociată în momentul potrivit.

Securitatea informaţiilor nu este doar o problema tehnică. Ea este, în primul rând, o problemă managerială.

Managementul riscului reprezintă un proces de identificare şi estimare a riscului, care implică în acelaşi timp luarea de măsuri în vederea reducerii riscului până la un prag acceptabil.

Managementul riscului permite administratorilor tehnologiilor informaţionale (IT) să echilibreze costurile operaţionale şi economice ale măsurilor de protecţie şi să obţină câştiguri în ceea ce priveşte fiabilitatea misiunii prin protejarea sistemelor IT şi a informaţiilor care sprijină scopurile şi obiectivele organizaţiei lor. Principalul obiectiv al managementului riscului este de a permite organizaţiei să îşi îndeplinească misiunile printr-o securizare îmbunătăţită a sistemelor IT folosite pentru stocarea, procesarea, sau transmiterea informaţiilor organizaţionale. Probele obţinute în timpul procesului de management al riscului pot ajuta managerii în luarea de decizii bine informate pentru managementul riscului; în justificarea cheltuielilor pentru un buget IT şi în autorizarea sistemelor IT eficiente. O metodologie bine structurată de management al riscului poate să ajute procesul de management în identificarea mijloacelor de control pentru asigurarea capacităţii de securitate misiunii. În actualul mediu de afaceri, capitalul informaţional al unei organizaţii este expus numeroaselor riscuri. Dacă riscul nu este identificat în mod clar, atunci protecţia capitalului organizaţional nu poate fi asigurată. Cu toate acestea, este necesară definirea exactă a noţiunii de risc într-un anumit context.

***Riscul*** poate fi definit ca o ameninţare care poate să exploateze eventualele slăbiciuni ale unui sistem ori a unei întregi organizaţii. Sunt mai multe modalităţi de abordare a riscului. Din acest punct de vedere, riscul se referă la acel tip de risc asociat cu un eveniment potenţial dăunător care se petrece în absenţa mijloacelor de control specifice, care în mod normal ar putea să anuleze potenţialul său negativ.

1.2 Sistemul de management al riscurilor informaţionale

*Managementul riscurilor informaţionale* reprezintă procesul de identificare, analiză, evaluare şi reducere a riscurilor informaţionale. Managementul riscurilor informaţionale este parte componentă a Sistemului de Management al Securităţii Informaţionale (SMSI).

Un *sistem de management al securităţii informaţionale* reprezintă o abordare sistematică a gestionării informaţiilor sensibile ale organizaţiei în scopul protejării acestora. Implementarea unui SMSI nu se concentrează doar asupra aspectelor tehnice. Abordarea organizaţiei trebuie să fie holistică şi să aibă în vedere resursele umane, tehnologia şi procesele implicate [2].

Eficacitatea SMSI depinde de:

* stabilirea obiectivelor de securitate care să reflecte cerinţele organizaţiei;
* sprijinului conducerii;
* existenţa abilităţilor necesare realizării analizei riscurilor, a vulnerabilităţilor şi a analizei de impact;
* instruirea angajaţilor;
* monitorizata controalelor implementate.

La începutul anilor ’90 BSI (British Standard Institution) a dezvoltat o serie de standarde ca răspuns la cererile industriei, guvernului şi mediului de afaceri de a crea o structură comună pentru Securitatea Informaţiei.

ISO/IEC 27001:2005 (fostul BS 7799-2:2002) este un standard care stabileşte cerinţele pentru un Sistem de Management al Securităţii Informaţiei. Ajută la identificarea, managementul şi minimizarea ameninţărilor care afectează de obicei informaţia.

* formularea cerinţelor de securitate şi a obiectivelor;
* asigurarea ca riscurile de securitate sunt “stăpânite” din punct de vedere al costului;
* asigurarea unei conformităţi cu legislaţia şi diverse reglementări;
* identificarea si clarificarea proceselor existente de management al securităţii informaţiei;
* folosinţa lui de către management pentru a determina statusul activităţilor de management al securităţii informaţiei;
* folosinţa de către auditori interni si externi pentru a determina gradul de conformitate cu politicile, directivele ţi standardele adoptate de către organizaţie;
* furnizarea de informaţii relevante despre politicile de securitatea informaţiei, standarde şsi proceduri, catre partenerii comerciali;
* furnizarea de informaţii relevante despre securitatea informatiei, clienţilor societăţii [3,4].

După o perioada de cinci ani în familia ISO/IEC 27001:2005 apare un nou membru de standartizare ISO/IEC 27005:2011,care tratează managementul riscurilor de securitate informaţională. Standardul prevede linii directorii pentru managementul riscurilor de securitate a informaţiilor într-o organizaţie, sprijinind cerinţele sistemului de management al securităţii informaţiilor definite de ISO/IEC 27001[19,20].

Organizaţii de toate tipurile sunt ingrijorate faţă de ameninţările care ar putea compromite securitatea lor informaţionala şi gestionarea acestui aspect a devenit o preocupare principală pentru departamentele de tehnologie a informaţiei (IT). Noul standard internaţional ISO / IEC 27005 descrie procesul de gestionare a riscurilor securităţii informaţiei şi a acţiunilor conexe.

Ameninţările pot fi premeditate sau accidentale, şi se pot referi fie la utilizarea, aplicarea sistemelor IT sau aspecte fizice şi de mediu. Aceste ameninţări pot lua orice formă de la furtul de identitate, riscurile de a face afaceri on-line, respingerea atacurilor asupra serviciului de la distanţă, spionaj, furt de echipamente sau a documentelor prin intermediul unui fenomen seismic sau climatic, incendii, inundaţii sau probleme de pandemie. Aceste ameninţări pot duce la diverse impacturi, de exemplu, pierderile financiare sau deteriorarea, pierderea unor servicii de reţea esenţiale, pierderea încrederii clienţilor prin eşecul echipamentelor de telecomunicaţii.

Un risc este o combinaţie dintre consecinţele care ar urma de la producerea unui eveniment nedorit şi probabilitatea de apariţie a evenimentului. Evaluarea riscurilor cuantificate sau calitative permite managerilor de a acorda prioritate riscurile în funcţie de gravitatea perceputa a acestora sau de alte criterii stabilite.

1.3 Evaluarea şi analiza riscurilor informaţionale

Analiza riscurilor informaţionale reprezintă combinaţia dintre consecinţele care ar urma de la producerea unui eveniment nedorit şi probabilitatea de apariţie a evenimentului. Riscul poate fi definit ca o ameninţare care poate să exploateze eventualele slăbiciuni ale unui sistem ori a unei întregi organizaţii. Sunt mai multe modalităţi de abordare a riscului. Dintre acestea se disting câteva, şi anume: o analiză cantitativă şi o analiză calitativă.

Evaluarea riscurilor cantitative sau calitative permite managerilor de a acorda prioritate riscurile în funcţie de gravitatea percepută a acestora sau de alte criterii stabilite [11].

Din punt de vedere managerial analiza riscurilor este reprezentată după urmatoarele procese:

* procesul de identificare;
* evaluare şi analiză;
* reducere a riscurilor.

Riscul nu poate fi niciodată eliminat, ci redus la un nivel acceptabil pentru organizaţie

În mod obişnuit, riscul poate fi exprimat cu ajutorul unei formule matematice, prezentate în formula (1.1):

**Riscul = Ameninţări** x **Vulnerabilităţile** x **Valoarea informaţiei**. (1.1)

Conform acestei formule, riscul reprezintă o funcţie între probabilitatea ca o anumită ameninţare să exploateze o potenţială vulnerabilitate, şi impactul care rezultă din acest eveniment advers asupra capitalului organizaţiei.

***Vulnerabilitatea*** este o slăbiciune a unui activ sau a unui grup de active care pot fi exploatate de către unul sau mai multe ameninţări.

Managementul vulnerabilităţii este o funcţie de bază pentru securitatea IT.

Sursele de identificare a vulnerabilităţilor, pot fi:

* mecanisme de control a accesului;
* configuraţie neadecvată a echipamentelor;
* defecte software (bug-uri);
* tehnologii utilizate (neactualizate);
* modul de organizare;
* neinstruirea utilizatorilor;
* amplasare clădirilor, camerelor, server-elor.

***Ameninţările*** la adresa integrităţii şi securităţii unei organizaţii se pot exercita prin mai mulţi vectori. Cei mai frecvenţi, sunt:

* programele maliţioase;
* organizaţiile criminale şi teroriste;
* utilizatorii răutăcioşi sau răuvoitori;
* anumite persoane din interiorul organizaţiei (insideri), care au acces la date şi procedee utilizate în sistemul de securitate al organizaţiei respective;
* persoane din afara organizaţiei (outsideri ), dar care au acces la anumite informaţii extrem de sensibile pentru securitatea organizaţiei;
* cataclismele naturale.

Clasificare a ameninţărilor, dată de Digital security, prevede cîteva criterii de clasificare, şi anume: natura, tipul de expunere, sursă şi ţinta ameninţării.

*După natura ameninţărilor* la adresa securităţii informatice, pot fi distinse ameninţări ***tehnologice*** şi ***organizaţionale***. În consecinţă, vom avea nivelul superior de clasificare.

După *tipul de expunere*, ameninţările tehnologice pot fi împărţite, la rîndul lor, în ***ameninţări fizice*** şi ***ameninţări logice***. Ameninţările organizaţionale pot fi: ***impact asupra personalului*** şi ***acţiunile personalului****.*

*După sursa ameninţărilor*, poate fi dată următoarea clasificare:

1. ameninţări tehnologice/fizice:
2. persoana;
3. împrejurări de forţă majoră;
4. refuzul resurselor tehnice sau de program.
5. ameninţări tehnologice/logice:
6. insider (intrus din interior);
7. outsider (intrus din exterior).
8. ameninţări organizaţionale/impact asupra personalului:
9. impact fizic asupra personalului;
10. impact psihologic asupra personalului.
11. ameninţări organizaţionale/acţiunile personalului:
12. acţiuni deliberate;
13. acţiuni accidentale.

În dependenţă de *ţinta ameninţării*, poate fi redată o continuitate a clasificării, şi anume:

1. ameninţări tehnologice/fizice (persoana, împrejurări de forţă majoră şi refuzul resurselor tehnice sau de program):
2. ameninţări asupra resurselor;
3. ameninţări asupra canalelor de comunicaţie.
4. ameninţări tehnologice/logice:
5. insider (intrus din interior), asupra resurselor (sistem de operare, resurse informaţionale sau informaţii).
6. outsider (intrus din exterior):
7. ameninţări organizaţionale cu impact, atât fizic, cât şi psihologic, asupra personalului sunt făcute:
8. cu scopul de a obţine informaţii sensibile ale organizaţiei;
9. cu scopul de a întrerupe procesele de business.
10. ameninţări organizaţionale/acţiunile personalului, atât cele deliberate, cât şi cele accidentale sun orientate asupra:
11. informaţiilor;
12. continuităţii afacerii.

Pentru a putea selecta şi implementa contramăsuri adecvate riscurilor asociate sistemelor informaţionale este necesar ca ameninţările la adresa acestora să fie identificate şi bine evaluate.

Înaintea determinării ameninţărilor, vulnerabilităţilor şi înaintea atenuării riscurilor, trebuie determinat ce se încearcă să se protejeze - după cum argumentează Berryman (2002), trebuie făcut un inventar complet al sistemului informaţional.

Evaluarea riscului poate fi făcută după mai multe clause, precum pierderile care pot fi produse, frecvenţa de producere etc.

Dacă se consideră o mulţime de riscuri { *r*k | 0 <*k* ≤ *q*}, unde *q* este numărul maxim de riscuri, asociate unei organizaţii se poate introduce o relaţie peste această mulţime de riscuri.

Astfel, se poate aprecia că două riscuri *r*1şi *r*2 distincte (*r*1 ≠ *r*2) pot fi ordonate, printr-o relaţie de ordine parţială, considerând relaţia dintre costurile respectivelor riscuri, adică prin pagubele produse de acestea: *r*1 ≤ *r*2 dacă şi numai dacă *C*(*r*1) ≤ *C*(*r*2), unde s-a notat prin *C*(*ri*) costul riscului *i.*

Similar se poate aprecia că un risc *r*1 mai frecvent, ca apariţie, poate fi mai costisitor decât un risc *r*2 care se produce mai rar, cu condiţia ca pagubele produse să fie evaluate peste un acelaşi interval de timp.

Valoarea unui risc *rk* este, de cele mai multe ori, estimată prin produsul dintre costul său şi frecvenţa sa de apariţie:

*V*(*rk*) = *C*(*rk*)*P*(*rk*) (1.2)

***Aceasta valoare poate fi considerată ca fiind o bună metrică a riscului, în general*** [11].

În figura 1.1 este prezentat cum are loc procesul de gestiune a riscului conform standartului internationa ISO 27005:2011.



Figura 1.1- Procesul de gestiune a riscurilor informaţionale

Managementul şi analiza riscului este procesul de indentificare a riscurilor şi determinarea soluţiei optime de gestiune a lor[12]

După desemnarea liderului şi formarea echipei, procesul de analiză a riscurilor se va derula în următoarele faze:

* identificarea resurselor informaţionale;
* gruparea şi ierarhizarea resurselor informaţionale;
* identificarea riscurilor;
* asociere riscuri la resurse;
* evaluarea riscurilor;
* identificarea mijloacelor de protecţie;
* întocmirea recomandărilor;
* acceptarea riscului;
* comunicarea riscului;
* monitorizarea şi revizuirea riscului.

1.4 Identificarea, gruparea şi ierarhizarea resurselor informaţionale

**Scopul identificării a resurselor informaţionale** este crearea un tablou de ansamblu al infrastructurii informaţionale a organizaţiei. Resurse informaţionale sunt considerate aici ca fiind: datele, aplicaţiile, tehnologiile, încăperi, resurse umane [1].

O altă informaţie indispensabilă analizei de mai departe este interdependenţa resurselor (ex.: ce sistem, cu ce date gestionează, ce tehnologii utilizează, unde este amplasat şi cine administrează). Rezultatul acestei faze poate fi o listă (sau mai multe liste, pentru fiecare categorie separat) cu toate resursele informaţionale identificate în cadrul organizaţiei.

**Gruparea şi ierarhizarea resurselor informaţionale** este necesară pentru determinare priorităţilor de protejare a lor Echipa va selecta în continuare criteriile de clasificare a resurselor ca fiind critice, esenţiale şi normale. Este important ca între membrii echipei să existe o interpretare univocă a acestor criterii. Clasificare resurselor trebuie să ţină cont de interdependenţele dintre ele. Numărul de resurse în fiecare categorie este cumva arbitrar, însă totuşi e preferabil limitarea numărului de resurse critice pentru a evita confuzia. Rezultatul acestei faze este o listă de resurse informaţionale prioritare din punct de vedere al nivelului de criticitate a lor.

* *resurse critice –* organizaţia sau subdiviziunea posesoare a resursei nu poate să-şi continue activitate în lipsa resursei respective;
* *resurse esenţiale –* organizaţia sau subdiviziunea posesoare a resursei poate să-şi continue activitatea, însă pentru o perioadă determinată de timp, însă resursa trebuie neapărat restabilită;
* *resurse normale –* organizaţia sau subdiviziunea posesoare a resursei poate să-şi continue activitatea pentru o perioadă îndelungată de timp, totuşi anumite persoane vor fi parţial afectate, fiind impuse să găsească alternative.

Clasificarea înseamnă etichetări crescătoare ale documentelor sau informaţiilor, de la cel mai de jos nivel, unde se situează informaţiile deschise su neclasificate, la cele confidenţiale, urcând spre informaţii secrete şi strict secrete.

În clasificarea informaţiilor s-a plecat de la ideea că informaţiile care prin compromitere pot costa vieţi umane sunt marcate drept secret, în timp ce informaţiile a căror compromitere costă pierderea multor vieţi umane sunt definite strict secrete.

Regula de baza a identificării si clasificării informaţiei este că informaţiile pot circula doar în sus, de la confidenţial la secret şi srict secret, în timp ce în sens invers, de sus în jos, pot circula doar dacă o persoană autorizată ia decizia de declasificare a acestora.

Se utilizează două strategii de bază privind securitatea naţională, şi anume:

* + tot ceea ce nu este interzis este permis;
  + tot ceea ce nu este permis este interzis.

Etapa de clasificare a riscurilor este esenţială în desfăşurarea procesului de evaluare a riscurilor profesionale. Clasificarea este o operaţie ce poate avea următoarele caracteristici:

**Informaţii subiective** *-* realizată de indivizi pornind de la ideile pe care şi le formează asupra riscului bazându-se pe experienţa şi cunoştinţele lor

Acest tip de clasificare are următoarele caracteristici:

* + dimensiune redusă – secretul poate fi exprimat doar prin câteva cuvinte; din care cauză poate să fie uşor furat şi distribuit altora;
  + perceptibilitate universală– nu este nevoie de pregătire specială pentru a înţelege secretul, oricine poate să-l fure;
  + supuse arbitrarului– pentru a intra în posesia lor un adversar le poate fura, secretul nu poate fi descoperit independent;
  + conţinutul poate fi schimbat– secretul poate fi modificat şi în ultima clipă;
  + sunt perisabile după scurt timp– secretele au o viaţă scurtă, el poate fi ţinut doar pentru o perioadă scurtă de timp.

**Informaţii obiective** – sunt acele informaţiile care chiar dacă sunt descoperite, dezvoltate sau controlate de către guvern, pot fi deja cunoscute sau descoperite independent de o altă ţară . În această categorie intră informaţiile ştiinţifice sau secretele ştiinţifice. Aceste informaţii pot avea un control absolut, ele ţin de natura lucrurilor nu de un secret.

Informaţiile obiective au următoarele caracteristici:

* sunt confuze – de regulă, nu se bazează pe o formulă magică, pentru descrierea informaţiilor ştiinţifice sunt necesare rapoarte lungi, din această cauză ele nu se pot transmite uşor;
* pot fi înţelese numai de oamenii de tiinţă;
* nu sunt supuse arbitrarului – şi alţii pot să afle răspunsul la o anumită întrebare ştiinţifică, dacă formulează întrebarea respectivă;
* nu sunt supuse schimbării – au caractermetern; un fenomen natural are o singură valoare;
* pot avea o viaţă lungă ca secret – alţii pot descoperi informaţiile în mod independent, dar o astfel de descoperire necesită mult timp, ceea ce va conduce la păstrarea secretului pentru o lungă perioadă de timp.

**Informaţiile tehnice – secrete obiective**

O altă categorie de informaţii nu se încadrează perfect în categoriile cunoscute, obiective sau subiective, ele fiind informaţiile tehnice, de genul proiectelor şi execuţiilor tehnice ale unor noi arme (de exemplu), diferite de caracterul ştiinţific al proiectării, şi sunt cunoscute ca informaţii tehnice văzute ca secrete obiective.

Caracteristicile informaţiilor tehnice sunt asemănătoare celor ştiinţifice, dar există unele diferenţe. Faţă de informaţiile ştiinţifice, informaţiile tehnice nu sunt fenomene naturale, ci înseamnă o metodă, un proces, o tehnică sau un echipament angajate în crearea unui produs. Se poate afirma că informaţiile tehnice sunt utilizate pentru exploatarea informaţiilor ştiinţifice.

**Secrete comerciale**. Secretele comerciale includ informaţiile despre procesele de fabricaţie, reţetele unor produse, precum şi alte informaţii obiective care pot fi descoperite independent de către alţii. Multe secrete comercia le sunt asemănătoare informaţiilor ştiinţifice şi tehnice.

1.5 Identificarea şi clasificarea riscurilor

Identificare riscurilor presupune selectarea dintr-o listă cu riscuri comune aferente tehnologiilor informaţionale, a celor pe care membrii echipei le consideră aplicabile infrastructurii proprii. Riscurile care se vor considera că nu merită atenţie sunt înlăturate din listă. Riscurile trebuie să fie explicit identificate în raport cu una sau mai multe resurse. Unele din ele pot fi detaliate, pentru a corespunde cazurilor concrete de utilizare ale unor resurse informaţionale[1].

Etapa de clasificare a riscurilor este esenţială în desfăşurarea procesului de evaluare a riscurilor profesionale.

Clasificarea este o operaţie ce poate avea următoarele caracteristici:

* *clasificarea subiectivă -* realizată de indivizi pornind de la ideile pe care şi le formează asupra riscului bazându-se pe experienţa şi cunoştinţele lor;
* *clasificarea obiectivă*–plecând de la date statistice, anchete, etc;
* *clasificarea calitativă* – stabilirea unui sistem de ordin comparativ;
* *clasificarea cantitativă* – reprezintă calculul probabilităţilor;
* oricare ar fi tipul de clasificare ales de întreprindere, nu trebuie uitate două obiective principale ale acesteia;
* să permită dezbaterea în ceea ce priveşte prioritatea acţiunilor;
* să sprijine planificarea acţiunilor.

Asociere a riscurilor la resurseare loc o particularizare a riscurilor pentru fiecare resursă critică în parte. Din lista de riscuri acceptate, se selectează acele riscuri ce sunt aferente resursei analizate, cu adăugarea comentariilor de vigoare.

# 1.6 Metodologii şi instrumente de management al riscurilor informaţionale

Edward Humphreys, organizatorul grupului de lucru ISO/IEC care a dezvoltat standardul ISO/IEC 27005:2011 comentează că acesta este un standard esenţial pentru aceea care doresc să-şi gestioneze riscurile eficient şi, mai ales, să fie în conformitate cu popularul standard al sistemului de management al securităţii informaţiei ISO/IEC 27001” [14,15].

Au fost dezvoltate mai multe metodologii şi instrumente de analiză şi control al riscurilor informaţionale, printre care CRAMM (Marea Britanie, compania Insight Consulting), FRAP (SUA, compania RiskWatch), Mehari (Franta, Risicare) şi GRIF (Rusia, compania Digital Security), EBIOS (Franţa, Exprima necesitatea şi identificarea obiectivelor de securitate), OCTAVE(SUA,Operationally Critical Treat, and Vulnerability Evaluation). Folosind o metodologie corespunzătoare pentru analiza riscurilor, organizaţia îşi poate identifica propriile cerinţe legate de securitate.

**Metoda Cramm**

Metoda CRAMM (CCTA Risk Analysis and Managment Method) a fost elaborată de către Central Computer and Telecommunications Agency din Marea Britanie la indicaţiile guvernului britanic. Din anul 1985 este utilizat ca un standard naţional de organizaţiile guvernamentale şi comerciale din Marea Britanie. Ulterior CRAMM a câştigat popularitate în întreaga lume. Compania Insight Consulting Limited este preocupată de dezvoltarea şi întreţinerea software-ului omonim, pe baza metodei CRAMM[13,16].

Înprezent sistemul CRAMMeste uninstrumentdestul deputernic şi universal, care permite, pe lîngă analiza riscului, şi soluţionarea sarcinilor de audit, precum:

* analiza sistemului informaţional şi estimarea documentaţiei respective latoate etapele analizate;
* petrecerea auditului în conformitate cu legislaţia ţării, precum şi cu standardul ISO 27001 – Sistemul de management al Securităţii Informaţionale;
* elaborarea politicii de securitate şi a planului de asigurare a continuităţii afacerii [17].

La baza metodei CRAMM stă o abordare complexă privind analiza şi evaluarea riscurilor, care combină metodele cantitative şi calitative de analiză. Metoda este universală şi poate fi implementată atât de organizaţiile mari, cât şi de cele mici, atât de sectorul guvernamental, cât şi cel comercial. Versiunile software-ului CRAMM, ce vizează diferite tipuri de organizaţii, se deosebesc prin baza lor de cunoştinţe.

Metodologia CRAMM este structurată în trei etape:

* analiza, identificarea şi evaluarea activelor protejate;
* identificarea şi evaluarea riscurilor;
* selectarea contramăsurilor de securitate adecvate.

Pentru fiecare etapă se defineşte un set de date iniţiale, succesiunea de evenimente, chestionare pentru a desfăşura interviuri, liste de verificare şi un set de rapoarte.

Estimarea resurselor protejate (etapa I) se face pe o scară de la 1 la 10, şi pot fi mai multe criterii de evaluare-pierderi financiare, pierderea reputaţiei, etc.

La etapa a doua sunt identificate şi evaluate ameninţările la adresa securităţii informaţiilor, sunt căutate şi evaluate vulnerabilităţile sistemului protejat. Nivelul de ameninţare este evaluat pe următoarea scală: foarte mare, mare, medie, scăzut, foarte scăzut. Nivelul de vulnerabilitate este evaluat ca: mare, mediu sau scăzut. Pe baza acestor informaţii se calculează evaluare ariscurilor pe scară de la 1 la 7.

Etapa a treia generează contramăsuri pentru riscurile identificate.

În figura 1.2 este reprezentată interfața grafică a softului Cramm

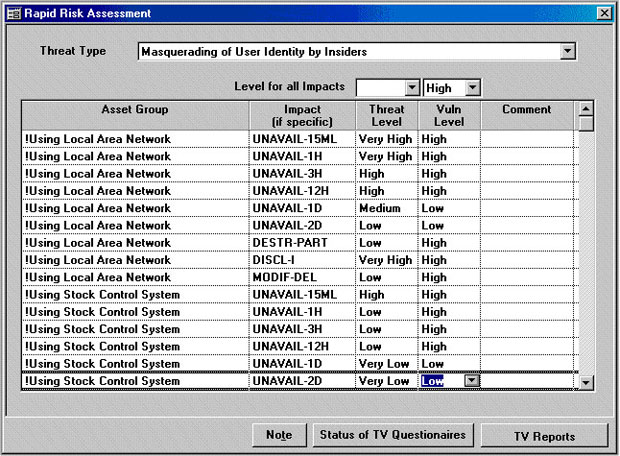


Figura 1.2- Contramăsuri pentru riscurile identificate

În figura 1.3 sunt reprezentate nivelele metodei Cramm

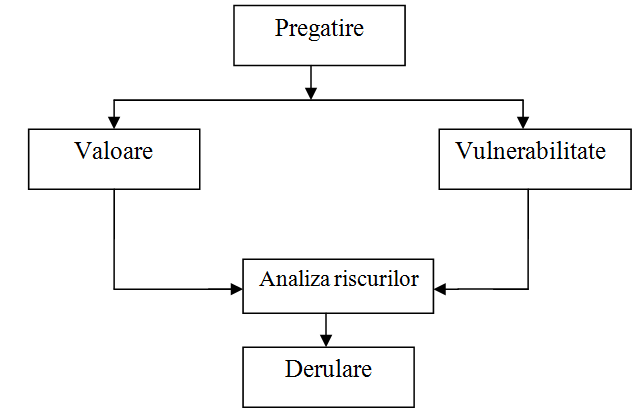
****

Figura 1.3 -Metodologia CRAMM

Principalele *dezavantaje*ale metodei CRAMM sunt:

* utilizarea metodei CRAMM necesită o pregătire specială şi o calificare înaltă a auditorului;
* CRAMM este mult mai adecvat pentru auditul unui sistem informaţional existent, aflat în stadiul de exploatare, decât pentru un sistem în curs de dezvoltare;
* auditul petrecut după metoda CRAMM reprezintă un proces destul de lung, care poate dura luni neîntrerupte de lucru al auditorului;
* software-ul CRAMM generează o mulţime de documente, care nu întotdeauna sunt utile în practică;
* CRAMM nu permite crearea propriilor şabloane de rapoarte sau modificarea celor existente;
* nu există posibilitatea de a completa baza de cunoştinţe a sistemului CRAMM, ceea ce provoacă unele dificultăţi în adaptarea acestei metode la nevoile specifice ale organizaţiei;
* software-ul CRAMM există doar în limba engleză;
* taxa de licenţă este de la 2000 la 5000USD.

**Metoda RiskWatch**

Software-ul RiskWatch[17,21] este un instrument puternic pentru analiză şi gestionarea riscurilor. În familia sistemului RiskWatch intră produse pentru diferite tipuri de audit de securitate:

- RiskWatch for Physical Security – pentru metode fizice de protecţie a sistemelor informaţionale;

- RiskWatch for Information Systems-pentruriscurile informaţionale;

- HIPAA-WATCH for Healthcare Industry - pentru a evalua conformitatea cu cerinţele standardului HIPAA(US Healthcare Insurance Portability and Accountability Act);

- RiskWatch RW17799 for ISO 17799 – pentru a evalua cerinţele standardului ISO 17799.

Metoda RiskWatch utilizează în calitate de criterii de evaluare şi gestionare a riscurilor probabilitatea pierderilor anuale (Annual Loss Expectancy, ALE) şi evaluarea rentabilităţii investiţiei (Return on Investment, ROI).

Spre deosebire de CRAMM, RiskWatch este mai mult axat pe o estimare cantitativă precisă a raportului de pierderi de pe urma ameninţărilor de securitate şi costurile de creare a unui sistem de securitate.

De asemenea, trebuie remarcat faptul că acest produs consideră riscurile informaţionale şi riscurile fizice ale reţelelor de calculatoare împreună.

Sistemul RiskWatch are la bază metodologia de analiză a riscurilor, formată din patru etape[8,9,10].

*Prima etapă* – defineşte domeniul de cercetare. Aici se descriu un şir de parametri, precum tipul organizaţiei, structura sistemului analizat (în general), cerinţele de bază privind securitatea.

Pentru a facilita analiza, în modelele corespunzătoare tipului organizaţiei (sistem informaţional de afaceri, sistem informaţional guvernamental/ militar, etc.), există liste ale categoriilor de resurse protejate, pierderi, ameninţări, vulnerabilităţi şi măsuri de protecţie.

Dintre acestea, sunt selectate cele care există de fapt în organizaţie.

De exemplu, la categoria de pierderi pot fi menţionate:

* întârziere şi refuzul serviciului;
* divulgarea informaţiilor;
* pierderile directe (de exemplu, distrugerea echipamentelor de foc);
* viaţă şi Sănătate (personal, clienţi, etc.);
* modificarea datelor;
* pierderile indirecte (de exemplu, cheltuieli de restabilire);
* reputaţie.

***A doua etapă***– reprezintă datele de intrare care descriu caracteristicile specifice ale sistemului. Datele pot fi introduse manual sau importate din rapoartele generate de instrumentele de cercetare a vulnerabilităţilor reţelelor de calculatoare.

În această etapă sunt descrise detaliat resursele,pierderile şi clasele de incidente. Clasele sunt obţinute prin compararea categoriei de pierderi şi categoriei de resurse.

În scopul identificării eventualelor vulnerabilităţi se foloseşte un chestionar, care conţine mai mult de 600 de întrebări.Întrebările sunt legate de categoriile de resurse.

Se setează frecvenţa de apariţie a fiecărei ameninţări identificate, nivelul vulnerabilităţii şi valoarea resurselor.

Toate acestea sunt folosite pentru a se calcula efectul de introducere a a mijloacelor de protecţie.

În figura 1.4 este reprezentată interfața grafică a softului RiskWatch

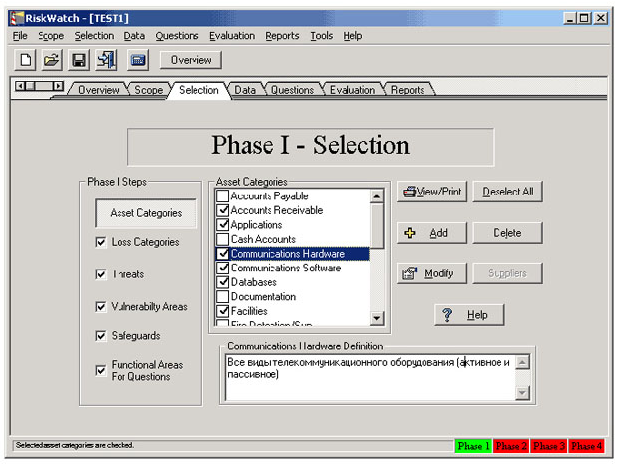


Figura 1.4 – Definirea categoriilor de resurse protejate

În figura 1.5 sunt evidențiate evaluările Lafe și Sale a metodei RiskWatch

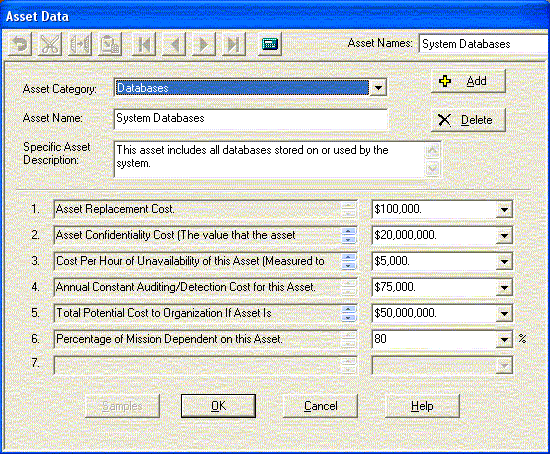


Figura 1.5 - Evaluările LAFE şi SAFE pentru una dintre ameninţări

*A treia etapă,* cea mai importantă - evaluarea cantitativă. În această etapă, se estimează profilul riscului şi sunt selectate măsurile de securitate. În primul rând, sunt stabilite legăturile dintre resurse, pierderi, ameninţări şi vulnerabilităţi, evidenţiate la etapele (riscul este descris prin setul de patru parametri).

De exemplu, în cazul în care costul unui server este 150.000 $, iar probabilitatea că aceasta va fi distrus de foc în decursul anului este egală cu 0,01, pierderile preconizate ar fi de 1.500 $.

Formula cunoscută

*m = p x V* (1.2)

unde

m-aşteptare,

p- probabilitatea apariţiei unei ameninţări,

V - valoarea resursei,

a suferit unele modificări, ca urmare a faptului că RiskWatch utilizează unele evaluări determinate de Institutul American de Standarde NIST, denumite LAFE şi SAFE.

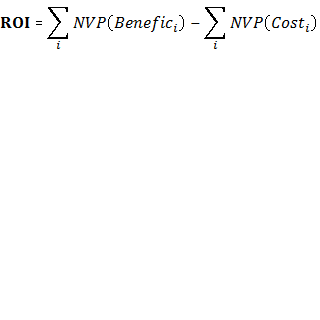
LAFE (Local Annual Frequency Estimate) – frecvenţa medie anuală de realizare a unei ameninţări într-un anumit loc (de exemplu, oraş).

SAFE (Standard Annual Frequency Estimate) - frecvenţa medie anuală de realizare a unei ameninţări într-o anumită parte a planetei (de exemplu, în America de Nord).

Vom introduce, de asemenea, un factor de corecţie care permite să ia în considerare faptul că, în urma realizării unei ameninţări, resursa protejată nu poate fi distrusă în totalitate, doar parţial.

RiskWatch include o bază de date cu estimările LAFE şi SAFE, precum şi o descriere generală a diferitor tipuri de remedii. Efectul de introducere a contramăsurilor de protecţie cantitativ se descrise de către coeficientul ROI (Return on Investment - Randamentul investiţiilor), care arată randamentul investiţiei într-o anumită perioadă de timp. Acesta se calculează prin formula:

 (1.3)



Unde

Costi - costul de implementare şi menţinere a măsurii de protecţie i;

Benefici - evaluare beneficiilor (de exemplu, reducerea pierderilor), pe care le aduce introducerea măsurii de protecţie;

NPV (Net Present Value - valoarea netă actualizată) - oferă o corecţie pentru inflaţie.

***Etapa a patra*** - generarea de rapoarte. Tipuri de rapoarte:

Rezultate scurte.

Rapoarte complete şi de sinteză cu privire la elementele enumerate la etapele 1 şi 2.

Raportul de valoare a resurselor protejate şi pierderile estimate în urma realizării ameninţării.

Raportul despre ameninţări şi contramăsuri.

Raport privind coeficientul ROI.

Un raport privind rezultatele auditului de securitate.

În figura 1.6 sunt reprezentați indicatorii ROI a metodei pentru diferite măsuri de protecție

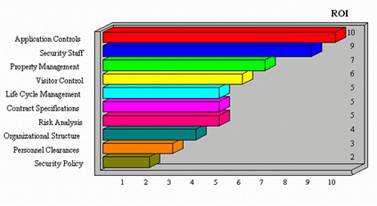


Figura 1.6 - Indicatorul ROI pentru diferite măsuri de protecţie

Astfel, sistemul descris permite evaluarea nu numai riscurile care există în prezent în întreprindere, dar, şi beneficiile care pot fi aduse prin introducerea mecanisme de securitate fizice, tehnice, logice sau de alt gen. Rapoartele întocmite şi graficele oferă elemente suficiente pentru luarea deciziilor de schimbare a sistemului de securitate a companiei.

Pentru utilizatorii de la noi, problema este că RiskWatch utilizează indicii de evaluare LAFE şi SAFE. Însăşi metodologia poate fi aplicată cu succes. În concluzie, pot remarca că metodologia poate fi implementată, ţinîndu-se cont de următorii fctori:

- prezenţa unor experţi capabili de a oferi estimări fiabile ale pierderilor de la ameninţări la adresa securităţii informaţionale;

- disponibilitatea la întreprindere a statisticilor fiabile privind incidentele din zona securităţii informaţiilor;

- necesitatea de o cuantificare exactă a efectelor ameninţărilor sau de a evalua destul de calitativ.

Metoda RiskWatchinclude următoarele *dezavantaje*:

* această metodă este potrivită dacă se realizează analiza riscurilor la nivelul tehnic şi logic de protecţie, fără a ţine seama de factorii de organizare şi administrare.
* metoda nu ia în consideraţie o abordare integră a securităţii informaţiilor.
* software-ul RiskWatch există doar în limba engleză.
* costul ridicat al unei licenţe (de la $ 10 000 pe scaun pentru o companie mică).

**Metoda GRIF**

Metodologia Grif este un sistem complex de analiză şi administrare a riscurilor securităţii informaţionale. GRIF este realizat în 2006 de compania rusă Digital Security şi oferă o imagine completă a securităţii resurselor informaţionale din sistem şi permite să se definească o strategie optimă pentru orice companie [18, http://www.dsec.ru].

Sistemul GRIF:

- analizează nivelul de protecţie a resurselor valoroase ale companiei;

- evaluează prejudiciul potenţial pe care compania poate să-l suporte ca urmare a ameninţărilor la adresa securităţii informaţiilor;

- permite să gestioneze în mod eficient riscurile prin selectarea celor mai optime contramăsuri în raport preţ/performanţă.

Sistemul GRIFeste compus din două părţi: modelul fluxului de informaţii şi modelul ameninţări şi vulnerabilităţi[5,6,7].

*Modelul fluxului de informaţii* include date despre toate resursele cu informaţii valoroase, utilizatorii care au accesla acestere surse, tipurile şi drepturile de acces. Se înregistrează date despre mijloacele de protecţie pentru fiecare resursă, legătura dintre resurse în reţea şi caracteristicile politicii de securitate ale companiei. Rezultatul programului reprezintă un model complet al sistemului informaţional.

*În prima fază* a programului,utilizatorul defineşte toate obiectele sistemului informaţional: departamente, resurse(obiecte specifice ale modelului sunt grupuri de reţea, dispozitive de reţea, tipurile de date, grupurile de utilizatori, procesele de business).

*La pasul doi* utilizatorul specifică legăturile, se determină ce resurse şi căror departamente şi grupuri de lucru le aparţin, ce informaţii sunt stocate pe aceste resurse şi ce grupuri de utilizatori au acces la ea. De asemenea, utilizatorul sistemului indică mijloacele de protecţie a resursei şi informaţiei.

*Laetapa finală* utilizatorul răspunde la o listă de întrebări privind politica de securitate realizată în cadrul companiei, ceea ce permite de a estima nivelul real de securitate al sistemului şi evaluare a riscurilor.

*Modelul ameninţărilor şi vulnerabilităţilor* implică identificarea vulnerabilităţilor pentru fiecare resursă ce conţine informaţii valoroase şi ameninţările care pot fi realizate prin aceste vulnerabilităţi. Rezultatul reprezintă o imagine completă a punctelor slabe din sistemul informaţional şi daunele care i se pot aduce.

În prima etapă a programului utilizatorul introduce obiectele sistemului informaţional: departamente, resurse(obiective specifice pentru acest model: ameninţări la adresa sistemului informaţional, vulnerabilităţile, prin intermediul cărora sunt realizate ameninţările).

Sistemul GRIF include cataloage de ameninţări şiv ulnerabilităţi. Folosind catalogul ameninţărilor şi vulnerabilităţilor, utilizatorul poate selecta ameninţările şi vulnerabilităţile specifice sistemului informaţional. Cataloagele conţin aproximativ 100ş i, respectiv, 200 deameninţări şi vulnerabilităţi.

La pasul doi, utilizatorul indică legătura, de exemplu care sunt resursele departamentelor, care sunt ameninţările la adresa resurselor date şi, prin intermediul căror vulnerabilităţi sunt realizate ameninţările.

Algoritmul sistemului GRIF analizează modelul construit şi generează un raport care conţine valorile de risc pentru fiecare resursă. Configuraţia rapoartelor poate fi concisă pentru administrare sau detaliată pentru lucrul în continuare cu rezultatele.

Modulul de gestionare a riscurilor, permite analizarea motivelor de risc după prelucrarea datelor introduse în algoritm.Astfel, cunoscându-se cauza, se poate gestiona cu datele necesare pentru realizarea şi implementarea contramăsurilor şi, astfel, a reduce nivelulde risc. Datorită calculului eficienţei fiecărei contramăsuri posibile, precum şi determinarea valoarii riscului rezidual, utilizatorul are posibilitatea să aleagă cele mai optimale contramăsuri, care va reduce riscul la nivelul acceptat de organizaţie cu costuri minime.

Ca urmare a utilizării sistemului GRIF se obţine un raport detaliat privind nivelul de risc al fiecărei resurse preţioase din sistemul informaţional,toate cauzeled e risc, cu o analiză detaliată avulnerabilităţii şi o evaluare cost-eficienţă a contramăsurilor posibile.

În figura 1.7 este reprezentată valoarea resurselor, resursele după departamente şi descrierea ameninţărilor.

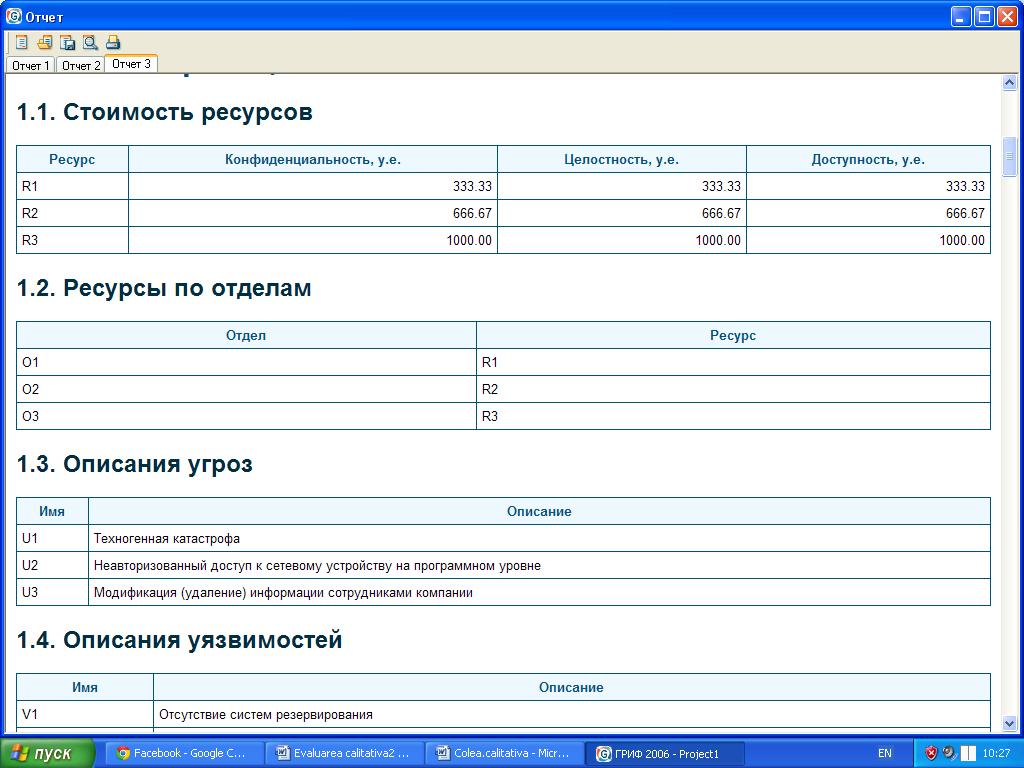


Figura 1.7 - Generare raport

În figura 1.8 sunt reprezentate valorile fiecărei resurse.Sunt indicate nivelele de confidențialitate,integritate și disponibilitate.

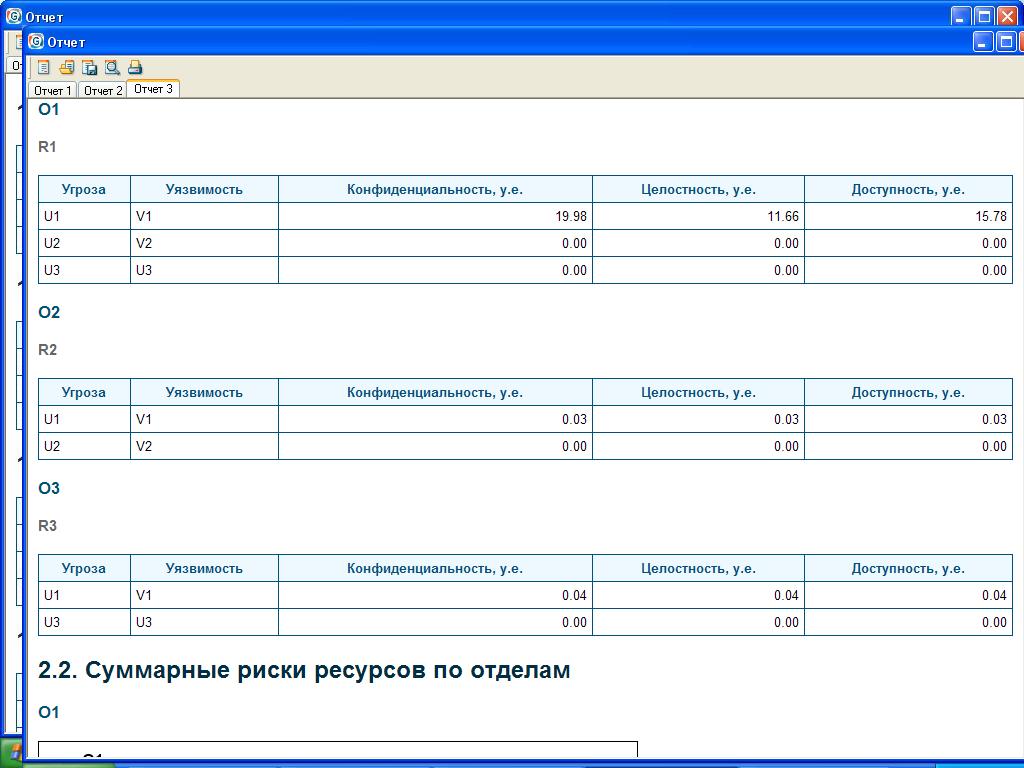


Figura 1.8 - Reprezentarea resurselor şi valorilor

În figura 1.9 sunt indicate și grupate riscurile după departamentele stabilite.

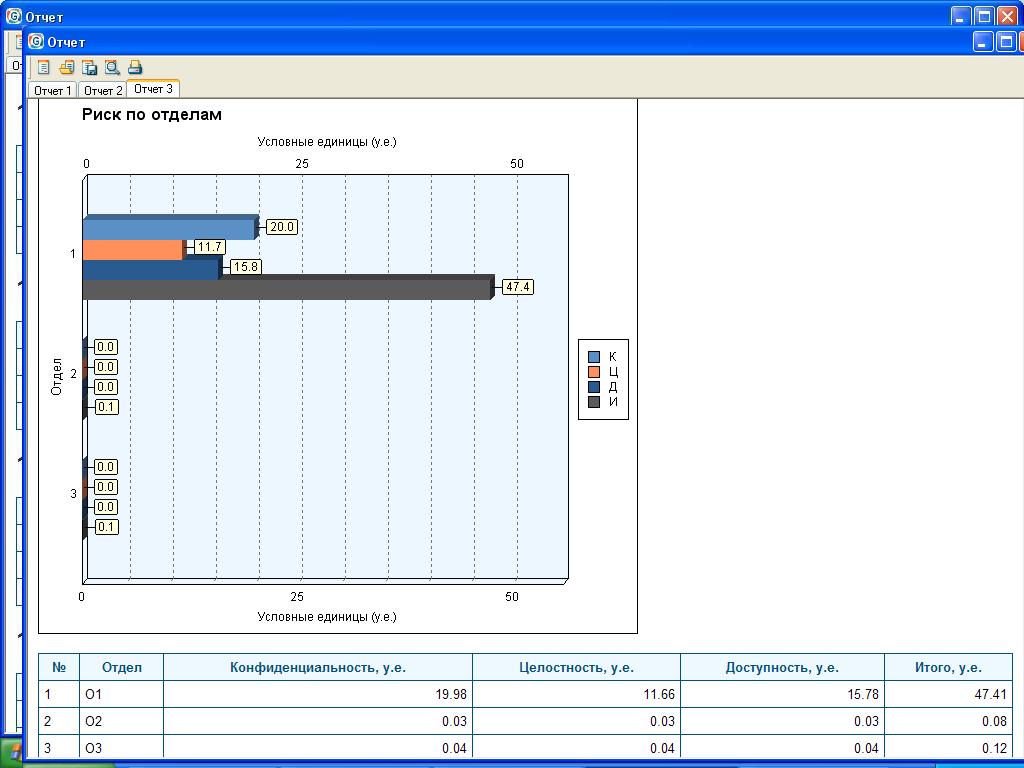


Figura 1.9 - Reprezentarea riscurilor după departamente

În figura 1.10 sunt indicate daunele produse aspra resurselor.

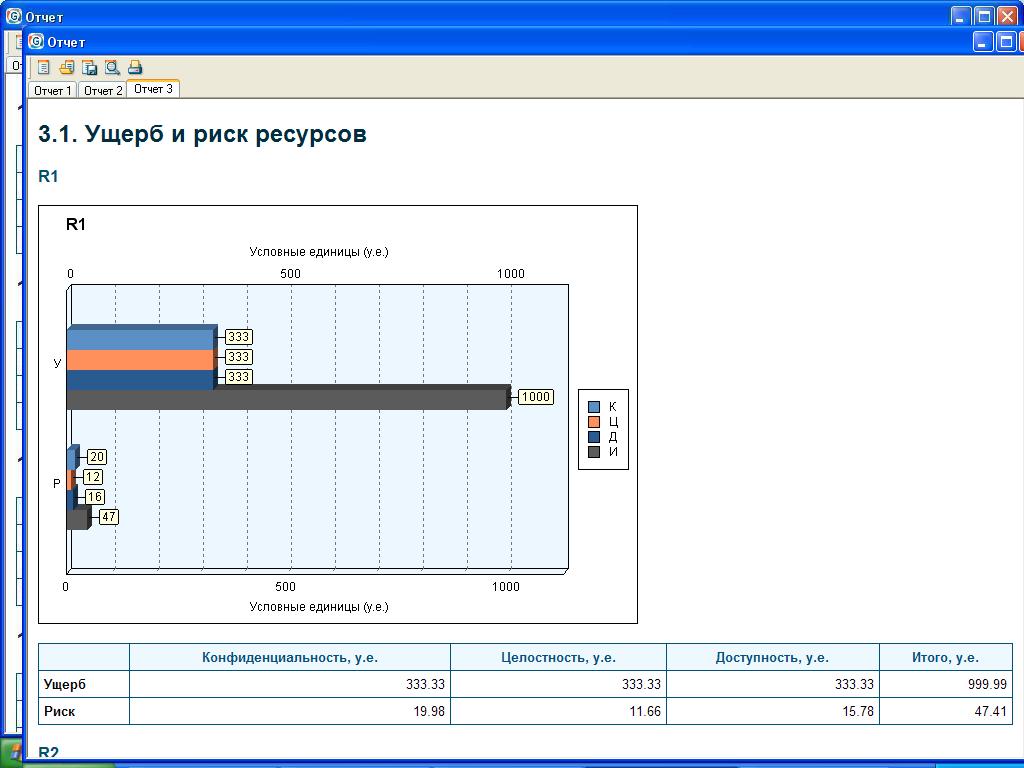


Figura 1.10 - Daunele şi riscurile resurselor

În figura 1.11 sunt indicate daunele și riscurile fiecărui departament.

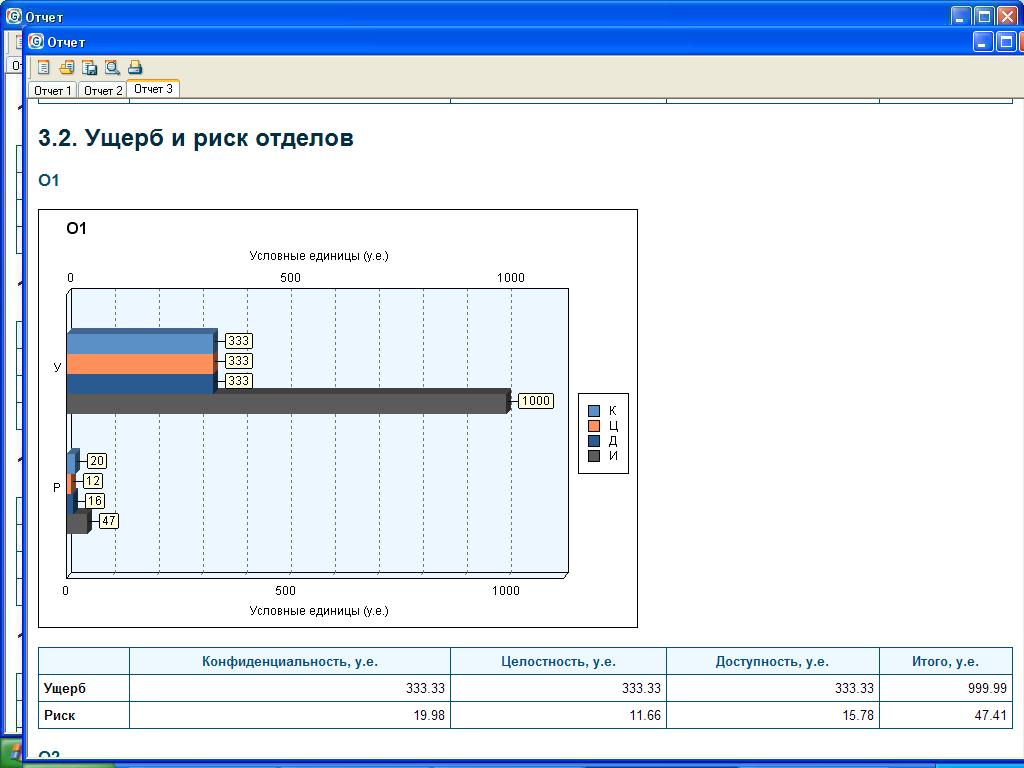


Figura 1.11 - Daunele şi riscurile departamentelor

În figura 1.12 sunt indicate daunele produse și riscurile pentru fiecare sistem informațional.

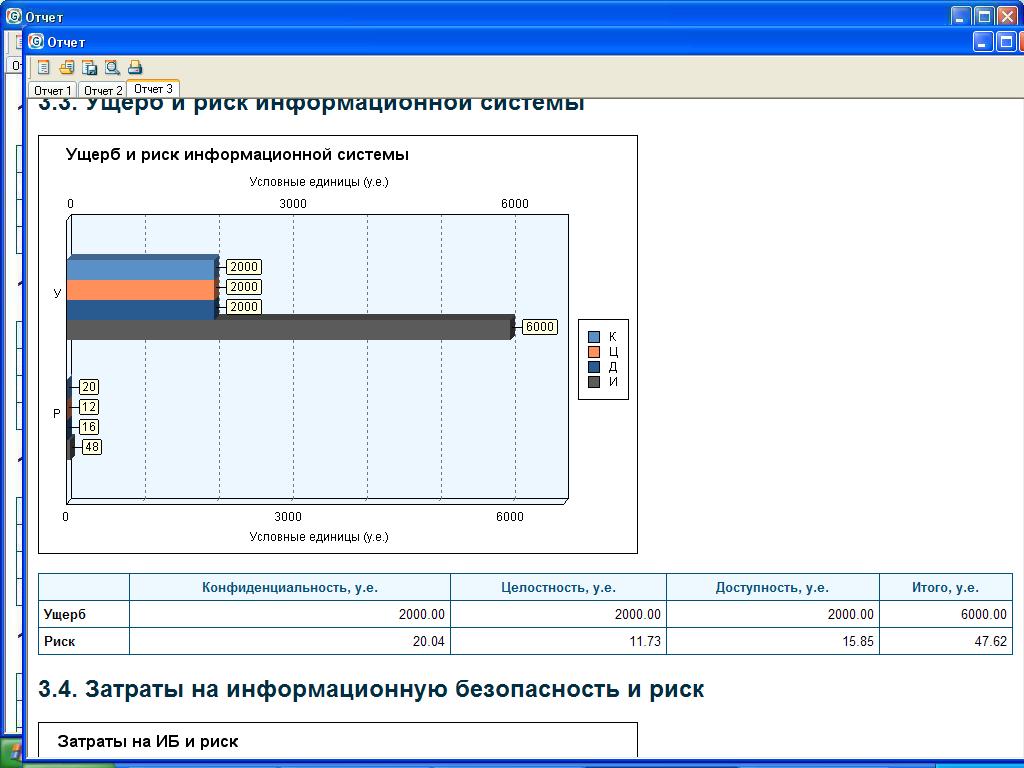


Figura 1.12 - Daunele şi riscurile sistemelor informaţionale

2 Proiectarea sistemului

2.1 Denumirea completă a sistemului şi abrevierea

Sistemul informaţional de evaluare cantitativă a riscurilor informaţionale, este un sistem datorită căruia persoana responsabilă de securitatea informaţionalăva putea modela o companie reprezentată de fluxul informaţional. Această metodă constă din trei etape: modelarea sistemului, relaţii şi politicile de Securitate, dupa această se generează un raport în care se exemplifică analiza sistemului şi riscurile asupra sistemului.

Pentru aceasta întreprindere am creeat şi structura organizatorică, membrii ce fac parte din aceasta companie pentru a întreţine activitatea şi serviciile sistemului.

În figura 2.1 este reprezentată organiograma companiei.

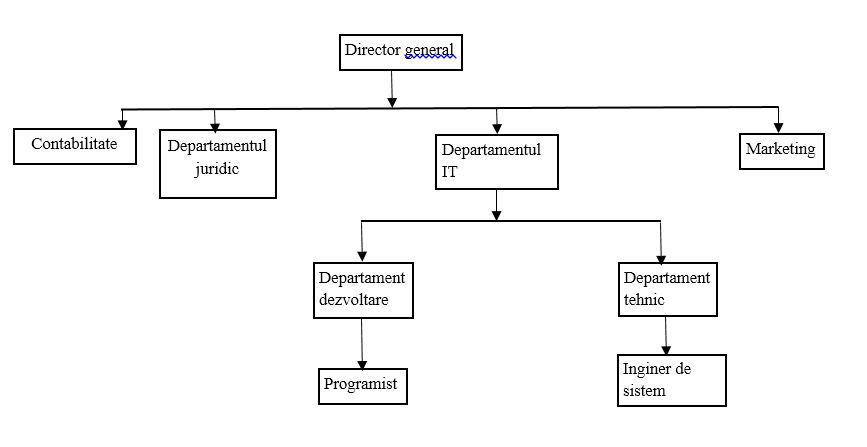


Figura 2.1 – Organigrama companiei

**Analiza problemei**

Organizarea va consta din trei părţi: modelarea sistemului, relaţii şi politici de securitate. Prima parte constă din indicarea secţiilor, indicarea grupurilor de reţea, specificarea echipamentelor de reţea, specificarea grupurilor de utilizatori, specificarea resurselor informaţionale, specificarea tipurilor de informaţii şi identificarea business proceselor.

A doua parte constă din relaţii, pentru fiecare secţie a companiei şi resursele sale se specifică tipurile de informaţii, grupurile de utilizatori, business procesele, mijloacele de protecţie a resurselor şi mijloacele de protecţie a informaţiilor.

A treia etapă politică de securitate constă dintr-un set de reguli şi norme formate sub forme de întrebari pentru a realiza o analiză a sistemului informaţional sub forma unui raport, acest capitol constă din acţiuni de organizare, politica de securitate, securitatea personalului, securitatea fizică, managementul comunicaţiilor şi a proceselor,controlul acceselor şi formarea şi întreţinerea sistemului.

2.2 Dispoziţii generale

Avem următoarele dispoziţii generale:

* inventarierea resurselor informaţionale;
* clasificarea resurselor informaţionale;
* analiza şi aprecierea riscurilor informaţionale;
* standarde şi literatura necesară pentru securitatea informaţională;
* cerinţele securităţii informaţionale;
* politici de securitate;
* pregătirea raportului şi a recomandărilor practice;
* instruirea şi obligaţiunile personalului.

În tabelul 2.1 sunt descrise bussines-procesele

**Tabelul 2.1** – Descrierea business-proceselor

|  |  |
| --- | --- |
| **Business procesul** | **Descrierea succinta** |
| * 1. Dezvoltare | Proces ce asigură modelarea sistemului. Răspunde de gestiunarea conţinutului vizual, posibilitatea de ajustare a elementelor propuse pentru a reda cu exactitate conţinutul dorit. |
| * 1. Accesibilitate | Proprietatea sistemului de interacţiune cu baza de date care este formată dintr-un set reguli şi ameninţări care ar putea influenţa asupra sistemului nostru. |
| * 1. Persistenţă | Posibilitatea sistemului de a interacţiona cu cele trei module de baza: modelarea sistemului, relaţii şi politicile de securitate. |
| * 1. Gestiunea | Proces bazat pe redarea într-o formă gafică prielnică clienţilor pentru o accesibilitate intuitivă şi rapidă. |

**Destinaţia şi scopul elaborării sistemului informaţional**

Sistemul informational de analiza a riscurilor are ca scop generarea unui raport în care datorită datolor introduse despre companie şi introducerea politicilor de Securitate ne generează starea sistemului şi ameninţările la momentul dat, iar după introducerea normelor de Securitate ce au fost introduse asupra sistemului ne mai formează un raport în ce tapa suntem la starea actuală şi asupra căror ameninţări mai avem de lucru.

2.3 Cerinţele faţă de sistem

**Cerinţe faţă de funcţionalităţile sistemului**

Pentru funcţionarea sistemului avem nevoie de un system de operare, în acest caz ca OS vom folosi Windows os produs al Microsoft deoarece este un OS stabil, accesibil, uşor de rulat ce nu are cerinte mari .. La nivel de dezvoltare vom utiliza medoul de programare NetBeans IDE cu pachetul Java Development Kit 8.0

**Cerinţe faţă de echipamentul tehnic**

Pentru a face faţă serviciilor propuse avem nevoie de un calator fie un laptop sau o statie de lucru, cu un processor minim de doua nucleie cu o frecventa minima de 2 Ghz si o memorie ram de 1 GB. Ce se ruleaza în orice perioada de timp sub diferite condiţii de utilizare.

**Cerinţe faţă de personal şi calificarea lui**

***Politica de utilizare a datelor cu caracter personal***

Compania are grijă de a acţiona de bună credinţă în strângerea, stocarea, protecţia şi prelucrarea datelor personale, în scopurile clar stabilite şi în conformitate cu legea Republicii Moldova de protecţie a datelor personale, precum şi a altor legi internaţionale aplicabile, în cazul existenţei unor asemenea legi. În acest context, Compania va lua toate măsurile tehnice şi organizaţionale necesare în scopul protejării datelor personale ce aparţin furnizorilor, împotriva distrugerii sau pierderii neintenţionate, modificării, dezvăluirii sau accesului neautorizat. Compania depune grija necesară şi poartă răspundere pentru protecţia datelor personale ale furnizorului, care au fost obţinute sau livrate prin folosirea serviciilor ce fac obiectul condiţiilor de utilizare, cu excepţia cazurilor de: forţă majoră, evenimente întâmplătoare sau acţiuni rău intenţionate din partea altor persoane terţe, precum şi în cazurile în care utilizatorul a făcut informaţia accesibilă şi altor persoane terţe.

2.4 Proiectarea sistemului în UML

**Diagrama *Use Case***

În figura 2.2 sunt specificate opţiunile prestate de sistemul informaţional. Aici am folosit relaţia de asociere care există între actor şi cazurile de utilizare. Relaţia de asociere se reprezintă grafic printr-o linie. Tot aici am folosit relaţia de dependenţă cu stereotipul „extend” şi „include”. Fluxul informaţional se extinde în nivelurile de analiză a riscurilor, care la rindul său pot fi foarte mari, mari, medii, scăzute şi foarte scăzute. Aceşti indici se includ respectiv în nivelul de analiză a riscurilor informaţionale.

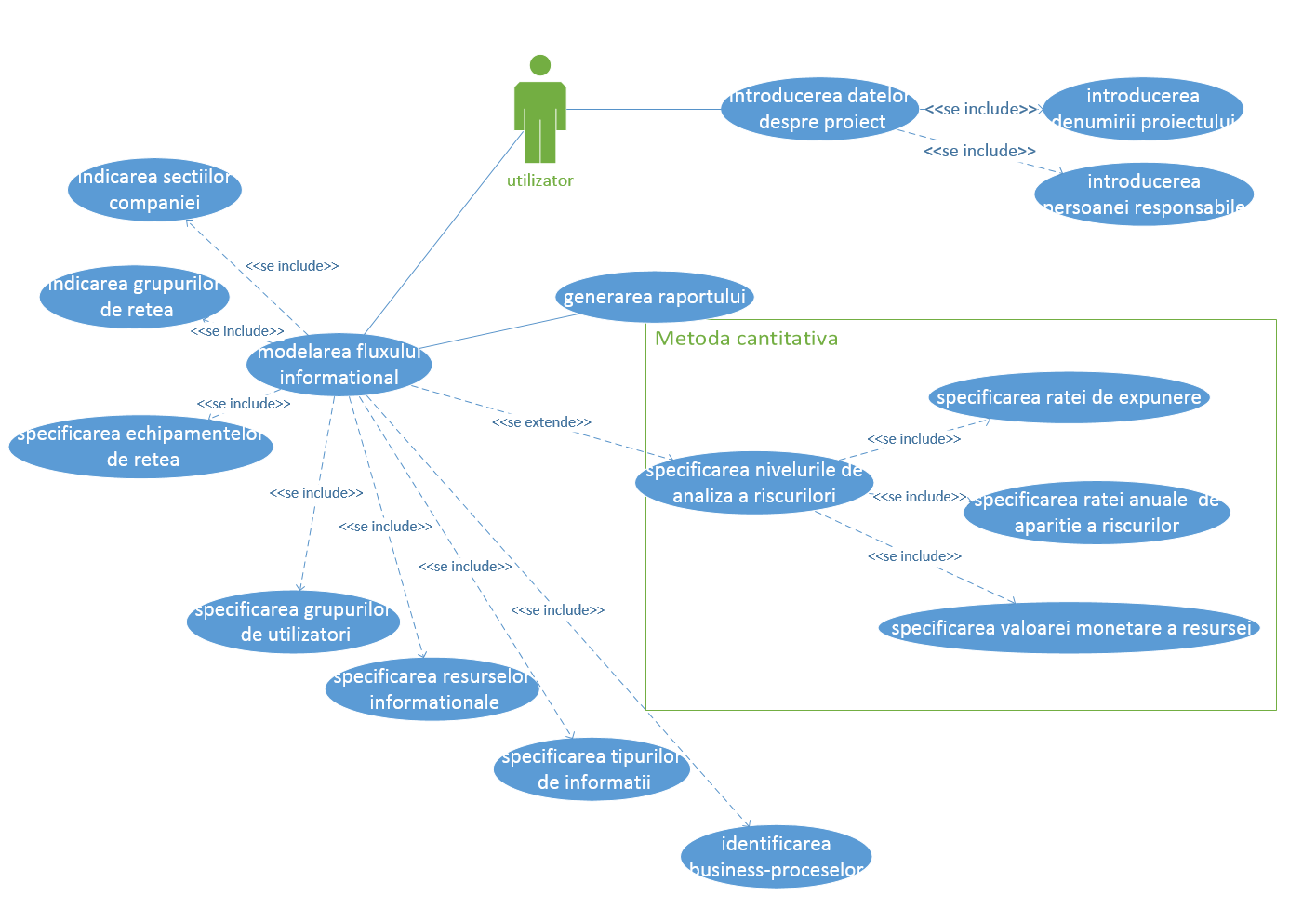


Figura 2.2– Modelarea sistemului

În figura 2.3 am reprezentat elementele auxiliare ce stau la baza analiza riscurilor informaţionale. Aici distingem relaţii de includere, ce persistă în diagrama dată. Este descrisă menirea sistemului informaţional şi care sunt elementele ce caracterizează sistemul.

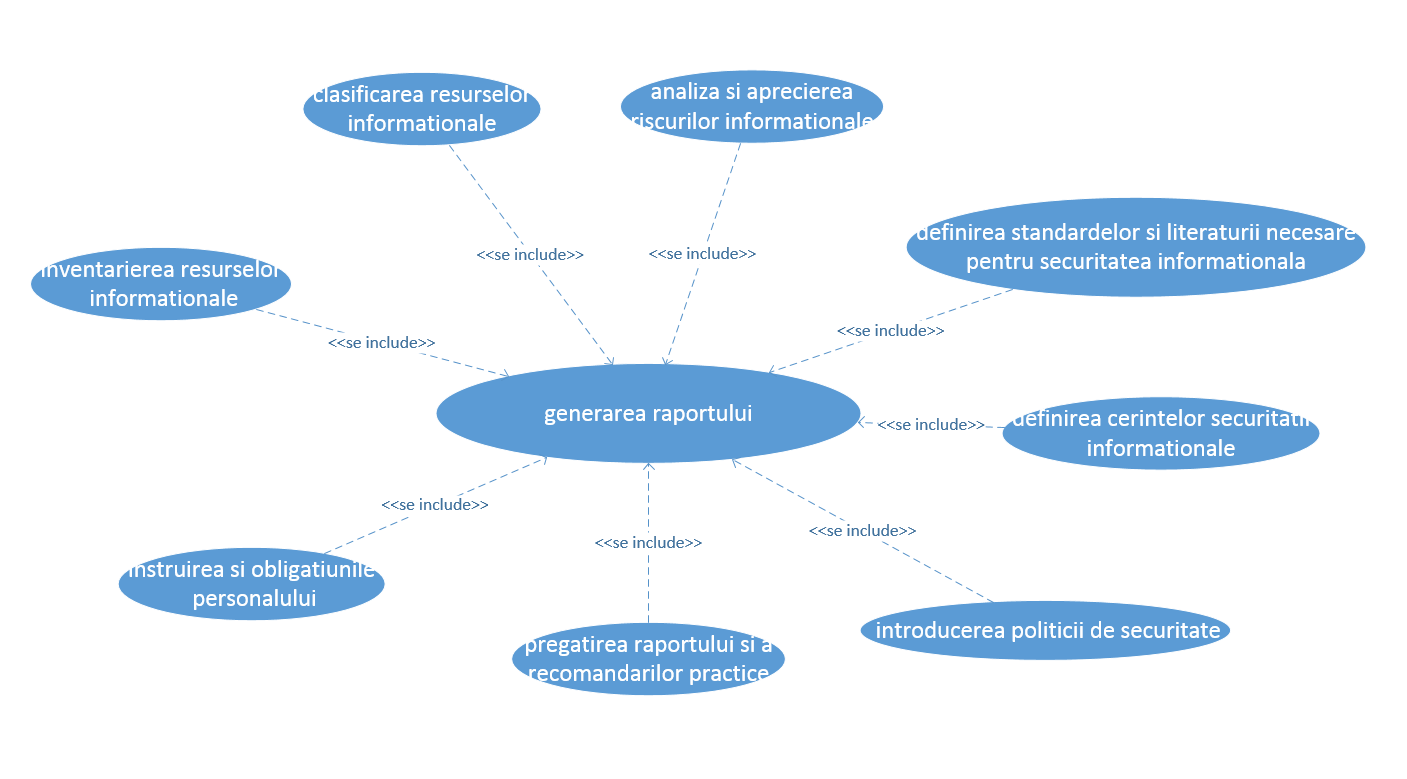


Figura 2.3- Scopul Modelarii

În diagrama din figura 2.4 am specificat tipurile echipmanentelor tehnice, care la rîndul lor formează resursele informaţionale ale sistemului dat. Se folosesc servere, staţii de lucru, calculatoare şi dispozitive mobile. Sunt introduse paginile web şi copiile de rezervă. La fel avem relaţii de extindere între resurse informaţionale şi date despre resurse. La rindul său, datele despre resurse sunt precedate de relaţiile de includere a denumirii,tipului resurselor.

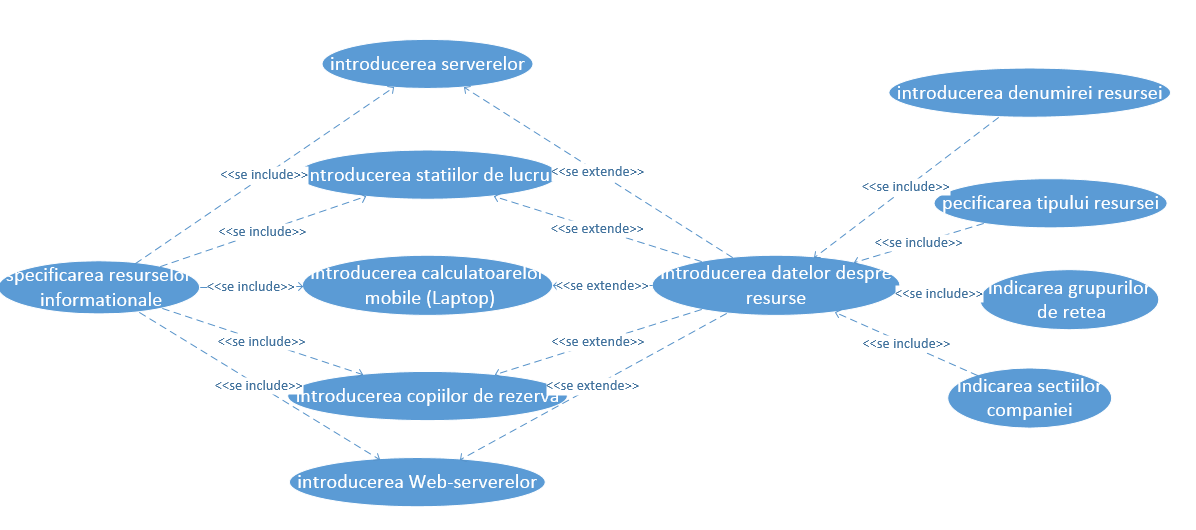


Figura 2.4- Resursele informationale

În figura 2.5 este reprezentată politica securităţii informaţionale aplicate sistemului este unul dintre cele mai importante elemente în vederea întreţinerii şi corespunderii sistemului informaţional la standarde mondiale.

Elementele numerotate în diagrama fac parte din familia politicii de securitate. Aceste elemente sunt importante pentru a răspunde la întrebari ce ţin de securitatea sistemului.

Sunt folosite relaţii de includere.

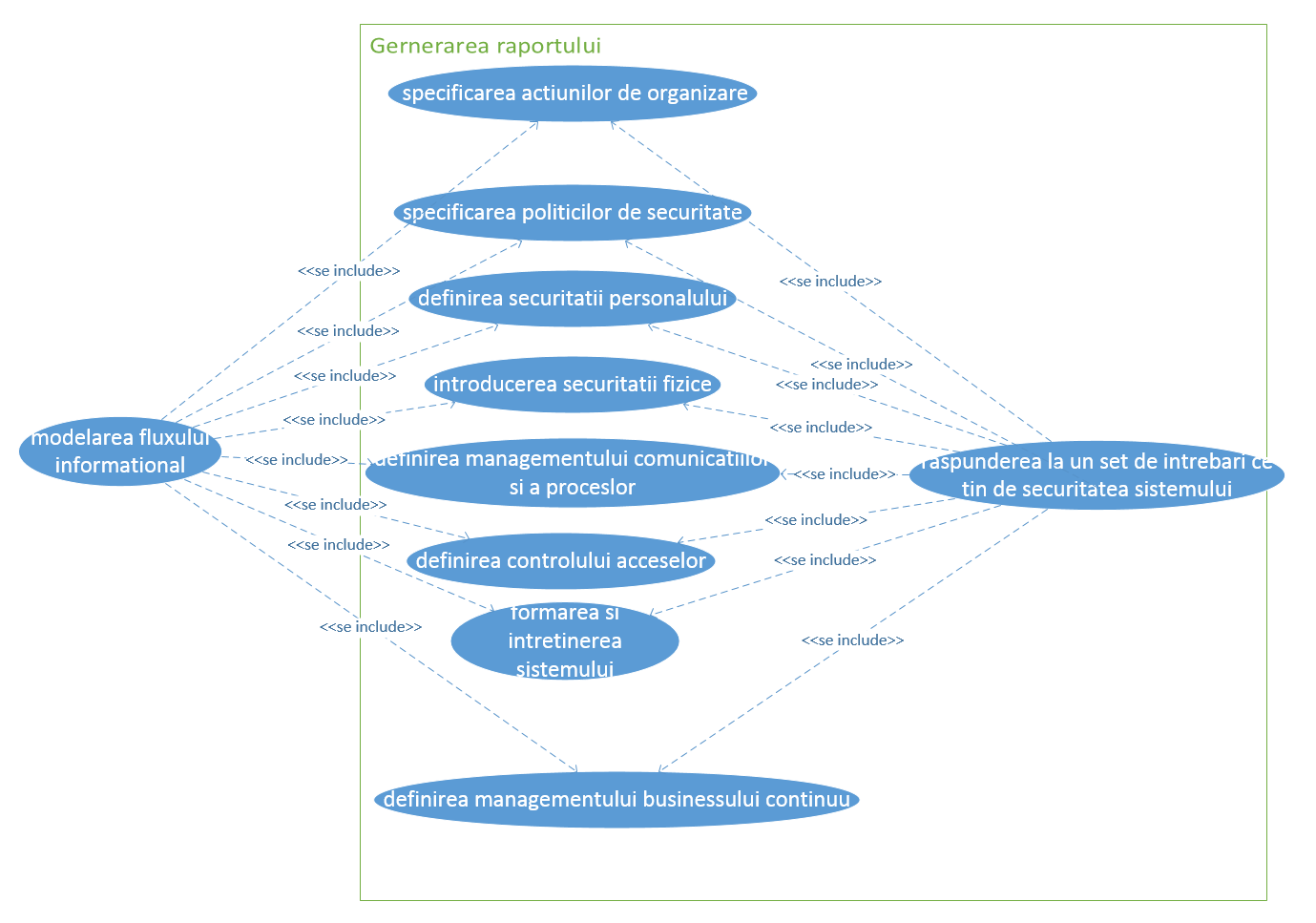


Figura 2.5– Politica de securitate

În figura 2.6 este reprezentată diagrama de secvenţă, în care utilizatorul modelează sistemul informaţional, datorită obiectelor şi paşilor definiţi în figura de mai sus.

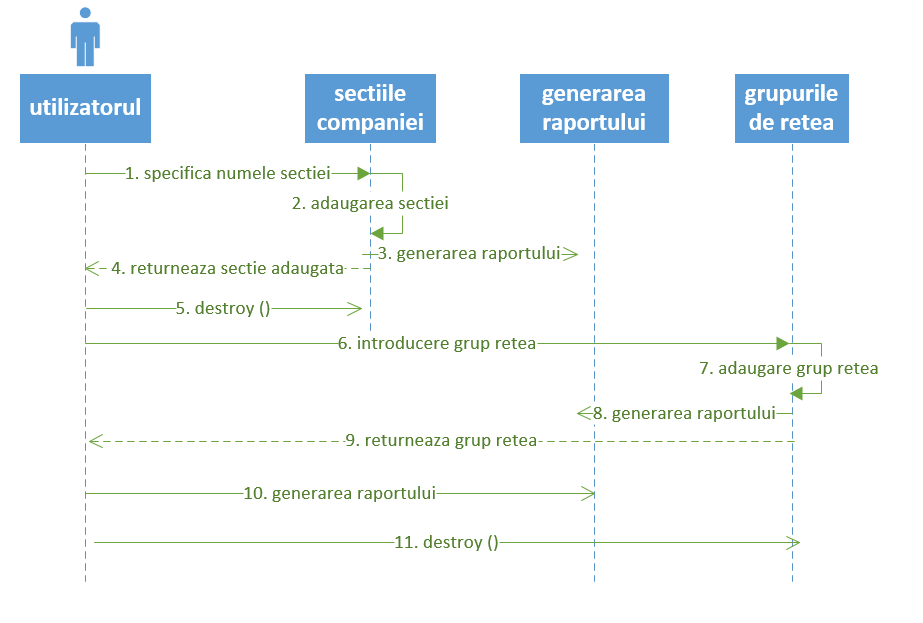


Figura 2.6-Diagrama de secvenţă

În figura 2.7 sunt reprezentate elementele de bază a sistemului informaţional. Aici sunt specificate resrusele informaţionale, tipurile de informaţii, grupurile de utilizatori antrenate, procesele business, metodele şi mijloacele tehnice de protecţie a informaţiei şi a resursei respective.

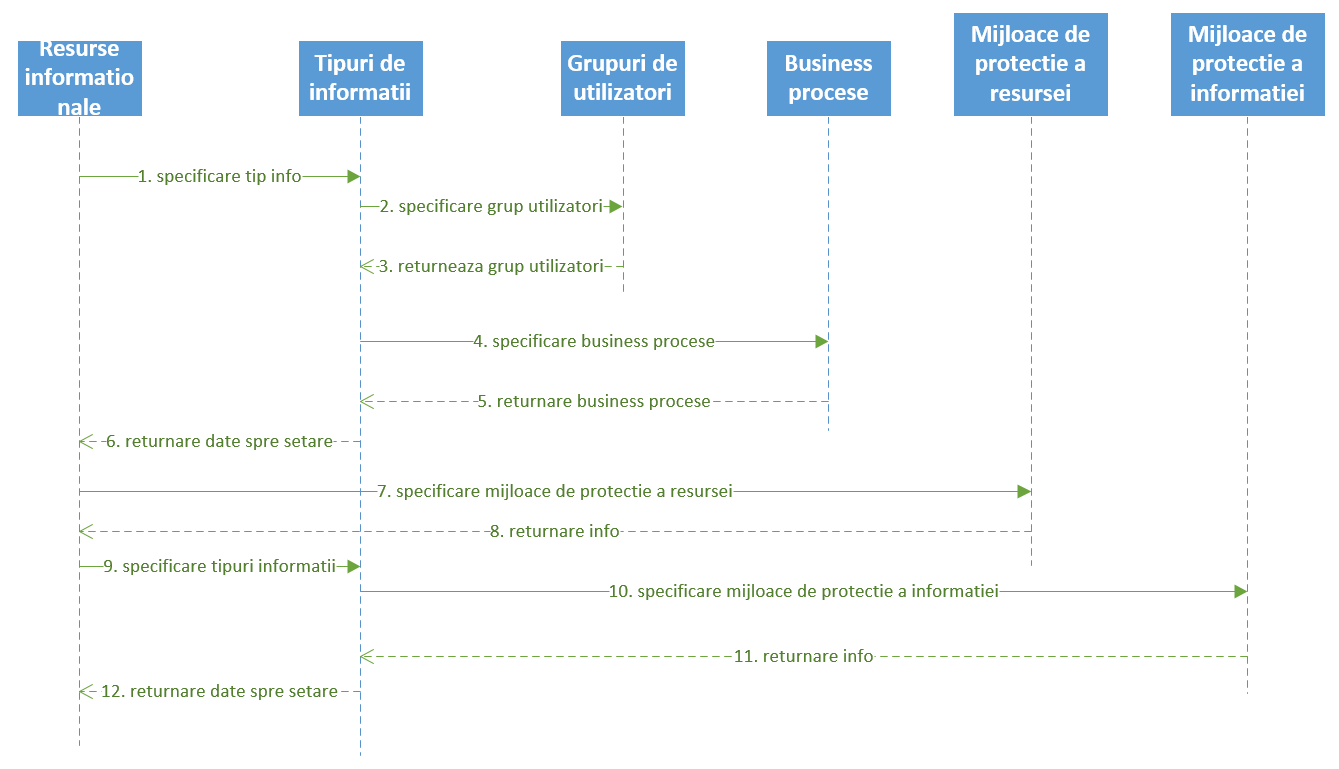


Figura 2.7- Diagrama de secvență

**Diagrama Claselor**

În figura 2.8 diagrama claselor, sunt reprezentate două relaţii de asociere între sistem şi nivelurile de analiză a riscurilor şi a datelor de proiect. Este şi o relaţie de realizare între sistemul informaţional şi interfaţa acestuia. În cazul nostru, relaţia de realizare se explică prin faptul că o clasă implementează o interfaţă. Relaţiile de asociere exprimăo interacţiune între obiectele ce aparţin claselor diferite.

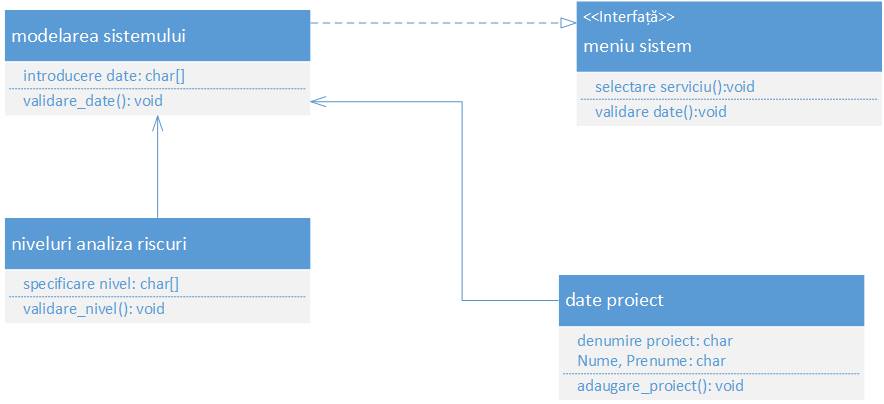


Figura 2.8 - Diagrama Claselor

În figura 2.9 este reprezentată o altă diagrama a claselor. Aici persistă relaţia de moştenire. Ea indică faptul că o clasă moşteneşte caracteristicile unei clase parinte.În plus, clasa clasa copil poate avea caracteristicile proprii.

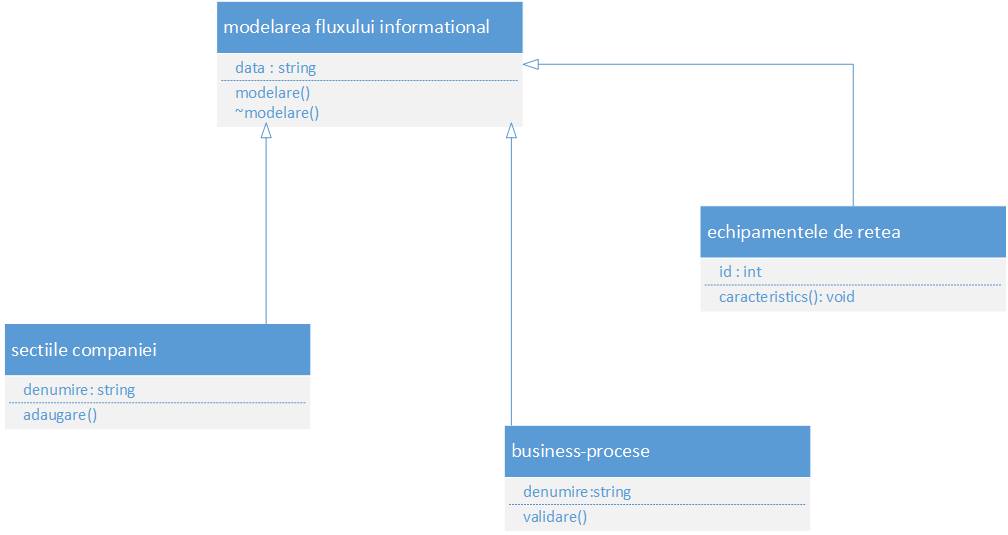


Figura 2.9 - Diagrama claselor

**Diagrama de stare**

În figura 2.10 este reprezentată o diagramă de stare. Aici momentul cheie este procesul de lucru cu un proiect. Este posibilitatea de a creea un nou proiect, de a modela sistemul informaţional dorit, de a evalua riscurile în mod cantitativ şi calitativ şi în final să obţinem un raport final.

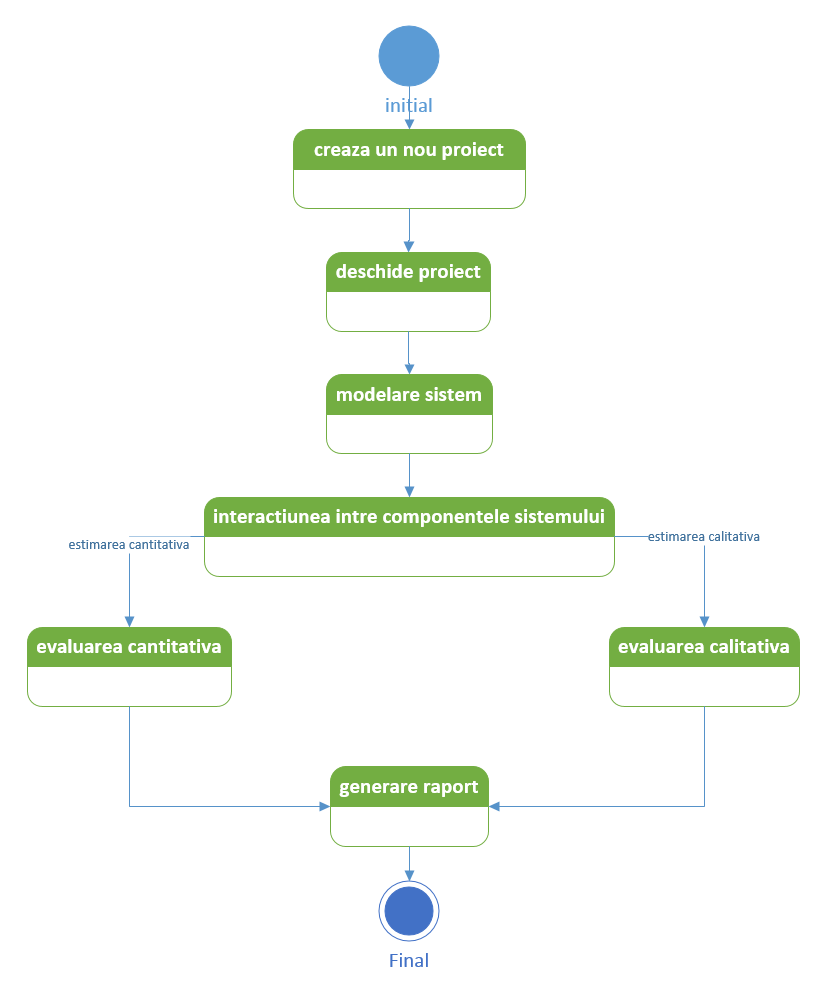


Figura 2.10 - Diagrama de stare

În figura 2.11 este reprezentată o diagramă de stare, pentru nivelul de analiză a riscurilor informaţionale prin metoda cantitativă, precedată de 5 nivele de bază.

Starea reprezintă un complement al descrierii unei clase.

Diagrama de stare dată prezintă toate stările prin care trece un obiect al clasei precum şi evenimentele care pot modifica starea.

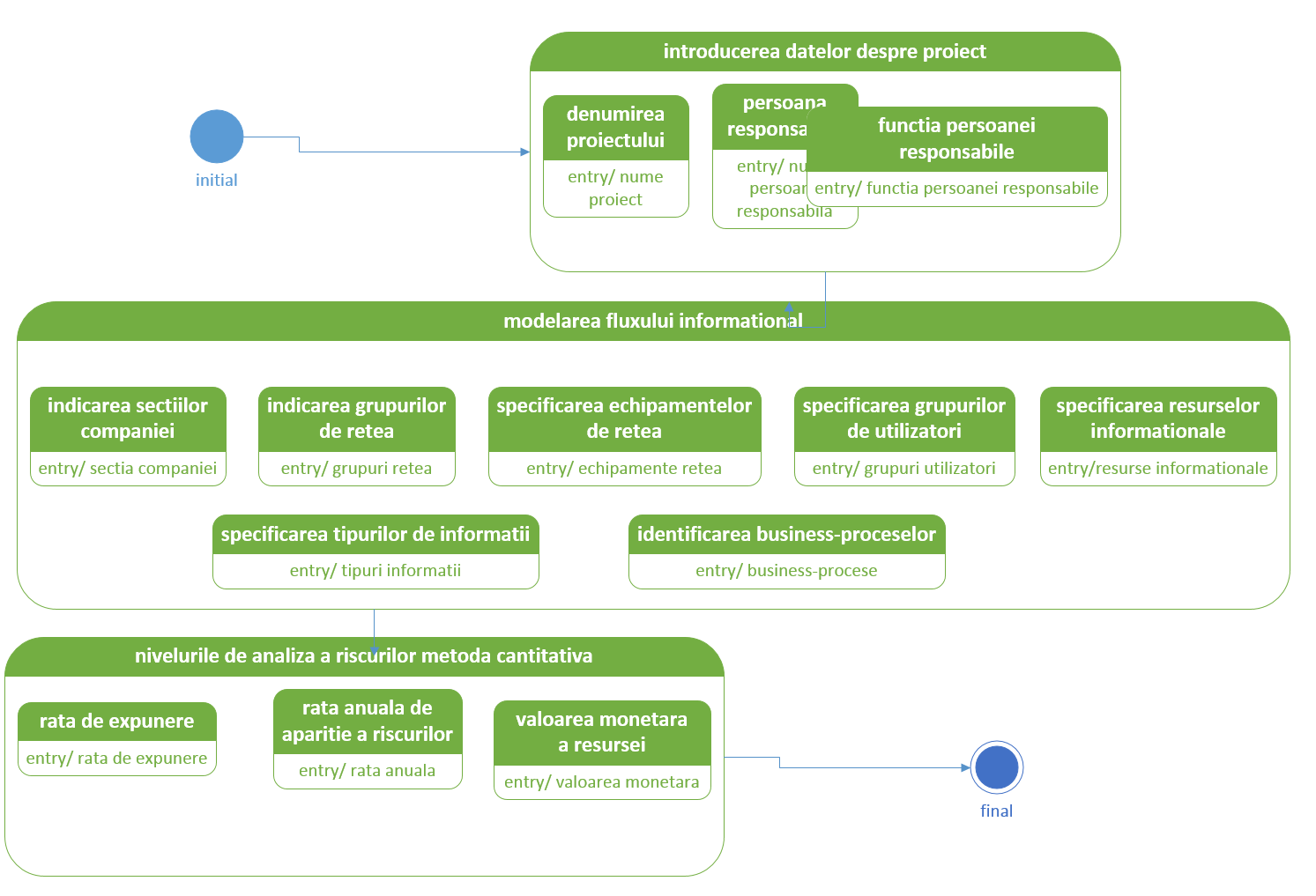


Figura 2.11- Diagrama de stare

În diagrama de activitate din figura 2.12, am descris modul de funcţionare al sistemului informaţional.

Am reprezentat subdiviziunile:modelarea sistemului, relaţii şi politica de securitate. Prin intermediul diagramei de activităţi, sunt modelate business procesele ce sunt descrise în figura de mai sus.

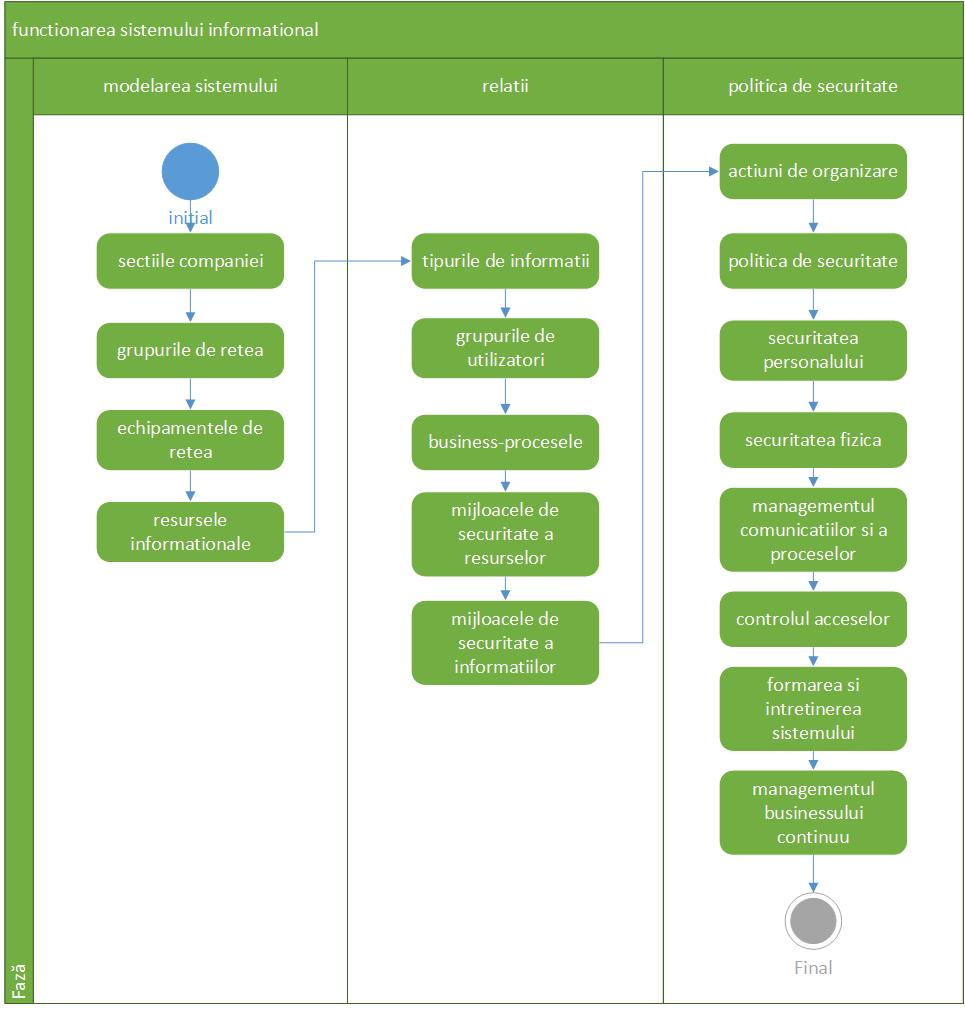


Figura 2.12 - Diagrama de activităţi

În figura 2.13 este reprezentat modul de lucru cu un proiect. Este posibilă introducerea datelor despre proiect, persoana responsabilă şi funcţia ocupată de acesta în sistem. Pentru reprezentarea stărilor paralele am folosit Fork si Join.Metoda Fork este folosită pentru divizarea în mai multe fluxuri paralele iar Join pentru a uni aceste fluxuri în fluxuri paralele. În final are loc generarea raportului.

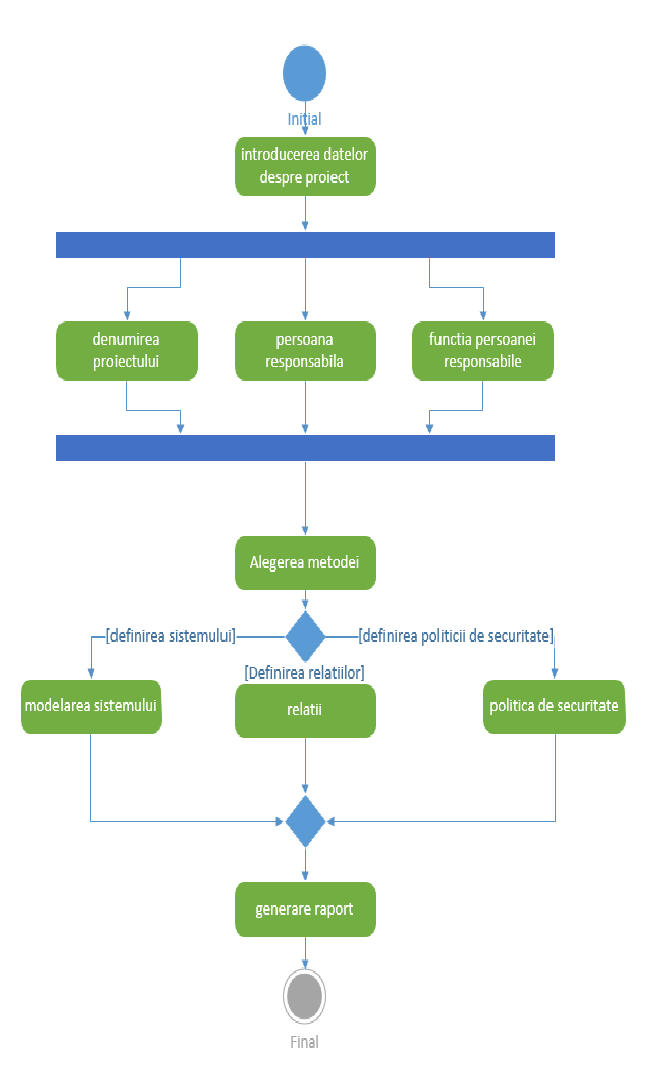


Figura 2.13 - Diagrama de activități

În figura 2.14, diagrama de activităţi este descrisă metoda cantitativă de analiză a riscurilor informaţionale.

Metodele Fork şi Join nu sunt folosite în această diagramă.

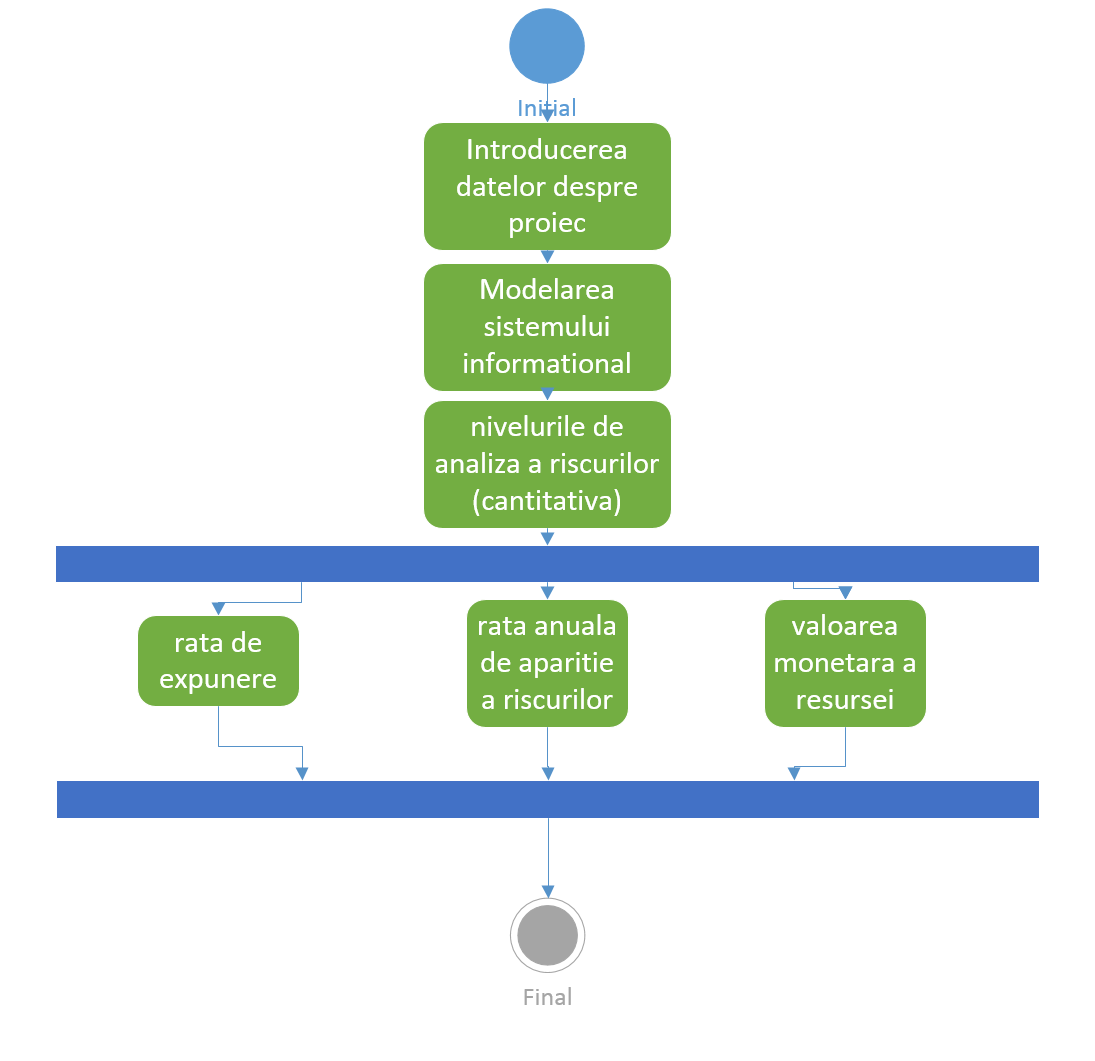


Figura 2.14 - Diagrama de activități

**Diagrama de Componente**

În figura 2.15 este reprezintată o diagramă de componente. Aplicaţia finală va rula pe baza limbajului de programare Java ce va lucra cu doua librării de bază,cea SDK si Framework.

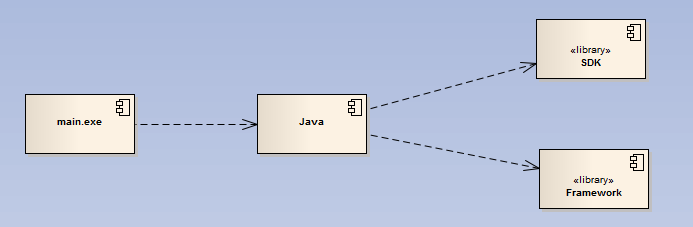


Figura 2.15 -Pachetele sistemului

În figura 2.16 este reprezentată diagrama de componente care specifică dependenţa dintre componentele sistemului,evidenţiind interacţiunea componentei centrale „main.exe”. Odată ce modificăm structura clasei,se modifică şi structura componentei.

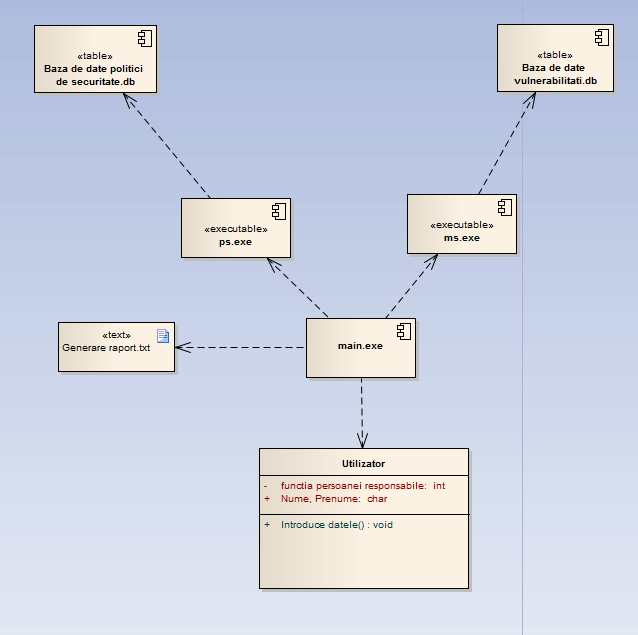


Figura 2.16 -Interacțiunea sistemului

În figura 2.17 este redată componenta principală „main.exe”, ce reprezintă aplicaţia de bază, în cazul de faţă se prezintă acţiunile pe care le face persoana responsabilă. Acesta are acees la baza de date a vulnerabilităţilor sistemlui informaţional, care poate şi sa modeleze sistemul, adăugînd echipamente, secţii şi de a modifica sistemul.

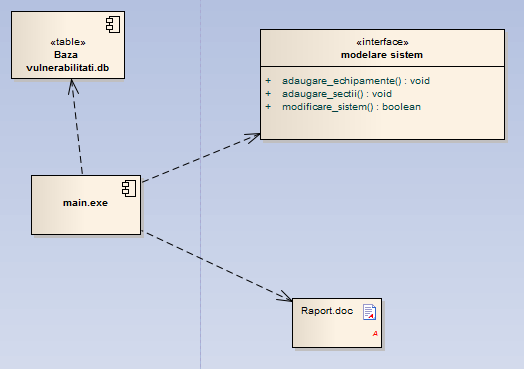


Figura 2.17- Generarea raport

În figura 2.18 este reprezentată diagrama de amplasare în care componentele sînt grupate pe noduri. Avem trei noduri de bază:modelarea sistemului, politici de securitate şi sistemul informaţional. Între ele are loc schimbul reciproc de date.

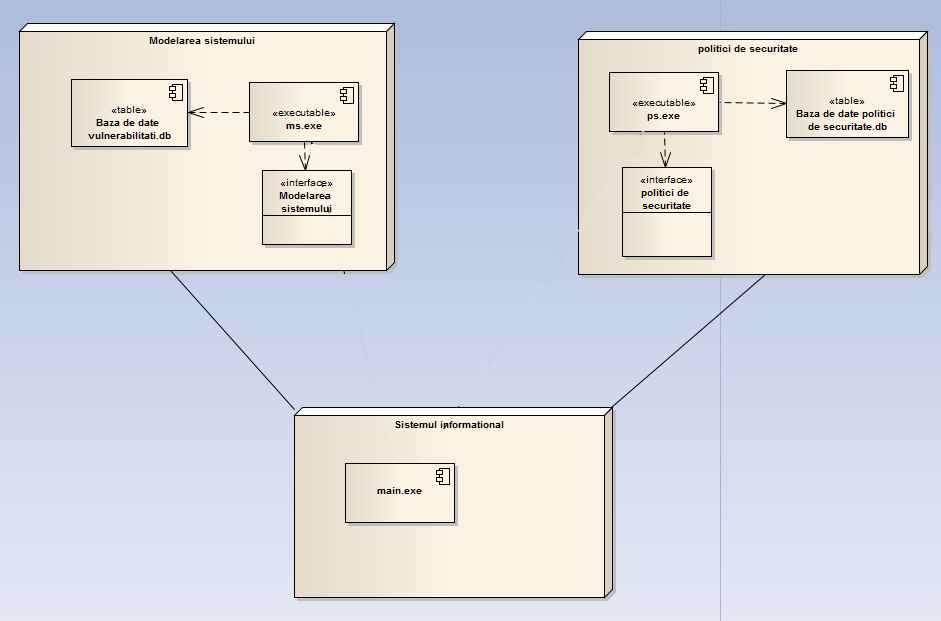


Figura 2.18 -Diagrama Desfăşurărilor

# 3 Realizarea sistemului

3.1 Mediu de dezvoltare

3.2 Analiza cantitativă a riscurilor informaţionale

Analiza cantitativă a risculu ieste procesul prin care se urmăreşte evaluarea numerică a probabilităţii şi impactului fiecărui risc asupra obiectivelor proiectului şi influenţa asupra riscului general al proiectului.

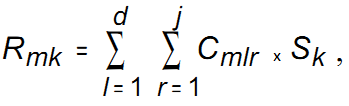
Evaluare cantitativă a riscurilor informaţionale ar consta din trei paşi:

* calculul probabilităţii de exploatare a ameninţărilor pentru a atingerea obiectivului;
* calculul probabilităţii de realizare a ameninţărilor prin depăşirea barierelor de protecţie;
* cdentificarea relaţiilor cheie: ameninţări, resurse protejate, vulnerabilităţi şi mijloace de protecţie.

Evaluarea riscurilor corespunzător indicatorilor de cost a resurselor, indicatorilor de ameninţări şi vulnerabilităţi prin metoda tabelară (calcularea riscului pentru fiecare resursă protejată şi calcularea riscului total la realizarea fiecărei ameninţări). De a identifica realist costurile, programul şi obiectivele ce pot fi realizate

Din punct de vedere cantitativ, nivelul de risc - este o funcţie a probabilităţii de realizare a unei anumite ameninţări şi mărimea posibilelor pierderi.

Riscul, din punct de vedere a unei ameninţări concrete, asociată unei resurse, se poate calcula după formula:

 (3.1)

unde,

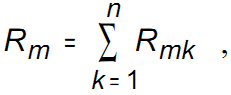
Сmlr - probabilitatea realizării ameninţării m prin depăşirea barierei de protecţie l, asociată cu vulnerabilitatea r (se ia în considerare că bariera de protecție poate să lipsească);

Sk – costul resursei protejate;

j – numărul de vulnerabilităţi;

d – numărul de mijloace de protecţie.

Riscul total de realizare a unei ameninţări concrete, se poate calcula după formula:

 (3.2).

unde,

n – numărul de resurse protejat.

Estimarea Rentabilităţii Investiţiei (RI) va fi obținută pentru fiecare măsură de control prin formula:

(3.3)

unde,

Cl– costul anual pentru aplicarea barierei de protecție l,

rl– indicele de eficacitate pentru bariera l,

Metoda cantitativă expusă are însă anumite neajunsuri, printre acestea se pot enumera:

* dificultatea de a găsi un număr care să cuantifice cât mai exact frecvenţa de producere a unui eveniment;
* dificultatea de a cuantifica anumite valori, de exemplu, sunt foarte greu de definit disponibilitatea unei informaţii şi calculul pierderilor când această caracteristică lipseşte;
* metoda nu face distincţie între ameninţările rare, dar care produc dezastre mari ca valoare (incendiu, cutremure, tornade etc.), şi ameninţările dese care produc dezastre mici ca valoare (erori de operare), în ambele cazuri efectele financiare fiind asemănătoare;
* alegerea numerelor folosite poate fi considerată subiectivă, muncă laborioasă care necesită timp şi consum de resurse.

3.3 Intrări în analiza cantitativă al riscurilor informaţionale

Planul managementului riscului.Este documentul rezultat din procesu anterior de planificare a managementului riscului.

Riscurile identificate. Sunt ieşiri din procesul de identificare a riscului.

Lista riscurilor prioritare.Este o rezultantă a procesului de analiză calitativă a riscului.

Lista riscurilor pentru analize suplimentareşi management.Deasemenea, este oieşire din proces de analizăcalitativăa riscului.

Informaţii istorice.Sunt informaţii provenite de la proiecte anterioare similare, studii referitoare la riscurile proiectelor, baze de date despre risc etc.

Evaluările experţilor.Datele de intrare în analiza cantitativă a riscului pot să provină de la echipa de proiect sau de la experţi în domeniu din cadrul organizaţiei sau din afara acesteia.

Alte ieşiri din planificarea proiectului. Cele mai utile ieşiri din celelalte procese de planificare a proiectului sunt estimările duratelor activităţilor, structura activităţilor proiectului, costurile estimate pentru aceste activităţi, precum şi obiectivele tehnice ale proiectului.

3.4 Mijloace şi tehnici pentru analiza cantitativă a riscului

*Interviul* -tehnicile de intervievare sunt utilizate pentru a cuantifica probabilitatea şi impactul riscurilor asupra obiectivelor proiectului. Primul pas îl constituie realizarea unor interviuri despre riscurile proiectului cu participarea responsabililor sau a experţilor. Informaţia care este necesară depinde de tipul distribuţiilor de probabilitate care vor fi utilizate pentru modelarea riscului. Se stabilesc astfel argumentele care au stat la baza parametrilor atribuiţi distribuţiilor de probabilitate ale modelelor de risc care vor constitui elemente de intrare pentru strategiile de răspuns la risc.

În figura 4.1 este reprezentat procesul de analiză a ricului



Figura 3.1 - Procesul de analiză cantitativă a riscului

*Analiza de senzitivitate:*această tehnică ajută la determinarea acelor riscuri care au cel mai mare potenţial de impact asupra proiectului. Aceasta examinează gradul în care incertitudinea fiecărui element de risc al proiectului influenţează obiectivele proiectului atunci când celelalte elemente variabile şi incerte sunt menţinute la valorile lor cele mai probabile.

*Analiza arborilor de decizie:* se utilizează pentru a reprezenta problema de decizie considerând implicaţiile alegerii dintre alternativele disponibile. Metoda utilizează probabilităţiler riscurilor precum şi elemente de pierdere sau câştig pentru fiecare secvenţă decizională. Rezolvarea arborelui de decizie indică decidentului o evaluare în termeni cantitativi a riscului fiecărei decizii în condiţii de incertitudine;

*Simularea:* aceasta utilizează un model al proiectului care translatează incertitudinile specificate până la un anumit nivel de detaliere privind impactul potenţial asupra obiectivelor proiectului şi apoi la nivelul întregului proiect.

3.5 Algoritmul de analiză cantitative a riscurilor informaţionale

**Datele de intrare**

Pentru evaluarea riscului informaţiei este nevoie de a analiza securitatea şi arhitectura sistemului informaţional. Prin urmare proiectantul sistemului informaţional trebuie mai întîi de toate să descrie arhitectura acestuia, şi anume:

* resurse, ele păstrează informaţii preţioase;
* grupurile de reţele, pe care se găsesc resursele sistemului(reţeaua fizică între reţele);
* departamente, care includ resursele;
* tipurile de informaţii;
* daunele pentru fiecare tip de informaţie;
* bussiness procese, în care se prelucrează informaţia;
* grupurile de utilizatori, care au acces la informaţie;
* clasele căreia îi aparţin grupurile de utilizatori;
* accesul grupurilor de utilizatori la informaţie;
* caracteristicile acestui grup;
* măsurile de protecţie a informaţiei;
* măsurile de protecţie a locului de muncă.

Din aceste date este posibilă crearea un model complet a sistemului informaţional a companiei, la baza căruia va fi făcută analiza protecţiei fiecărui tip de informaţie bazînduse pe resurse şi analiza riscurilor .

**Principiul de lucru al algoritmului**

Riscul se evaluează aparte pentru fiecare legătură (grup de utilizatori - informaţie), modelul crează legătura „subiect - obiect”, luînd în considerare toate caracteristicile acestuia.

Riscul fiecărui tip de informaţie se calculează după trei tipuri de ameninţări de baza:

* confidenţialitate;
* integritate;
* accesibilitate.

Datorită acestor criterii de ameninţări, proiectantul sistemului are o viziune mai simplificată pentru inţelegerea acestora în caz contrar evaluarea riscului nu este totdeauna posibilă.

**Evaluarea riscurilor şi ameninţărilor confidenţialităţii şi integrităţii**

Evaluarea riscurilor şi ameninţărilor confidenţialităţii şi integrităţii.

Determinăm tipul accesului grupului de utilizatori la informaţie. De aceasta va depinde cantitatea măsurilor de protecţie. Pentru accesul local sau de la distanţă se iau diferite măsuri de protecţie;

Determinăm dreptul de acces grupului de utilizatori la informaţie. Aceasta este important pentru integritate, dacă la accesul cu dreptul de „citire” integritatea informaţiei nu trebuie încălcată. Determinarea dreptului de acces influienţează la măsurile de protecţie a informaţiei;

Probabilitatea ameninţării depinde de categoria de utilizatori. De exemplu, utilizatorii anonimi sunt cea mai mare amenintare la informaţiile sensibile ale companiei, deci, dacă grupul are acces la informaţii, creste riscul ca o ameninţare. De asemenea, în funcţie de clasa de utilizatori, se schimbă mijloacele lor de apărare. De exemplu, pentru utilizatorii de pe internet autentificati si anonimi, nu putem determina mijloacele de protectie a locurile de muncă;

Un tip special de protecţie este un software antivirus. In conditiile actuale de functionare a sistemelor calculatoarelor şi anume stocarea şi prelucrarea informaţiei de către resursele software periculoase este ameninţarea cea distructivă. În cazul în care resursa nuare instalat un program anti-virus, atunci probabilitatea de ameninţare a confidenţialităţii, integrităţii şi disponibilităţii creşte dramatic. Modelul primeşte în considerare acest lucru;

Acum avem toate datele necesare pentru a determina mijloacele de securitate a informaţiilor şi a locurilor de muncă a grupurilor de utilizatori. Însumarea valorilor de medii efective, se obţin coeficienţii de securitate. Dacă la resursă este acces local şi de la distanţă, această etapă va fi determinată de trei coeficienţi: coeficient de securitate locală, coeficient de securitate de la distanţă şi coeficientul de siguranţă a locurilor de muncă locală a utilizatorilor. Din aceşti coeficienţi alegem coeficientul minim. Cu cît este mai minim coeficientul, cu atît mai slabă este securitatea;

Se ia in consideraţie sistemele criptografice pentru securitatea datelor la accesul de la distanţă. Daca utilizatorului i se permite accesul de la distanţă la informaţii fărî a se folosi sisteme de criptare, aceasta poate să influienţeze puternic asupra integrităţii şi confidenţialităţii datelor;

În ultimul pas înainte de a obţine coeficientul de securitate pentru relaţia "informaţie- grup de utilizatori", analizăm numărul de persoane din grupul de utilizatori şi disponibilitatea lui la acceslul la internet. Toţi aceşti parametri afectează securitatea informaţiilor;

Deci, după ce parcurgem tot algoritmul, noi primim ultimul coeficient de securitate pentru relaţia „informaţie – grup de utilizatori”;

În continuare coeficientul obţinut trebuie înmulţit la probabilitatea de bază a realizării ameninţării securităţii informaţionale. Probabilitatea de bază se determină în baza estimărilor experţilor. Grupa de experţi, reieşind din clasele grupurilor de utilizatori, obţinînd acces la resurse, tipuri şi drepturi de acces la informaţii, calculează probabilitatea de bază a realizării riscurilor. Reînmulţind probabilitatea de bază şi coeficientul final de securitate, obţinem probabilitatea finală a realizării riscurilor[22,23].

În faza finală sunt determinate valorile probabilităţii impuse de anumite daune aduse de ameninţările şi riscurile acestora la adresa securităţii informaţionale pentru comunicare;

Pentru a ajunge la riscul pentru tipul de informaţii, trebuie mai întîi să utilizăm următoarea formulă:

(3.4)



unde:

= probabilitatea realizării riscului pentru tipurile de informaţii;



= probabilitatea de realizare a riscurilor pentru relaţia „informaţie – grup de utilizatori”;



= cantitatea grupurilor de utilizatori;



Apoi probabilitatea pentru informaţii obţinută înmulţim la daunele realizate de ameninţări, obţinînd în acest mod riscul de la realizarea ameninţării pentru informaţie;

tipurile de informaţii.

**Calcularea riscului privind ameninţarea accesibilităţii**

În etapa finală, valoarea primită de probabilitatea finala a daunelor impuse privind punerea în aplicare a ameninţărilor şi a riscurilor primim date despre noi ameninţări la adresa securităţii datelor pentru relaţia "informaţii – grup de utilizatori".

Deci:

La prima etapă determinăm timpul de nefuncţionare pentru informaţii;

În continuare este nevoie de a calcula coeficientul securităţii pentru relaţia „informaţie – grup utilizatori”. Pentru ameninţarea accesibilităţii, coeficientul securităţii se determină luînd în consideraţie dreptul de acces a grupului de utilizatori la informaţie şi resursele rezervate;

La fel ca şi pentru ameninţările încălcării confidenţialităţii şi accesibilităţii, programele antivirus sunt o resursă specială pentru siguranţă;

Impunînd coeficientul de siguranţă a timpului de nefuncţionare a informaţiei, obţinem timpul de nefuncţionare a informaţiei, luînd în consideraţie resursele de siguranţă a informaţiei. Se calculează în ore pe an;

Parametru specific pentru relaţia „informaţie – grup utilizatori” – timpul de nefuncţionare pentru unităţile de reţea. Accesul la resursa îl poate avea diferite grupe de utilizatori, utilizînd diferite unităţi de reţea. Pentru unitatea de reţea, timpul de nefuncţionare îl indică proprietarul sistemului informatic. Timpul de nefuncţionare a unităţii de reţea se sumează cu timpul de nefuncţionare a informaţiei, obţinute în urma aplicării algoritmului. În acest fel obţinem timpul de nefuncţionare final în relaşia „informaţie – grup utilizatori”;

Valoare timpului de nefuncţionare pentru informaţie, luînd în considerare toate grupurile de utilizatori, ce au acces la ea, se calculează după următoarea formulă:

(3.5)



unde:

– timpul de nefuncţionare pentru informaţie



– timpul de nefuncţionare critic maximal



– timpul de nefuncţionare pentru relaţia „informaţie – grup utilizatori”



n – cantitatea de grupuri de utilizatori

Daunele pentru ameninţările accesibilităţii se stabilesc în ore. Înmulţind timpul de nefuncţionare final şi daunele de la realizarea ameninţării, obţinem riscul realizării ameninţării accesibilităţii pentru relaţia „informaţie – grup utilizatori”.

**Rezultatul algoritmului**

În urma prelucrării datelor cu algoritmul obţinem următoarele date:

* riscul realizării după trei criterii de bază a ameninţărilor pentru tipul de informaţii;
* riscul realizării după trei criterii de bază a ameninţărilor pentru resurse;
* riscul realizării sumare a tuturor ameninţărilor pentru resurse;
* riscul realizării după trei criterii de bază a ameninţărilor asupra sistemului informatic;
* riscul realizării a tuturor ameninţărilor pentru sistemul informatic.

# 3.6 Calculul riscului securităţii informaţionale pe baza unui model de flux de informaţii Metoda Microsoft

În tabelul 3.1 este indicat nivelul de expunere,numerotat de la 1 la 5 și respectiv pentru fiecare nivel este indicată o descriere succintă a riscului activului.

**Tabelul 3.1**- Rata de expunere

|  |  |
| --- | --- |
| **Exposure Rating** | **Confidentiality or Integrity of Asset** |
| 5 | Severe or complete damage to asset, e.g. externally visible and affects business profitability or success |
| 4 | Serious but not complete damage to asset, e.g. affects business profitability or success, may be externally visible |
| 3 | Moderate damage or loss, e.g. affects internal business practices, causes increase in operational costs or reduction of revenue |
| 2 | Low damage or loss, e.g. affects internal business practices, cannot measure increase in costs |
| 1 | Minor or no change in asset |

În tabelul 3.2 este indicat nivelul de expunere și procesul care are loc pentru fiecare nivel.Pentru fiecare nivel este caracteristică o descriere succintă.

**Tabelul 3.2**-Descriere

|  |  |  |
| --- | --- | --- |
| **Exposure Rating** | **Availability** | **Description** |
| 5 | Work stoppage | Substantial support costs or business commitments canceled. |
| 4 | Work interruption | Quantifiable increase in support costs or business commitments delayed. |
| 3 | Work delays | Noticeable impact to support costs and productivity. No measurable business impact. |
| 2 | Work distraction | No measurable impact, minor increases in support or infrastructure costs. |
| 1 | Absorbed by normal business operations | No measurable impact to support costs, productivity, or business commitments. |

În tabelul A.1 din anexa A sunt prezentate mai multe tipuri de resurse, nivele de pătrundere, încercările de a evita conectarea nedorită la resurse, vulnerabilităţile, gradul de risc, probabilitatea apariţiei riscului şi soluţii.

Observăm că fiecare resursă este caracterizată de nivele de securitate precum: nivelul fizic, aplicaţie, host, reţea şi informaţii. Fiecare nivel dispune de riscurile şi vulnerabilităţile sale şi ne indică pericolele.

Nefiind securizate, resursele informaţionale mai tîrziu aduc pagube uriaşe companiilor. Rata de expunere a riscului este înaltă, medie şi joasă.

Aceste date sunt indicate în tabel. Probabilitatea apariţiei riscului la fel este indicată prin termenii înalt, mediu şi scăzut. În ultima coloană a tabelului, sunt indicate sfaturi privind sporirea securităţii fiecărei resurse.

În tabelul A.1 din anexa A sunt colectate date în urma procesării lor. Avem indicate informaţii cu privire la data colectării, numele activelor cît şi clasa lor, vulnerabilităţile depistate, descrierea vulnerabilităţilor şi o notă acordata riscului.

Observăm ca şi aici, fiecare resursă este caracterizată de un grad de impact, deseori înalt. Sunt evidenţiate locurile slabe prin care poate fi manipulată o resursă informaţională şi rata impactului.

Prin culoarea roşie se are invedere impactul înalt al activului iar culoarea verde impactul scăzut.

Datele sunt prelucrate conform tabelelor A.2-A.5 și figurilor A1, A2 din Anexa A

ARO – frecventa de aparitie a amenintarilor asupra riscurilor

SLE – valoarea pabgubei pentru aparitia unui eveniment

ALE – Paguba anuala asteptata

În tabelul 3.3 este reprezentată estimarea cantitativă de anaiză a riscurilor informaționale

**Tabelul 3.3** - Estimarea cantitativă

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Risk Description** | **Asset Class Value** | **Exposure Rating** | **Exposure Value** | **SLE** | **ARO** | **Quantitative Estimate (ALE=SLE\*ARO)** |
| Informatie despre personal Risk | $ 10000 | 4 | 80% | $ 8000 | 0.5 | $ 4000 |
| Informatie despre contabilitate Risk | $ 10000 | 2 | 40% | $ 4000 | 0.3 | $ 1200 |
| Proiectele elaborate | $ 10000 | 3 | 60 % | $ 6000 | 0.5 | $ 3000 |
| Date backup | $ 5000 | 1 | 20 % | $ 1000 | 0.2 | $ 200 |
| Server FTP | $ 10000 | 5 | 100 % | $10000 | 0.5 | $ 5000 |
| Statii de lucru | $ 2500 | 3 | 60 % | $ 1500 | 0.3 | $ 450 |
| Server Backup | $ 5000 | 5 | 100 % | $ 5000 | 0.4 | $ 2000 |
| Router | $ 10000 | 3 | 60 % | $ 6000 | 0.5 | $ 3000 |

4. Descrierea sistemului

Sistem informaţional de analiză cantitativă a riscurilor informaţionale. Acest sistem în baza unor datelor de intrare ca : resursele informaţionale, ameninţări şi vulnerabilităţi va genera un raport în baza metodei de analiză cantitativă a riscurilor informaţionale.

În figura 4.1 este reprezentată interfaţa grafică a softului creat unde avem: Departamente, Resurse, Riscuri, Vulnerabilităţi şi metodele de analiză a riscurilor informaţionale. Din categoria Resurse informaţionale avem: Servere backup, Web servere, Servere baze de date, Staţii de lucru fixe (calculatoare) şi staţiile de lucru mobile Laptopuri.

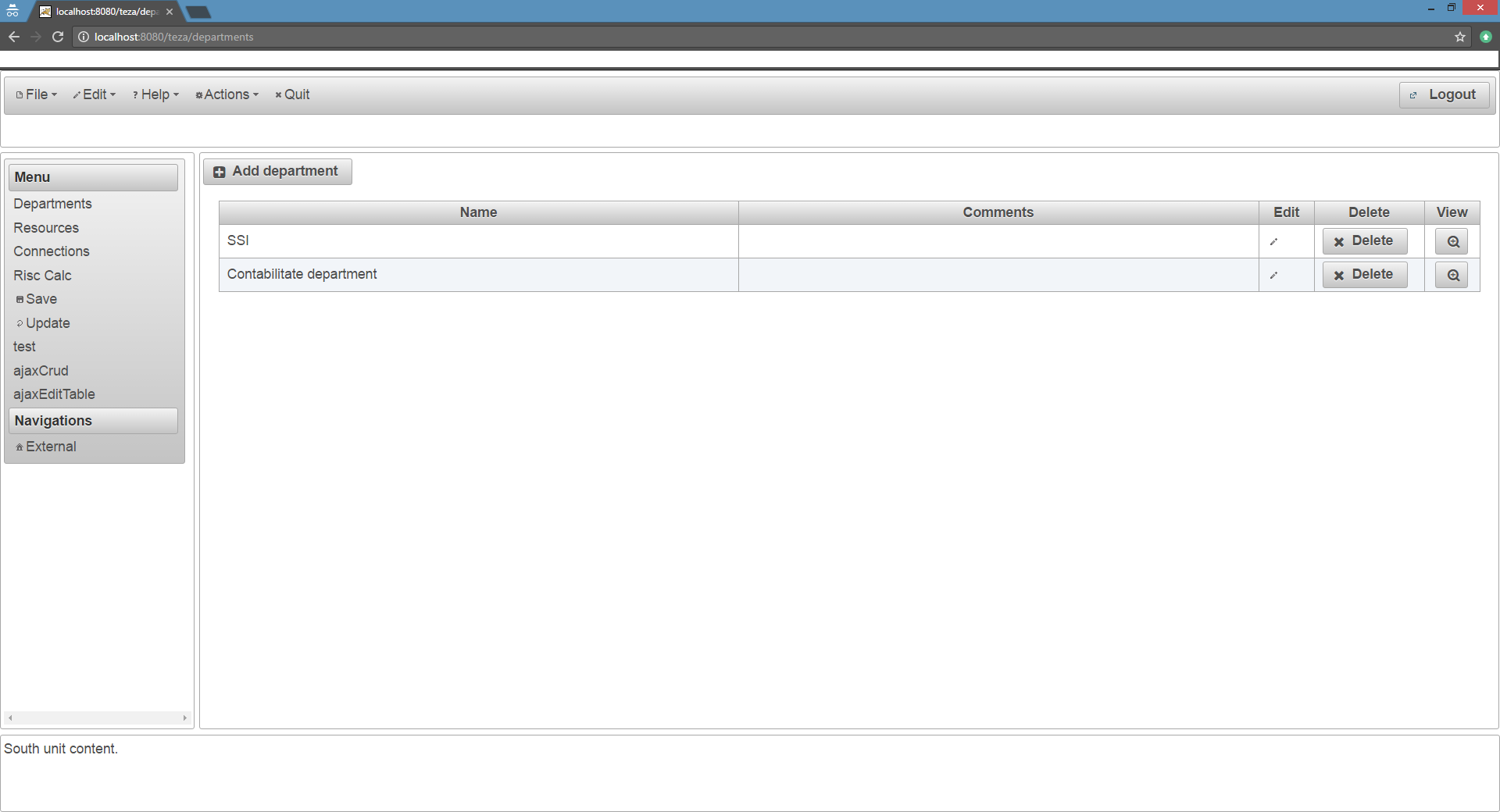


Figura 4.1- Interfața grafică

În figura 4.2 avem reprezentate conexiunile dintre departamente, resurse, riscuri și vulnerabilități. De asemenea este afișat și modul de introducere acestora.

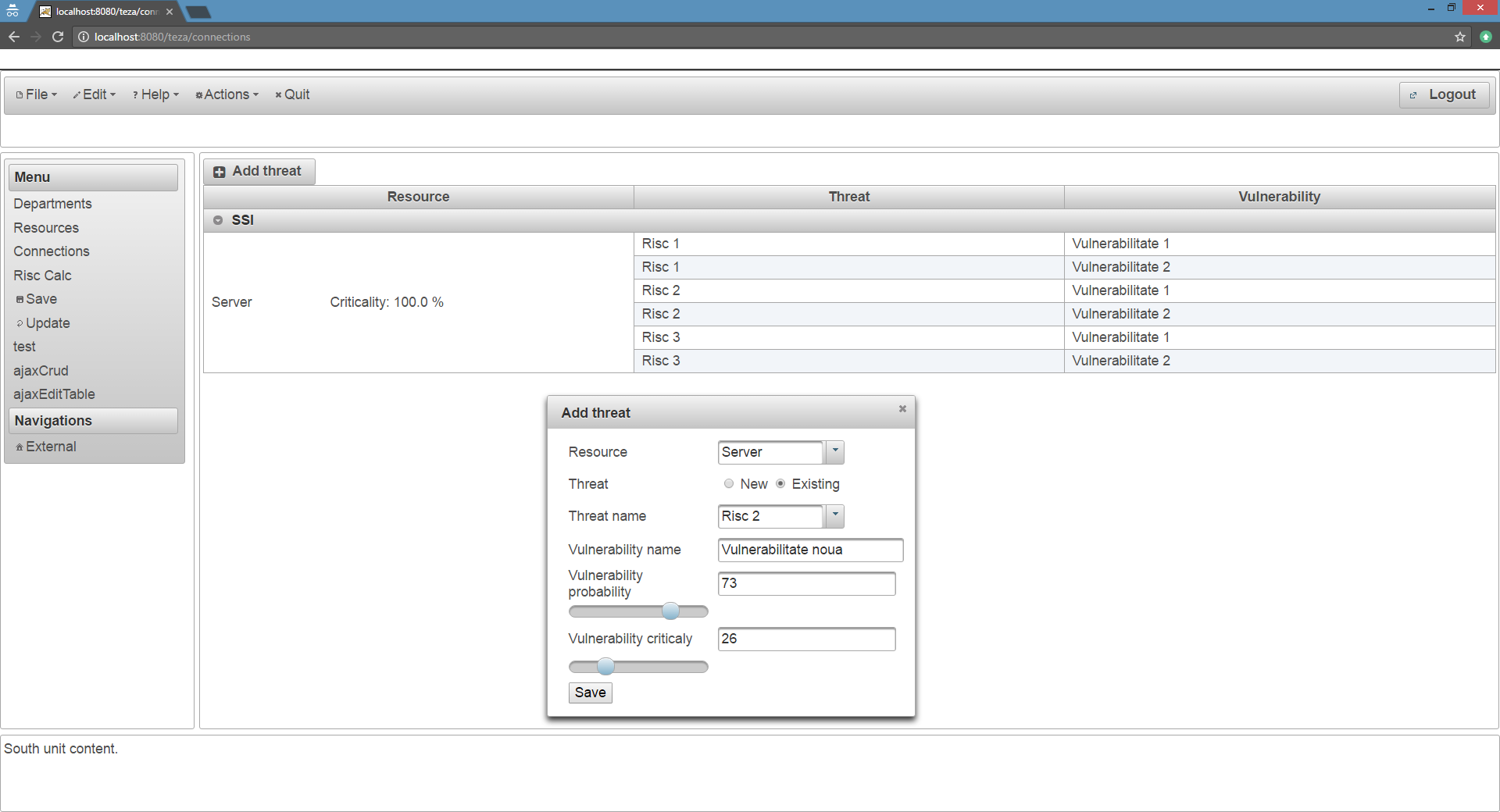


Figura 4.2 - Conexiuni

În figura 4.3 avem reprezentat un rezumat de tip tabel care include toate datele introduse în sistem.

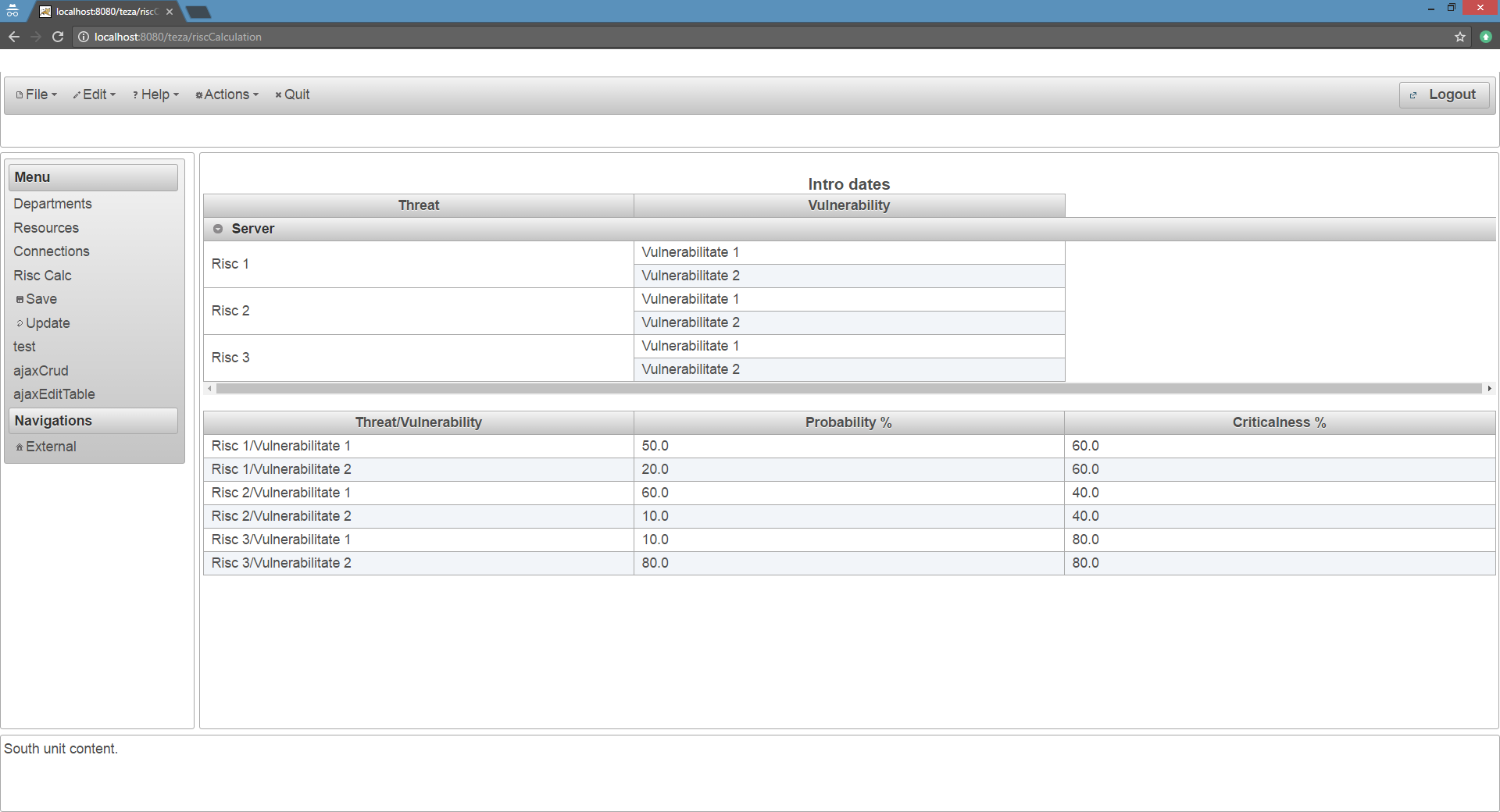


Figura 4.3 – Date de intrare

În continuare urmează generarea raporturilor unde utilizatorul va avea opțiunea de a alege tipul raportului, și datele care le va include acesta. De asemenea se va include și modulul de cheluieli a sistemului informațional, si modulul de aplicare a contramăsurilor, care vor fi indicate rezultatele și diferența acestora in raport.

# 5 Argumentarea economică

**Descrierea proiectului**

Scopul produsului nostru este de a evedenţia principalele vulnerabilităţi ale sistemului informaţional,cît şi valorile bunurilor,activelor.Acest produs este binevenit pentru o companie care realizează importanţa valorii datelor,nevoia de a le securiza la un nivel corespunzător şi valoarea economică a companiei.

Criteriul de lucru al produsului soft se bazează pe analiza cantitativă şi calitativă a riscurilor informaţionale pentru un sistem informaţional.

Acest produs reprezintă un instrument soft de prevenire şi evaluare a riscurilor informaţionale.El interacţionează cu o mulţime de factori tehnici şi umani cum ar fi:acces neautirozat,interceptare tehnică,social engineering;defectarea echipamentelor şi calamităţi naturale.

În zilele noastre sfera tehnologiilor informaţionale şi cu atît mai mult protejarea lor,adică securitatea informaţională joacă un rol crucial în vederea asigurării celor 4 piloni de bază:disponibilitate,confidenţialitate,integritate şi disponibilitate ale datelor sensibile.Începînd de la companii şi pînă la organizaţii mari,ce operează cu echipament tehnic,prelucrează date sensibile de însemnătate mare,au nevoie de acest produs,pentru a putea prezice fenomenul de apariţie ale unor vulnerabilităţi,erori,riscuri.Se zice că este mai uşor de prevenit,decît mai apoi de lecuit.Previziunea este mama înţelepciunii.

Dacă vom analiza utilitatea acestui instrument soft,ne gîndim doar la multitudinea riscurilor şi a ameninţărilor de factori interni şi externi şi este evident că utilitatea instrumentul este foarte mare.Ea va ajuta compania să facă calcule pentru diferite riscuri şi vulnerabilităţi,bunuri,active,etc.

Instrumentul reprezintă un set de mai multe echipamente tehnice,precum ar fi servere,staţii de lucru de la distanţă,echipamente periferice,cărora noi trebuie să le oferim un grad de vulnerabilitate.Sunt mai multe întrebări la care trebuie să raspundem ca în final să avem generat un raport,în care să se stipuleze vulnerabilitatea şi costul riscului pentru fiecare echipament în parte.Interfaţa va fi plăcută iar raportul va conţine tabele şi diagrame colorate pentru utilizatori,cu explicaţii şi detalii tehnice.

Cum am precizat mai sus,produsul va opera cu 2 modalităţi de evaluare a riscurilor:analiză cantitativă şi cea calitativă.

**Algoritmul de analiză calitativă**.În urma proiectării sistemului al unei companii,vor fi afişate următoarele date:

* inventarierea resurselor;
* gradul şi însemnătatea riscului pentru fiecare resursă a companiei;
* gradul şi însemnătatea riscului după setarea contramăsurilor;
* recomandările experţilor.

Persoana care deţine un sistem informaţional,va trebui să descrie arhitectura sistemului său:

* resursele pe care este stocată informaţia;
* secţiile şi resursule deţinute ;
* tipurile de informaţii sensibile;
* grupurile de utilizatori;
* metode şi tehnici de securizare a informaţiei.

Cel de-al doilea algoritm de analiză al riscurilor este **analiza cantitativă.**

Fiecare resursă a companiei este luată în calcul.Ele sunt supuse diferitor riscuri informaţionale şi se calculează probabilitatea riscurilor şi toate ameninţările.Algoritmul dat ne va oferi date precum:

* inventarierea resurselor;
* gradul riscului pentru fiecare resursă;
* gradul riscului pentru fiecare resursă dupa aplicarea contramăsurilor;
* eficienţa aplicării cotnramăsurilor.

Instrumentul dat analizează riscurile din exterior şi interior,calculează pagubele şi costul resurselor informaţionale ale unei companii.Este un instrument foarte eficient de a perfecţiona sistemul de securitate al companiei şi oferă detalii tehnice importante pentru a spori gradul de securitate.O putem numi şi o forma al unui audit de securitate virtual,apliact pe staţiile de lucru.

**Planul calendaristic**

Planul calendaristic include etapele de desfăşurare a procesului de repartizare şi elaborare a sarcinilor. Elaborarea v-a dura 3 luni, pe parcursul acestui timp se va coopera cu viitorii utilizatori pentru a afla opiniile privitor la funcţionalitatea bazei de date. Planul calendaristic include informaţia referitoare la executarea în timp a acţiunilor planificate. Rezultatele planificării sunt enumerate în tabelul 5.1

În tabelul 5.1 este prezentat grupul de lucru şi membrii acestuia.Fiecare lucrător are abrevierea sa respectivă în coloana alăturată.

**Tabelul 5.1 -** Componenţa grupului de lucru

|  |  |  |
| --- | --- | --- |
| Numărul | Funcţia îndeplinită | Executanţi |
| 1. | Conducătorul proiectului | C |
| 2. | Executant | E |
| 3. | Programator | P |
| 4. | Tester | T |

În tabelul 5.2 este prezentat volumul de lucru, tema, zilele alocate pentru finisarea sarcinii şi persoana din echipă care este responsabilă de efectuarea lucrării, sunt prezente şi comentarii pe marginea efectuării temei.

**Tabelul 5.2** -Planul calendaristic

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr acţiunii | Denumirea acţiunii | | Perioada,  (zile) | Persoane implicate | Comentarii |
| 1 | Stabilirea temei pentru teza de licenţă | | 5 | C  E | Sarcina a fost propusă de C, discutată cu D |
| 2 | Acceptarea temei pentru teza de licenţă | | 1 | E  C |  |
| 3 | Efectuarea analizei sarcinilor propuse | | 2 | C  E | Studierea amanunta a sarcinilor propuse |
| 4 | Studierea informaţiilor necesare pentru teza de licenţă | | 20 | C  E | Documentarea cu informaţiile necesare |
| 5 | Elaborarea structurii sistemului de evaluare a riscurilor informaţionale | | 15 | E  P |  |
| 6 | Elaborarea şi implementarea standardelor pentru sarcina propusă | | 10 | E  P | Implementarea standardului ISO 27001 |
| 7 | Crearea programului pentru generarea raportului | | 5 | E  P | În urma execuției programului se generează raportul |
| 8 | Crearea interfeţei , verificarea şi testarea programului | | 1 | E  P  T | Finalizarea sistemului |
| 9 | Testarea vizuală şi crearea variantei definitive a programului pentru analiza riscurilor, corectarea lui în cazuri necesare | | 3 | E  T |  |
| 10 | Redactare sintaxei pentru generarea procedurilor de intrare/ieşire a rapoartelor | | 2 | E  T |  |
| 11 | Calculare cheltuielilor pentru proiectul de licenţă | | 5 | C  E | În baza calcurilor se aplica toate cheltuielile care au stat la baza efectuării sistemului |
| Continuare tabel 5.2 | | | | | |
| 12 | Verificarea proiectului | | 4 | C  E | Verificarea şi analiza finală a proiectului, efectuarea ultimelor schimbări |
| 13 | Finisarea proiectului | | 2 | C  E |  |
| Total |  | | 75 |  |  |
| Inclusiv | |  |  |  |  |
| Conducatorul proiectului | | | 39 |  |  |
| Executant | | | 75 |  |  |
| Programa-tor | | | 31 |  |  |
| Tester | | | 6 |  |  |

**Calcule economice**

Pentru calcularea preţului de cost al dispozitivului sunt necesare de efectuat următoarele calcule: cheltuielile materiale si nemateriale, uzura echipamentelor, salarizarea angajaţilor si cheltuielile de regie a proiectului.

**Buget**

În tabelul 5.3 sunt prezentate valorile echipamentelor procurate şi tipul echipamentelor tehnice.

**Tabelul 5.3** -Imobilizări corporale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr. | Denumirea | Un. Mas | Preţ achiziţie, lei (fără TVA) | Cantitatea | Valoarea toatală, lei |
| 1 | Laptop Asus zenbook UX31A | buc | 13 000 | 1 | 13 000 |
| 2 | Imprimantă Brother hl5030 | buc | 3600 | 1 | 3 600 |
| 3 | Router | buc | 1 500 | 1 | 1 500 |
|  |  |  | Total |  | 18 100 |

În tabelul 5.4 sun prezentate imobilizările necorporale, softurile și platforma de programare.

**Tabelul 5.4**-Imobilizări necorporale

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr. | Denumirea | Un. Mas | Preţ achiziţie, lei (fără TVA) | Cantitatea | Valoarea toatala, lei |
| 1 | OSWindos 7 | buc | 3 100 | 1 | 3 100 |
| 2 | Microsoft office | buc | 3 000 | 1 | 3 000 |
| 3 | NetBeans IDE 8.0.2 | buc | gratis | 1 |  |
|  |  |  | Total |  | 6 100 |

În tabelul 5.5 sunt prezentate consumurile materialelor directe pe perioada executării sistemului.

**Tabelul 5.5**-Consumuri materiale directe

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nr. | Denumirea | Un. mas | Preţ achiziţie pe unitate, lei (fără TVA) | Cantitatea | Valoarea totală, lei |
| 1 | CD | buc | 10 | 10 | 100 |
| 2 | Hîrtie A4 | buc | 80 | 1\*pachet (500 foi) | 80 |
| 3 | Rechezite de birou | buc | 270 | 1 | 270 |
| 4 | Carte SMSI | buc | 350 | 1 | 350 |
| 5 | Carte ISO 27001 | buc | 320 | 1 | 320 |
| 6 | Carte ISO 27005 | buc | 320 | 1 | 320 |
| 7 | Materiale de igienizare | buc | 250 | 1 | 250 |
| 8 | Materiale uz casnice | buc | 300 | 1 | 300 |
| 9 | USB-uri | buc | 170 | 2 | 340 |
| 10 | HDD extern | buc | 700 | 1 | 700 |
|  |  |  | Total |  | 3 030 |

**Retribuirea muncii**

La realizarea proiectului au contribuit patru persoane. Conducătorul de proiect are calificarea cea mai mare de experienţă personală. El participă la realizarea proiectului atunci cînd este necesar de fixat obiective şi de găsit soluţii majore. Conlucrează cu diplomantul pentru a afla cît mai multă informaţie despre rezultatul final aşteptat. Programatorul se ocupă de testarea si elaborarea programului.

Suma care este indicată ca salariul pentru executorii proiectului include şi impozitele de stat: plăţi în fondul social şi asigurarea medicală. Legea Bugetului asigurărilor sociale a stabilit impozitul pentru fondul social, în anul 2015, în valoare de 23%. Legea Republicii Moldova „Privind fondurile asigurării obligatorii de asistenţă medicală” a stabilit impozitul pentru anul 2015 în valoare de 4,5%.

În tabelul 5.6 este indicat volum de lucru pentru fiecare funcţie de angajat,salariul pe zi şi valoarea totală pentru toţi angajaţii.

Calculul indicatorilor

Frm – Fondul de retribuire a muncii.

FAS – suma contribuţiilor în Fondul Social

Cfs – cota contribuţiilor de asigurări sociale de stat obligatorii (23%)

FAM – suma contribuţiilor pentru Asigurare Medicală

Cam – cota prime de asigurare obligatorie de asistenţă medicală(4,5%)

FS = Frm x Cfs = 20 450 x 0,23 = 4704 (lei)

FAM = Frm x Cam = 20 450 x 0,045 = 921 (lei)

**Tabelul 5.6**-Consumuri materiale directe de remunerare a angajaţilor

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Nr. | Funcţia angajatului | Volumul de lucru, zile | Salariu pe zi, lei | Suma, lei | FAS, lei | FAM,  Lei |
| 1 | Executant | 75 | 100 | 7 500 | 1725 | 337,5 |
| 2 | Programator | 31 | 200 | 6 200 | 1426 | 279 |
| 3 | Tester | 6 | 150 | 900 | 207 | 40,5 |
| 4 | Conducatorul proiectului | 39 | 150 | 5850 | 1345 | 263,25 |
|  |  |  |  |  |  |  |
| Total |  |  | 20 450 |  | 4 704 | 921 |

**Cheltuieli indirecte**

În tabelul 5.7 sunt indicate cheltuielele ce ţin de întreţinerea încăperii şi serviciile comunale.

**Tabelul 5.7**-Cheltuieli indirecte

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Denumirea articolului | Un. Mas | Cantitatea | Tarif/un, lei | Durata proiectlui,  Luni | Valoarea totala, lei |
| Arenda încăperii | m2 | 20 | 300 | 3 | 18 000 |
| Paza | lunar | 1 | 450 | 3 | 1 350 |
| Energie electrică | Kw/h | 500 | 1,58 |  | 790 |
| Servicii internet | lunar | 1 | 230 | 3 | 690 |
| Materiale auxiliare | set | 1 | 1200 |  | 1200 |
|  |  |  |  |  |  |
| Total |  |  |  |  | 22 030 |

Pe lângă cheltuielile pentru materiale şi active este necesar de luat în calcul uzura tehnicii. În tabelul de mai jos am prezentat uzura echipamentului utilizat la producerea proiectului.

În tabelul 5.8 este reprezentat calculul fondului de amortizare a imobilizării corporale care se calculează conform formulei (5.1)

**Tabelul 5.8**-Fondul de amortizare imobilizări corporale

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Denumirea instalaţiei | Cantit. | Preţul, lei | Termenul de utilizare(ani) | Fondul de amortizare, lei |
| Laptop | 1 | 13 000 | 5 | 650 |
| Imprimanta | 1 | 3 600 | 5 | 180 |
| Total | | | | 830 |

Fondul de amortizare se calculează pentru 5 ani după formula:

(5.1)

Unde: T – este termenul de utilizare a componentei, în luni

T1 – este termenul de efectuare a proiectului, în luni

* Calculul uzurii pentru calculator:

FA laptop= (13 000x3)/60= 650 lei

* Calculul uzurii pentru imprimanta:

FA imprimanta= (3 600x3)/60=180 lei

În tabelul 5.9 este prezentat calculul fondului de amortizare a imobilizării necorporale ce se calculează după formula (5.2)

**Tabelul 5.9-** Amortizarea imobilizări necorporale

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Denumirea instalaţiei | Cantit. | Preţul, lei | Termenul de utilizare(ani) | Uzura, lei |
| OS Windows 7 | 1 | 3100 | 3 | 259 |
| Microsoft Office | 1 | 3000 | 3 | 250 |
| Total | | | | 509 |

Odată cu trecerea timpului,produsele soft se învechesc moral şi necesită un upgrade.

(5.2)

Unde: T – este termenul de utilizare a componentei, în luni

T1 – este termenul de efectuare a proiectului, în luni

* Calculul amortizării pentru OS Windows 7:

Am OS Windows 7 = (3100\*3)/36= 259 lei

* Calculul amortizării pentru Microsoft Office:

Am Microsoft Office= (3000\*3)/36=250 lei

**Preţ de cost**

Pentru a stabili calculul de livrare a proiectului către beneficiarul nostru vom face calculul cheltuielilor totale de elaborare la care vom adăuga un cuantum de 20%, profit net introdus de realizarea acestui proiect.

**Tabelul 5.10-** Cheltuielile totale de elaborare a proiectului

|  |  |
| --- | --- |
| Articole de calculaţie | Valoarea calculată (lei) |
| Consumuri materiale directe | 3030 |
| Fondul de remunerare a muncii | 20 450 |
| Fondul social | 4 704 |
| Asigurarea medicală | 921 |
| Cheltuieli indirecte | 22 030 |
| Fondul amortizare imobilizări corporale | 830 |
| Fondul amortizare imobilizări necorporale | 509 |
| Total | 53 813 |

**Rezultate financiare**

**Pentru început calculăm cifra de afaceri brută**

Cifra de afaceri cuprinde suma totală a veniturilor din operaţiunile comerciale efectuate de firmă, respectiv vânzarea de mărfuri şi produse într-o perioadă de timp determinată. În cuantumul cifrei de afaceri nu se includ veniturile financiare şi veniturile exceptionale, conform formulei (5.3).

(5.3)

=3x19000+2x17000+1x20000 = 111 000 lei (inclusiv TVA)

**Cifra de afaceri netă**

În cadrul reglementărilor contabile este definită cifra de afaceri netă care cuprinde „sumele rezultate din vânzarea de produse şi furnizarea de servicii care se înscriu în activitatea curentă a entităţii, după deducerea reducerilor comerciale şi a taxei pe valoarea adăugată, precum şi a altor taxe legate direct de cifra de afaceri , ce se calculează conform formulei (5.4).

(5.4)

=111 000 – 20%= 88 800 lei

**Profit brut**

În[contabilitate](http://ro.wikipedia.org/wiki/Contabilitate)şi[finanţe](http://ro.wikipedia.org/wiki/Finan%C8%9Be),profitul brutsauvenitul din exploatareeste o măsură a rentabilităţii unei[firme](http://ro.wikipedia.org/wiki/Companie)care exclude dobânda şi cheltuielile de impozit pe[venit](http://ro.wikipedia.org/wiki/Venit), conform formulei (5.5).

Profitul brut =[Venitul](http://ro.wikipedia.org/wiki/Venit)- Cheltuieli de funcţionare

(5.5)

-cost total

=88 800-53 813= 34 987 lei

**Profit net**

Venitul net este venitul rezidual al unei [firme](http://ro.wikipedia.org/wiki/Companie), după adăugarea veniturilor totale şi câştigurilor şi scăzând toate cheltuielile şi pierderile pentru perioada de raportare. Profitul net poate fi distribuit între deţinătorii de acţiuni comune sub formă de dividende sau deţinute de [firmă](http://ro.wikipedia.org/wiki/Companie) ca o completare a rezultatului reportat, conform formulei (5.6).

(5.6)

- Impozitul pe venit

Pentru persoane juridice Impozitul pe venit este 12%

=0,12x34987=4198 lei

= 34 987- 4198= 30 789 lei

**Rentabilitatea costurilor**

Rentabilitatea costurilor măsoară eficienţa consumului de resurse umane şi materiale.Se situează la un nivel scăzut,înregistrînd aproximativ aceeiaşi evoluţie ca şi rata rentabilităţii veniturilor, ce se calculează conform formulei (5.7).

(5.7)

= (34 987/53 813) x100%= 65%

**Noţiunea şi caracteristicile resurselor umane**

Managementul Resurselor Umane constă în ansamblul activităţilor orientate către asigurarea, dezvoltarea şi menţinerea resurselor umane în cadrul organizaţiei în vederea realizării cu eficienţă maximă a obiectivelor acesteia şi satisfacerii nevoilor angajaţilor.

Pe măsură ce organizaţiile se dezvoltă au de a face cu o serie de aspecte esenţiale ale managementului resurselor umane. Managerii creează un plan de atragere şi reţinere a persoanelor cu abilităţile de care are nevoie organizaţia. Implementarea planului presupune recrutarea, selecţia, integrarea, instruirea, recompensarea, alegerea beneficiilor celor mai potrivite şi evaluarea permanentă a performanţelor pentru a se verifica dacă sunt atinse obiectivele organizaţionale. Aceste activităţi reprezintă componentele managementului resurselor umane.

Efectuînd un program sau soft, e foarte important să luăm în consideraţie investiţiile şi beneficiile de pe urma proiectului realizat. Realizând calculele de mai sus am arătat care sunt cheltuielile pentru realizarea proiectului şi care beneficiu se aşteaptă la finalizarea proiectului.

Cum am şi specificat mai sus,acest instrument este foarte important pentru o companie care doreşte să menţină securitatea datelor la un nivel înalt,şi periodic politica de securitate trebuie revăzută şi îmbunătăţită.La prima vedere,costul instrumentului nu este aşa de mare pentru o companie.Daunele în urma scurgerii informaţiei pot fi cu mult mai mari.Respectiv compania trebuie singură să înţeleagă necesitatea şi importanţa acestui instrument de analiză cantitativă şi calitativă a riscurilor informaţionale.

**Bibliografie**

1. Popa Sorin Eugen, Securitatea sistemelor informaţionale,Universitatea „Vasile Alecsandri”, Bacău, 2007.
2. D.Oprea , Sistemul de management al securităţii informaţionale, Universității „Alexandru Ioan Cuza”, Iași, 2007
3. Consultanta ISO 27001 – Standard pentru Securitatea Informatiei,2006, [Resursă electronică]. – regim de acces:

http://www.consultanta-certificare.ro/iso-27001-securitatea-informatiei.html

1. ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements, 2005
2. ISO/IEC 27005, Information technology – Security techniques – Information security risk management systems, Second Edition, 2009, [Resursă electronică]. – regim de acces:

http://ionmuntean.com/2009/09/23/isoiec270052008/

1. ISO/IEC 27005 Информационная технология – Методы защиты – Менеджмент рисков
2. информационной безопасности. BS ISO/IEC 27005:2008. – 2008. – Технический перевод v.2.6 от 4.02.2011.
3. International Standardization Organization, ISO/IEC 27005, Second Edition 2011-06-01, Information Technology – Security Techniques – Information Security Risk Management
4. Veronika JINERENCO, Andrei ANGHEL ,Cond. șt. Rodica BULAI, Analiza riscurilor la adresa securitatii informationale, „Universității Tehnică a Moldovei”, Chişinău, 2012.
5. Măzăreanu P. Valentin, *Risk management and analysis: risk assessment (qualitative and quantitative)*, Analize științifice ale Universității „Alexandru Ioan Cuza”, Iași, 2007.
6. Ion I. Bucur, *Evaluarea și managementul riscurilor de securitate* // [Resursă electronică]. – regim de acces:
7. Cursuri master[Resursă electronică]. – regim de acces:

* http://www.xanderzone.ro/cursurimaster/C-II-4.pdf.
* http://www.xanderzone.ro/cursurimaster/C-II-2.pdf.
* http://www.xanderzone.ro/cursurimaster/C-II-1.pdf.

1. Analiza riscurilor informaţionale, [Resursă electronică]. – regim de acces:

http://www.securitatea-informatica.ro/

1. Amril Syalim Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft’s Security Management Guide [Электронныйресурс] // Amril Syalim, Yoshiaki Hori, Kouichi Sakurai – Режимдоступа: [Resursă electronică]. – regim de acces:
2. [Resursă electronică]. – regim de acces: http://rminv.enisa.europa.eu/tools/t\_mehari.html
3. Табаков Rot Artur, *IT Risk Assessment: Quantitative and Qualitative Approach*, Proceedings of the World Congress on Engineering and Computer Science, WCECS 2008, October 23-24, San Francisco, USA.
4. Полянский Д.А., Файман О.И., Mетодика аудита информационной безопасности объекта информатизации [Resursă electronică]. – regim de acces:

* http://bibliofond.ru/view.aspx?id=552378.
* OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM ,[Resursă electronică]. – regim de acces:
* http://www.cert.org/octave/octavemethod.html

1. Методики и программные продукты для оценки рисков, CRAM,FRAP, RiskWatch, [Resursă electronică]. – regim de acces:

http://www.intuit.ru/department/itmngt/riskanms/4/.

1. GRIF (Digital Security), [Resursă electronică]. – regim de acces:

http://www.dsec.ru.

1. EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), MÉTHODE DE GESTION DES RISQUES, [Resursă electronică]. – regim de acces:

http://rm-inv.enisa.europa.eu/tools/t\_ebios.html.

1. StormsA,[Using vulnerability assessment tools to develop an OCTAVE Risk Profile](http://www.sans.org), [Resursă electronică]. – regim de acces:

http://www.sans.org/.

1. [RiskWatch users manual](http://www.riskwatch.com), [Resursă electronică]. – regim de acces:

http://www.riskwatch.com/.

1. Nicolae Bârsan-Pipu, IonPopescu, Managementul riscului. Concepte, Metode,Aplicaţii,ed:Universităţii„Transilvania”Braşov’,2003,214p.