SISTEME DE COMUNICAȚIE COLABORATIVE VS SECURITATEA INFORMAȚIONALĂ

Iulia Mirescu

Iulia.mirescu@ici.ro

Institutul Național de Cercetare - Dezvoltare în Informatică, ICI Bucureşti

Rezumat: Epoca modernă se caracterizează prin multi-comunicare. În era Internetului, în care se pot găsi aproximativ trei miliarde de IP-uri care reprezintă modalitatea de contorizare a utilizatorilor conectați în rețeaua Internet la un moment dat, sunt disponibile informații din toate sferele de activitate, pentru diferite exigente informaționale. În această avalanşă de informații trebuie avute în vedere două observații: calitatea conexiunii (parametrii de comunicație harware şi software) în care este inclusă firește lipsa oricărui intruder de orice natură, adică securitatea actului de comunicare, şi al doilea element îl reprezintă mediul în care se face comunicarea şi în care toți participanții sunt mai mult sau mai puțin colaboratori. În lucrarea de față vom aborda sisteme colaborative şi modalități de asigurare a unui management corect al securității mediului informatic, vom dezvolta această lucrare.

Cuvinte cheie: sisteme de comunicație, sisteme colaborative, managementul securității sistemelor în formatice, securitatea sistemelor informatice şi informaționale, rețele private de comunicație.

Abstract: The modern era is characterized by multi-communication. In the Internet age, where you can find about three billion of IPs, which represents the fizical counter of the users connected to the Internet at a time, we can find information of all spheres of activity, corresponding to different information demands. In this avalanche of information should be considered two points: the quality of the connection (communication hardware and software parameters) that included the absence of any intruder of any kind, which means the act of communication security and the second element, is the environment of the communication in which all participants are more or less employees. About collaboration systems and some ways of ensuring proper management of information security environment we will talk about in this paper.

Key words: communication systems, collaborative systems, security management of information and informatic systems, private communication network.

1. Introducere

În zilele noastre, companiile adoptă deschideri din ce în ce mai mari către partenerii lor (utilizând relații fie instituționalizate, fie regulate sau sporadice), iar acest lucru reprezintă o caracteristică inevitabilă a evoluției pieței. Această nevoie de rețea se bazează pe mai multe aspecte: concurența, îmbunătățirea schimbului (de informații şi/sau bunuri), complexitatea tot mai mare a produselor. Capacitatea companiilor de a colabora între ele (în plus într-un mod eficient) devine în acest fel un factor determinant pentru evoluția lor şi pentru capacitatea de a supraviețui. La începutul anilor ’90 apărea pe piața ICT un nou concept: sisteme colaborative. Acesta s-a născut din necesitatea tot mai evidentă a unor comunități distincte de a-şi specializa serviciile, produsele software, sistemele informatice pe o anumită tipoplogie tematică profesională.

Colaborarea este un concept larg şi trebuie poziționat în funcție de numeroase alte concepte, clasificări şi definiții. În acest articol în mod deliberat nu se vor discuta termeni şi cuvinte (pentru a evita o dezbatere lexicală despre colaborare, cooperare şi aşa mai departe), ci ne vom concentra asupra nivelurilor de colaborare din punct de vedere conceptual şi vom rafina acest studiu de la conceptul general de colaborare către colaborarea specifică sistemelor informatice, în strânsă conexiune cu [2].

Sistemele colaborative reprezintă un subiect important al societății bazate pe cunoaştere şi o parte importantă a activităților umane sunt implicate în acest domeniu. Ştiința are un mare impact asupra dezvoltării diferitelor tipuri de sisteme de colaborare din domenii de activitate variate [1].

1.2 Tipuri de sisteme colaborative

Există mai multe criterii pentru clasificarea sistemelor de colaborare. După tipul de criterii de aplicare, sistemele de colaborare sunt:

- *sisteme colaborative în domeniul educației*: sunt aplicate în domeniul educațional şi vizează evaluarea şi consolidarea performanței din procesul educațional;
- *sisteme colaborative de apărare*: anvizajează domeniul militar şi sunt caracterizate de reguli stricte de funcționare şi organizare;
- *sisteme colaborative în productie*: sunt concepute pentru a creşte capacitatea de producție şi calitatea în diferite unități producătoare de bunuri şi servicii;
- *sisteme colaborative bancare*: sunt proiectate cu scopul de a analiza, şi de a determina factorii care afectează sistemul bancar şi componentele sale.[3]

După criteriile de organizare sistemele colaborative sunt:

- ***Lineare***

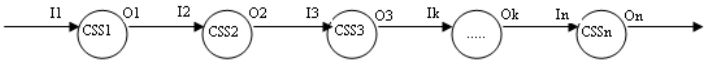

Figura 1. Structură lineară

În sistemul colaborativ liniar prezentat în figura 1, intrările inițiale sunt I1 şi ieşirile sunt On. La nivelele intermediare, ieşirile subsistemului k-1 sunt intrările pentru subsistemul k. Aceste tipuri de sisteme colaborative sunt întâlnite în domeniul educației, fiecare subsistem reprezentând o şcoală absolvită.

- ***Copac***

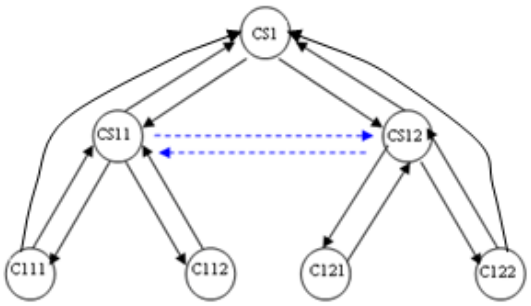

Figura 2. Structura copac

În sistemul colaborativ cu structură copac mesajele se deplasează între subsisteme, în sensul ierarhic ceea ce înseamnă că un mesaj de la nivelul doi va ajunge la nivel de top numai dacă trece în primul rând prin nivelul unu. În exemplul prezentat în figura 2, fiecare subsistem are mai multe intrări şi ieşiri multe ieşiri împreună cu fluxurile de informații se deplasează în ambele sensuri. În sistemele de colaborare cu structură copac, există şi excepții, ca în figura 2, în care un mesaj de la nivelul doi poate ajunge la nivel de top, fără a trece prin primul nivel. Schimbul de informații între fluxuri se poate face, de asemenea, la acelaşi nivel ierarhic; în exemplul din figura 2 între şi CS11şi CS12. Sisteme cu acest tip de organizare se pot întâlni în managementul organizațional şi în administrația publică.

- ***Rețea***

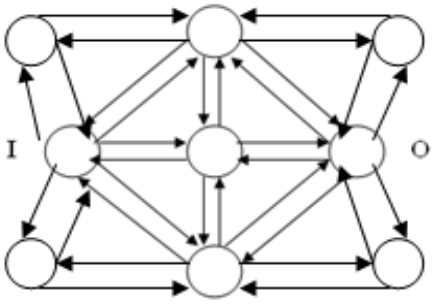

Figura 3. Structură de rețea

În cazul unui sistem colaborativ cu structură tip rețea, subsistemele sunt toate interconectate, astfel încât toate transferurile sunt interdependente. În cadrul unui astfel de sistem, mesajele circulă între toate componentele, fără nicio restricție. Sistemele colaborative de tip rețea se pot întâlni în domeniul producției şi în cel bancar [4]. Sistemele colaborative de tip Multi-Agent [5], cele mai des citate în articole scrise la conferințe şi prezentări, sunt considerate a fi cele care dezvoltă următoarele probleme:

- agenți – concepte cheie;
- fundamentele interacțiunii agenților;
- modele formale de colaborare;
- metodologia orientată multi-agent a ingineriei software;
- dezvoltarea sistemelor agent;
- agenți care au la bază unelte personale ale căutării colaborative.

2. Colaborarea şi sistemul informatic (Information System)

2.1 Colaborarea la nivelul întreprinderii

La nivelul întreprinderii, pe baza sintezelor din standardul **IEC TC 65/290/DC,** se desprind următoarele nivele de compatibilitate (denominările originale date între paranteze au fost convertite în nivele de compatibilitate) după cum urmează:

- nivelul 1 (coexistent): poate exista independent într-o rețea unică;
- nivelul 2 (interconectabil): poate impărtăşi sau schimba informații;
- nivelul 3 (interoperativ): poate impărtăşi functionalități sau servicii;
- nivelul 4 (interoperabil): poate funcționa în conformitate cu un comportament colectiv predefinit.

Compatibility level / Compatibility nature	1	2	3	4
Definition of a collaborative behavior				X
Sharing of functionalities and services			X	X
Exchange or sharing of information		X	X	X
Involvement in a communication network	X	X	X	X

Figura 4. Nivele de compatibilitate

Din acest studiu se desprind două consecințe. Prima poate fi dedusă în mod direct: nivele de colaborare introduc nivele colaborative. Cea de-a doua consecință este indirectă şi pune accent pe aspectele de vedere temporale ale colaborării: pentru a colabora, întreprinderile trebuie să construiască colectiv calea care le va aduce de la eterogenitate la nivelul corect de percepție. Acesta este un act dinamic, care aduce partenerii în relații instituționalizate, regulate sau sporadice.

	Data	Data and applications	Data, applications and processes
Sporadic exchange	Level 1	Level 3	Level 5
Instituted integration	Level 2	Level 4	Level 6

Figura 5. Poziția relativă de nivelelor de înțelegere între partenerii industriali

Pornind de la aceste considerente vom putea defini următoarele nivele de înțelegere (denominările native care sunt date între paranteze şi care au fost convertite în nivele de compatibilitate):

- nivelul 1 (comunicare): schimb sporadic de date,
- nivelul 2 (coordonare): schimb de date structurat şi instituționalizat,
- nivelul 3 (colaborativ): date sporadice şi schimb de aplicații,
- nivelul 4 (cooperare): schimb de date şi aplicații structurat şi instituționalizat.

Pentru a confrunta considerațiile expuse anterior cu problematica proiectării unui sistem informatic în context colaborativ, în cele ce urmează vom relata la nivel abstract şi conceptual puncte de vedere relative la conceperea sistemelor informatice colaborative (CIS – Collaborative Informtion System). În acest sens:

Reix, în [11], defineşte noțiunea de sistem informatic ca un set organizat de resurse (hardware, software, oameni, date, procese) în măsură să dobândească tratarea, stocarea şi exportul de informații (definite ca date, text, imagini, sunete, etc.) în organizații;

Bernus, în [8], consideră că un sistem informatic trebuie să se asigure că informațiile corecte sunt disponibile la locul potrivit, la momentul potrivit. Noțiunile de *locul potrivit şi momentul potrivit* se referă la un sistem de management al proceselor care sincronizează comportamentul şi contabilitatea informațiilor din interiorul IS (Information System).

Morley, în [9], prezintă IS ca un compus format din două subsisteme: un sistem de management al informațiilor (care pot fi actori, date şi procese) şi un sistem de calcul (inluzând resursele hardware şi software, baze de date şi funcții).

Cele trei puncte de vedere ale lui Reix, Bernus şi Morley subliniază câteva variabile care trebuie avute în vedere în modelarea unui sistem informatic. Putem rezuma aceste variabile în conformitate cu următorul principiu: un sistem informatic sprijină procesele întreprinderii în primul rând prin gestionarea serviciilor şi funcțiilor disponibile în cadrul companiei şi în al doilea rând, prin impactul pe care îl are informația, manifestat prin transport şi depozitare. Actorii şi resursele întreprinderii, total implicați în sistemul informatic în ansamblu, nu sunt prezentați în figura 6 datorită faptului că obiectivul principal al reprezentării îl constituie proiectarea unui IS.

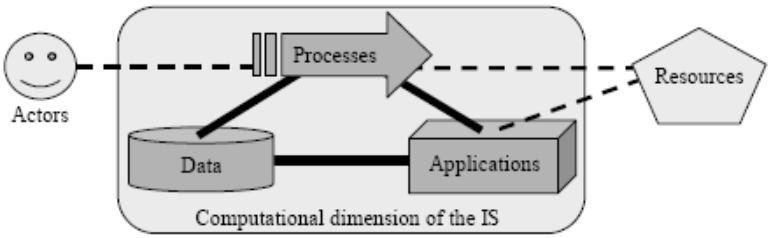

Figura 6. O imagine vizuală asupra unui IS

Acest punct de vedere al sistemului informatic (şi în special în partea sa de calcul) oferă avantajul de a fi coerent cu punctele expuse la subcapitolul 2.1 cu privire la nivelurile de colaborare şi criteriile de caracterizare statice (de date, aplicații şi procese). În consecință, vom folosi reprezentarea logică a IS pentru a studia consecințele colaborării unui IS şi ale partenerilor:

- **conversia de date:** pentru continuitate, interacțiunile între sistemele informatice au nevoie de instrumente eficiente de transformare a datelor (stil, format). În acest context, este esențial ca datele să poată fi transmise între partenerii de colaborare în mod eficient. Cu alte cuvinte, chiar dacă fiecare partener îşi poate conserva confidențialitatea şi, deci işi poate stabili drepturi de acces specifice pe care domeniul informațional accesat le permite, colaborarea între întreprinderi implică separarea în mod clar între sensul

semantic al datelor şi forma lor sintactică pentru o integrare informațională optimă;

- **managementul aplicațiilor:** în general, servicii şi aplicații ale diverşilor parteneri nu sunt construite pentru a fi compatibile. Cu toate acestea, colaborarea IS presupune ca interacțiunea dintre aplicațiile partenerilor să fie cât mai fluidă posibil (chiar dacă acestea sunt furnizate de IS eterogene). Este esențial ca IS să fie capabil să gestioneze accesul extern la acele aplicații (şi drepturile conexe). Soluții tehnice, cum ar fi EAI (Enterprise Application Integration) sau ESB (Enterprise Service Business) oferă suport concret către interoperabilitatea acestor servicii şi aplicații;
- **orchestrarea proceselor:** procesele pot fi văzute ca o "partitură muzicală" acompaniată de sistemul informatic (şi de sistemul de management al fluxului de lucru) prin gestionarea datelor şi apelurilor de servicii sau de aplicații. Într-un context de colaborare, execuția proceselor colective cu impact asupra tuturor partenerilor, trebuie să fie transparente şi ar trebui să influențeze derularea proceselor interne (în IS dintre parteneri). De aceea, procesele de colaborare trebuie să includă componente provenind din procesele private ale partenerilor asociați. Aceste procese private ar trebui protejate împotriva unei lecturări externe neautorizate, dar ele ar trebui să ofere de asemenea şi un acces parțial:
  - cel puțin la definițiile aplicațiilor pe care le oferă;
  - la datele de care au nevoie;
  - la informațiile pe care le trimit.

Aceasta este prețul contruirii unor procese colaborative.

În plus, dacă colaborarea între sistemele informatice poate fi formalizată prin utilizarea celor trei nivele "beton" (de date, aplicații şi procese), există, de asemenea, mai multe componente secundare din acest punct de vedere: interacțiuni între diferite niveluri (aplicații care pot utiliza, modifica datele; procesele aplicații de transmitere de date, etc):

- **cunoaşterea proprie şi compartimentarea conceptuală:** discontinuitatea temporală şi fracționarea colaborării implică faptul că potențialii parteneri îşi cunosc perfect propriul sistem informatic. Într-adevăr, este necesar să se definească eficient formatele de date schimbate, modurile de acces şi de utilizare a aplicațiilor. De asemenea părțile private şi publice ale fiecărui partener ar trebui să fie definite. În cele din urmă, componentele unuia din sistemele informatice aparținând unui partener pot fi pregătite pentru a fi compartimentate în scopul de a face legătura cu o posibilă implicare a unei întreprinderi / organizații în câteva rețele de comunicație distincte, în diferite momente şi pentru diferite intervale de timp.
- **flexibilitatea şi siguranța unui IS:** după cum am menționat în ipotezele cu privire la diverse întreprinderi / organizații care aparțin unei structuri de rețea, sistemele informatice trebuie să fie extrem de flexibile. Pentru a răspunde noului, sau cererilor de colaborare neaşteptate şi / sau inovative, conceptul de colaborare trebuie cu precădere să posede aceste cerințe. De asemenea, integrabilitatea sau gestionarea evoluțiilor şi schimbărilor unei colaborări în funcțiune reprezintă probleme fundamentale de substanță în acest caz. Diversitatea tipurilor de colaborare (instituționale, regulate sau sporadice) implică o nevoie crescândă de sisteme informatice (IS) sigure şi securizate în timpul adaptării acestora către astfel de deschideri (acesta este prețul care trebuie plătit pentru a fi un partener de încredere).
- **robustețea proceselor:** al treilea nivel de colaborare (cf. § 2.1) se caracterizează prin stabilirea *unui comportament de colaborare*. Acest principiu se bazează pe unul sau mai multe procese de colaborare, care definesc partea dinamică a colaborării şi certifică faptul că partenerii împărtăşesc aceeaşi viziune a comportamentului colectiv al rețelei. Procesul de colaborare (sau un model al acestui proces) este un punct-cheie al colaborării. Acesta trebuie să fie de încredere (fără a fi neapărat stabil din cauza constrângerii de

flexibilitate) la care se mai adaugă şi un punct de referinţă pentru parteneriat. Prin urmare, pare a fi legitim să se considere că construirea unui astfel de proces de colaborare ar trebui să fie completată cu activităţi de gestionare a riscurilor şi de îmbunătăţire a robusteţei.

2.2 Conceptul – Sistem Informatic Colaborativ (Collaborative Information System - CIS)

În legătură cu conversia datelor dintre parteneri, gestionarea aplicaţiilor din reţea precum şi cu dirijarea proceselor în funcţie de comportamentul global al colaborării se evidenţiază necesitatea unei:

- aderări la câteva dintre componentele şi caracteristicile unui sistem informatic al partenerilor;
- entităţi intermediare disponibilă şi independentă. Acest mediator ar trebui să gestioneze aspectele specifice ale fiecărui partener precum şi convenţiile structurale şi funcţionale specifice colaborării. Denumim o astfel de entitate suport de interoperabilitate, Sistem Informatic Colaborativ - Collaborative Information System (CIS):

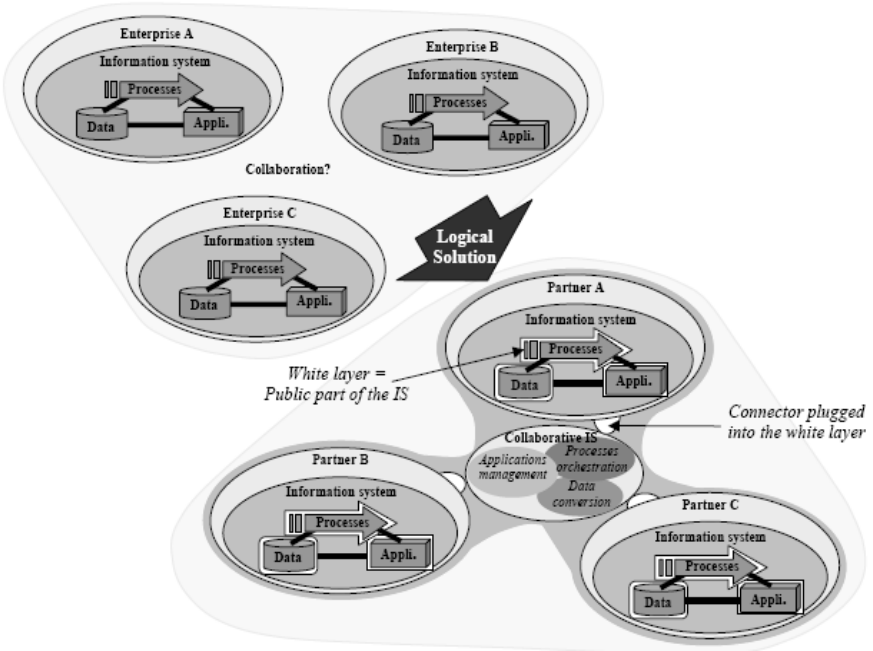

Figura 7. O propunere în plan logic pentru o colaborare de sisterm informatic

Acest CIS se bazează pe conectori ataşati la sistemele informatice ale partenerilor capabili să preia funcţiile părţilor publice şi private. Aceşti conectori pot accesa aplicaţiile publice de date şi procesele partenerilor pentru a oferi informaţiile necesare CIS ului (drepturi de acces şi alte caracteristici specifice pentru a fi gestionate la acest nivel). Mulţumită acestor module (conectori) CIS poate efectua colaborarea: prin conducerea şi controlul proceselor colaborative, prin gestionarea apelurilor de cereri de aplicaţii din partea partenerilor şi prin realizarea şi traducerea datelor de la un partener la altul (atunci când este necesar şi legitim în conformitate cu procesele globale).

În ceea ce priveşte noţiunile public / privat, vizibilitate şi acces la procese, aplicaţiile şi datele sistemelor informatice ale partenerilor provin din punerea în practică a convenţiilor colective prestabilite (conectori şi controlul CIS, deciziile convenţionale luate de comunitatea de parteneri implicaţi în reţea). În conformitate cu acest punct de vedere, procesele interne pot fi private, publice sau semi-private (în cazul în care doar o parte a unui proces este vizibil, de exemplu, intrările şi ieşirile unui serviciu), aplicaţiile pot fi private, publice sau controlate (dacă accesul este restricţionat), iar datele pot fi private sau publice.

2.2.1 Elemente care definesc un CIS

Bazându-ne pe delimitarea anterioară a conceptului de CIS, privită ca definţie de bază a conceptului de colaborare, se pot solicita în mod rezonabil elemente de conţinut ale unui astfel de sistem şi astfel, să ne întrebăm:

- Care cunoştinţe ar trebui să fie disponibile pentru a defini acest CIS?
- Ce caracteristici concrete ale reţelei şi partenerilor ar trebui să fie puse în comun pentru a proiecta acest CIS?

Morley, în [9], presupune că numeroşi actori concentraţi pe rolul esenţial al conceptului de informaţii în domeniul IS, care reprezintă în zilele noastre o abordare standard de referinţă, sunt orientaţi pe conceptul de proces. [13] subliniază că un sistem informatic inter-organizaţional are funcţia specifică de a sprijini procesele pentru a trece de/prin graniţele organizaţiei. În plus, Vernadat [12] defineşte un proces ca un set de paşi parţial clasat, executat în scopul de a obţine cel puţin un singur obiectiv. Astfel, de la sisteme simple de gestionare a informaţiilor, sistemele informatice devin sisteme de conducere care se ocupă de activităţi de informare (datorită în special instrumentelor de lucru furnizate de managentul fluxului de lucru). Conform acestor idei, putem deduce că definirea şi proiectarea unui astfel de CIS poate fi bazată pe modelarea proceselor tehnologice specifice inter-organizaţionale implicate într-un singură colaborare, cât mai precis posibil.

Modelarea proceselor este un subiect clasic (cf. [14]) şi Touzi [1] propune utilizarea limbajului BPMN (Business Process Modeling Notation) pentru a descrie procesele de colaborare specifice. În plus, Touzi sugerează folosirea UML (Unified Modeling Language) pentru a modela un CIS.

Touzi concluzionează ca principiu general pentru abordarea noastră că ştim să construim un model UML (al unui sistem de informare colaborativ adecvat) folosind cunoştinţele unui model global (despre o anumită colaborare) conţinute în modelele BPMN.

Figura 8. Principalului obiectiv

Pentru proiectarea unui CIS propunem următoarea abordare pornind de la utilizarea limbajului BPMN şi cu ajutorul UML, în patru paşi:

- **pasul 1:** traducătorul extrage din diagrama BPMN informaţii care descriu reţeaua de întreprinderi luate în considerare;
- **pasul 2:** acea informaţie este injectată în arhitectura logică special aleasă pentru CIS (în funcţie de cultura traducătorului);
- **pasul 3:** rezultatul obţinut este îmbogăţit cu cunoştinţe complementare din domeniul de modelare al întreprinderi (model specific al partenerilor şi al reţelei în sine). Acest pas implică intervenţia umană. [14] propune utilizarea conceptului de agent pentru o astfel de sarcină de îmbogăţire;
- **pasul 4:** în cele din urmă, modelul logic obţinut este proiectat pe arhitectura tehnologică aleasă cu scopul de a oferi un model UML exploatabil. Aceste etape sunt identificate în mod oficial pentru a clarifica metoda. De fapt, nu se disting atât de bine în punerea reală în aplicare. Paşii 1, 2 şi 3 sunt, de fapt, o scenă globală unică dedicată modelării logice (de exemplu, ar putea fi un ciclu iterativ care implică trei etape aproape simultan).

3. Securitatea

În economia globalizată schimbările recente din piață au condus la constituirea întreprinderilor care-şi depăşesc propriile frontiere, în aşa fel încât partenerii economici sunt consideraţi ca membri ai unei aceleiaşi organizaţii: ceea ce face ca organizaţiile să fie asimilate unei întreprinderi virtuale, unei întreprinderi extinse sau unei extinderi a strategiilor de alianţă bazate pe tehnologii. Această tendinţă este susţinută de dezvoltarea tehnologiilor bazate pe web ceea ce conduce la un sistem mondial de informare, în care fuzionează diferiţii parteneri cu propriile sisteme informatrice.

Mai mult decât atât, aşa cum tehnologia informaţiei poate fi văzută ca un element de conducere în funcţionarea celor mai multe întreprinderi, tot aşa şi indisponibilitatea sistemului informatic poate bloca în totalitate activitatea întreprinderii. Prin urmare, sistemul informatic al unei întreprinderi este o parte importantă a patrimoniului acesteia. Datorită acestei „deschideri" cerinţele de securitate trebuie să fie luate în considerare concomitent cu proiectarea proceselor de afaceri şi cu implementarea lor fizică.

Construirea unei politici de securitate este adesea redusă la implementarea unei „infrastructuri sigure". Acest punct de vedere redus oferă un răspuns tehnic la ameninţările şi vulnerabilităţile tehnice identificate. În acest context, trebuie luată în considerare vulnerabilitatea de nivel organizaţional. În conformitate cu acest punct de vedere mai mult global, accentul este pus pe sistemul informatic care urmează să fie securizat şi nu pe infrastructură.

Deoarece sistemele infomatice ale întreprinderilor sunt mai mult sau mai puţin interconectate la EDI, eBusiness sau la alte instrumente, politica de securitate trebuie să includă un proces de certificare la nivel mondial; în felul acesta se pot construi sisteme globale de securitate sigure. Pentru acest deziderat s-au definit şi proiectat standarde şi metode încă din anii 80 care urmăresc un nivel internaţional de certificare. Astfel, se pot construi sistemele globale de siguranţă.

Sistemul informatic cuprinde elemente atât tangibile (servere, dispozitive fizice, PC ...) cât şi necorporale (conţinutul sistemului informatic, procese), care se constituie în părţi ale patrimoniului întreprinderii şi care necesită măsuri de protecţie speciale care trebuie să fie stabilite. O protecţie "fizică"poate fi realizată pentru a proteja un echipament fizic în timp ce "serviciile de securitate" trebuie să fie definite pentru a proteja partea intangibilă:

- **confidenţialitatea informaţiei:** de exemplu, accesul trebuie să fie limitat doar la utilizatorii autorizaţi (atât pentru actorii interni cât şi pentru cei externi);
- **integritatea informaţiei:** de exemplu, conţinutul de protecţie împotriva modificărilor rău intenţionate ale informaţiei.;
- disponibilitatea sistemului informatic.

Pentru a sprijini aceste servicii la nivel înalt sunt necesare servicii suplimentare care trebuie să fie definite ca controale de acces, care sunt folosite pentru a identifica în mod "sigur", utilizatori, precum şi servicii non repudiere.

Adăugarea caracteristicilor de securitate acestor cerinţe presupune adăugarea unor componente speciale (hardware şi software). Pentru a defini o organizaţie de securitate corespunzătoare, costurile suplimentare implicate de infrastructură trebuie să fie comparabile cu costurile nelegate de securitate, calculate în conformitate atât cu nivelul riscurilor (în funcţie de vulnerabilităţi şi ameninţări), precum şi cu costurile implicate de atacurile de succes. Din punct de vedere tehnic, politica de securitate implică două mize majore:

- **securitatea de comunicaţie în reţea:** aceasta se referă atât la securitatea Intranet (acces redus persoanelor autorizate) cât şi la reţeaua publică de comunicaţie;
- **sistem de securitate a informaţiei**: protecţia informaţiei se sprijină pe intregralitate, confidenţialitate, acces securizat.

3.1 Proiectarea unei arhitecturi de securitate

Pentru a asigura o tranziție de la politica de securitate de tip organizațional la organizarea unei infrastructuri globale care să se potrivească cu aceste cerințe, CISCO propune abordarea *Safe* [12]. În mod uzual, între metodele utilizate la proiectarea unei rețele de securitate se construişte o arhitectură modulară începând cu „inima" sistemului informațional către părțile externe şi această arhitectură este compusă din: servere, sistem de management, rețelele campus, conexiunile externe (e-business, Internet, WAN), furnizorii de acces în sistem (internet sau furnizorii de rețele de telefonie).

Această metodă este în cea mai mare parte concepută având ca bază de plecare conceptul de infrastructură a unei rețele. În consecință, descrierea unei organizații de business este orientată spre a defini din punct de vedere logic sub-rețelele acelei organizații. Serviciile derivate din aceste sub-rețele logice aduc laolaltă alți actori (şi computerele lor) implicați în aceleaşi procese de afaceri. Apoi, aceste sub-rețele logice sunt utilizate ca cerințe obligatorii în definirea infrastructurii fizice, acordând o atenție specială atributelor de control al accesului. Apoi, fiecare serviciu este implementat în funcție de componente organizate pe diferite niveluri (componente aplicații, sistem informatic, caracteristici de comunicare) [26]. Pentru fiecare dintre ele sunt identificate potențiale atacuri şi/sau răspunsuri din punct de vedere tehnologic (sisteme criptografice, caracteristici de *tunnelling*, adresă de filtrare, porturi de control, configurare firewall, autentificare, sisteme de detectare a intruziunilor) pentru a construi o infrastructură consistentă (fig. 9), incluzând atât inter-site-ul de comunicare cât şi componentele de securitate intranet.

Security service / Threats	Confidentiality	Integrity	Availability
Unauthorised access	1	X	X
Application attack	X	1	2
Virus or Trojan horse	X	1	2
Password attack	1	2	3
Denial of service	X	X	1
IP spoofing	1	2	3
Packet sniffer	1	X	X
Network reconnaissance	1	2	3
Trust exploitation	1	2	3
Port redirection	1	2	3

Figura 9. Serviciu de securitate

Pentru a oferi o conexiune WAN între două site-uri protejate, se poate construi o rețea privată, sau se poate utiliza rețeaua publică de telefonie sau internetul. Această ultimă soluție este mai flexibilă. Cu toate acestea, ea implică luarea în considerare a amenințărilor în ceea ce priveşte comunicarea între site-uri dar şi protejarea fiecărui site.

În ceea ce priveşte rețeaua de telefonie utilizată, confidențialitatea datelor în timpul comunicării WAN este asigurată de către operatorul de telecomunicații. În plus, numerele de apel pot fi folosite pentru autentificarea site-urilor, asigurându-se astfel un mod eficient de filtrare atât pentru apelurile primite cât şi pentru conexiuni externe. Datorită investițiilor reduse dar şi nivelului inalt de securitate furnizat de către operatorul de telefonie, o astfel de conexiune ISDN este destul de obişnuită pentru IMM-uri, în ciuda costurilor implicate care sunt destul de importante. Cu toate acestea, unele componente de tip e-business (eMarket) utilizează adesea programele cadru de tip *Business Collaborative* disponibile numai pe Internet, ceea ce implică o conexiune de bază între site-uri.

Pentru a asigura confidențialitatea informației în timpul unei astfel de sesiuni de comunicații de date se poate stabili un tunel virtual VPN [17] şi în acest fel, doar informația codificată este răspândită în rețeaua publică şi de asemenea pot fi furnizate caracteristicile de bază de autentificare datorită punerii în comun a unui secret aparținând ambelor părți (prin chei criptografice, de exemplu).

Pentru a proteja fiecare site local, se pot utiliza firewall-uri care au ca sarcină filtrarea traficului [18]. Aceste filtre pot fi cuplate la un sistem de detecție a intruderilor (IDS) care are

menirea de a controla activitatea sistemului în ansamblul său [19]. Astfel de sisteme de detecție a intruderilor au la bază analiza gestionării datelor (atât la nivel de sistem cât şi la nivel de rețea), pentru a recunoaşte profiluri ale diferitelor atacuri [16], în scopul atenuării lor. Mai mult decât atât, aceste software-uri IDS pot fi cuplate la sistemul informatic sau la sistemul de management al rețelei, astfel încât disponibilitatea resurselor să poată fi verificată în fiecare moment, iar respingerea atacurilor asupra serviciului să poată fi eficient atenuată.

În ceea ce priveşte nivelul de aplicare, trebuie avută în vedere integritatea informațiilor şi confidențialitatea. Aceste cerințe conduc atât spre controlul autentificării accesului utilizatorului, precum şi spre protecția conținutului informațiilor. Autentificarea utilizatorului se poate face prin tehnici diferite:

- **login / parolă:** Eficiența acestui mecanism este puternic legată de parola aleasă;
- **infrastructură PKI** [21]: în acest caz, certificatul care autentifică identitatea utilizatorului. Un secret comun este partajat prin cheie de criptare, astfel încât partenerii pot proteja confidențialitatea datelor. Prin utilizarea de dispozitive externe (carduri inteligente, chei USB etc.) securitatea „logică" se cuplează la controalele fizice. Mai mult decât atât, o astfel de infrastructură poate fi utilizată pentru implementarea caracteristicilor non-repudiere: prin stocarea certificatelor schimbate pot fi reconstituite părți din procese.

Arhitecturile bazate pe Kerberos [22] sunt utilizate pentru cuplu login / parolă din arhitectura de accesare a sistemelor de control: sunt folosite simboluri pentru a permite accesul utilizatorilor la date sau pentru a utiliza aplicația. Această ultimă tehnică este legată de accesul la sistemele de control. Odată ce utilizatorul este identificat, sistemele de control al accesului pot fi folosite pentru a controla confidențialitatea informațiilor. O primă protecție poate fi setată prin configurarea funcțiilor de filtrare ale firewall-urilor: de exemplu, care maşină (identificată prin adresa IP) are permisiunea să comunice (in sau out) cu resurse diferite. Acest mecanism de tip firewall oferă protecție generală pentru o anumită resursă. Pentru a proteja informațiile cu mai multă exactitate, trebuie implementate sisteme de control al accesului, cum ar fi de exemplu, Tivoli Access Manager [23] sau Access Master [24] care oferă o descriere centralizată a autorizațiilor de acces necesare pentru a adera la diferite părți ale unui sistem informatic. În ceea ce priveşte sistemele distribuite, pot fi setate sisteme de control al accesului reprodus, câte unul pentru fiecare server. Prin urmare, pentru eficiență, mecanismul de reproducere trebuie să fie setat pentru a asigura o coerență la nivel global [25].

Organizarea infrastructurii pe care o propunem pentru o întreprindere virtuală este compusă din trei părți principale [29]:

- **intranetul întreprinderii** – interconectează propriile resurse, servere şi alte dispozitive;
- **extranetul întreprinderii** – este împărțit în două arii:
  - **intranetul VE** - care se compune din interconexiunile dintre componentele securiziate ale fiecărui extranet al intreprinderii, interconexiuni care se realizează prin linii ISDN sau prin tuneluri securizate prin intermediul Internetului;
  - **extranetul întreprinderii** – este strâns legat de internet şi de conținutul nesecurizat al informațiilor disponibile în mediu.

Fiecare intranet este securizat în diverse moduri:

- **fiecare intranet este ascuns** - datorită traducerii adresei. În acest mod, fiecare resursă nu poate fi văzută, sau administrată din exterior. Fiecare router (sau fiecare port de routere), care se interconectează la diferite rețele, implementează controale de acces în funcție de adresa maşinii, astfel încât o parte a rețelei proprii întreprinderii să nu poată fi accesată din exterior;
- **firewalls** – implementeză caracteristici de control al accesului şi servicii de autentificare atît prin intermediul numărului de apel de indentificare ISDN cât şi prin

management-ul PKI, filtrarea traficului, detecţia intruşilor;

- **servere proxy** - serverele sunt utilizate ca interfeţe între diferite reţele: informaţiile solicitate şi/sau transmise mediului întreprinderii sunt copiate mai întâi la proxy, filtrate de un software antivirus şi trimise către staţia de lucru care cere aceste informaţii. Transferul de informaţii către serverele proxy este supus politicii de implementare a controlului accesului la informaţii prin intermediul PKI sau prin login;

Desigur, după ce au fost îndeplinite cerinţelele de securitate ale IS, în fişierele .log sunt reţinute autentificarea, controlul accesului, procesele salvate care reprezintă un volum mare de activitate raportată. Din punct de vedere tehnic se pot utiliza diferite modele de securitate, astfel încât să se asigure securitatea atât a IS (Information System) cât şi a BP (Business Proccess). Pe baza caracteristicilor de securitate necesare care oferă rapoarte de activitate prin fişierele jurnal ale fluxului de lucru sau prin sistemele de raportare a fluxului de activităţi se poate reconstrui execuţia proceselor de business.Deoarece această activitate de raportare poate fi legată de valoarea adăugată a procesului în sine, se pot creea probleme în ceea ce priveşte protecţia datelor.

3.2. Securitatea vs. datele cu caracter personal

Datele cu caracter personal se definesc ca fiind acele informaţii strâns legate de identitatea personală. În zilele noastre, la locul de muncă când lucrăm cu software dedicat, sau când navigăm cu ajutorul browserelor prin Internet se pot înregistra informaţii de identificare cu caracter personal de către terţe persoane:

- mesaje de autentificare cu PKI care pot fi colectate şi puse în legătură cu contracte de schimb, astfel încât procesele de bază ale fluxului de lucru să poată fi parţial reconstruite de către partenerii celeilalte întreprinderi;
- informaţii de identificare (adresă de conectare, IP, numele calculatorului ...) sunt schimbate în timpul navigării pe Web. Mai mult decât atât, cookie-uri pot fi folosite pentru a raporta activitatea pe anumite servere;
- servere proxy folosite pentru a îmbunătăţi atât securitatea sistemului cât şi comunicarea, QoS înregistrează toate paginile web vizitate;
- sisteme de control al accesului la date care pot raporta atât informaţii de identificare 5t şi copii ale fişierului care conţine modificările operate.

Toate aceste procese „cyber-control" sunt concepute pentru a proteja sistemul informatic împotriva intruderilor (filtrare pe nume, adrese IP ...), pentru a oferi o siguranţă generală faţă de căderile sistemului sau utilizările în mod abuziv (în acest scop, fişierele jurnal şi fişierele de salvare a proceselor pot fi cuplate pentru a reconstrui părţi din procesele întrerupte), pentru a implementa controale asupra proceselor dematerializate (autentificare şi procese nerespinse). Unele practici/obiceiuri ale utilizatorilor, ca schimbul de cont de e-mail, pot conduce la violarea datelor private: în acest mod un proces poate „continua" chiar dacă unul dintre actori nu este prezent (ex: protecţia e-mailului) iar intimitatea este lezată. Protecţia datelor private trebuie să fie luată în considerare atât pentru colecţii de date (utilizatorii trebuie să fie conştienţi asupra informaţiilor cu caracter personal colectate) precum şi pentru prelucrarea datelor cu caracter personal (intern şi extern). Mai mult decât atât, trebuie asigurate caracteristici de securitate particulare pentru a oferi o siguranţă suficientă şi un nivel de securitate pentru aceste date cu caracter personal.

Pentru a oferi un nivel acceptabil de protecţie asupra confidenţialităţii datelor, ţările stabilesc strategii diferite. Astfel în timp ce în Statele Unite [28] este promovată o piaţă de auto-reglementare, în CEE este folosită protecţia juridică CEE, atât pentru utilizarea privată cât şi pentru utilizarea "profesională" a informaţiilor şi tehnologiilor de comunicare. Cât priveşte protecţia vieţii private trebuie să se înţeleagă în întreaga lume, că aceasta este asigurată prin acoduri speciale stabilite între părţile străine cu scopul de a face schimb de date cu caracter

personal, ca principiu de bază al sferei de siguranță.

În ciuda acestor diferențe „legale", practicile „echitabile" sunt definite pe baza aceloraşi principii:

- **transparență:** utilizatorii trebuie să fie conştienți de colectarea datelor cu caracter personal şi de prelucrarea lor;
- **necesitate:** Cyber-controlul trebuie să fie utilizat ca o completare a altor instrumente de securitate;
- **echitate:** scopul prelucrării datelor cu caracter personal trebuie să fie recunoscut;
- **proporționalitate:** nivelul de cyber-control trebuie să se potrivească cu riscurile.

Prin urmare procesele în cruce privind datele cu caracter personal trebuie să fie limitate şi să implice acorduri speciale ale instituțiilor de reglementare din diferite țări. Pentru a acorda atenție acestor constrângeri, organizarea de bază a fluxului de lucru prezentat anterior nu poate fi aplicată în mod direct. Pentru a rezolva problema de confidențialitate se propune adaptarea unui control de autentificare în sensul de a oferi un "o cheie de identificare pentru o singură utilizare". În acest scop se alege o arhitectură similară celei de tip Kerberos în care Key Manager (KM) gestionează utilizatorii şi drepturile de acces ale aplicațiilor. Apoi, utilizatorii emit o cerere pentru cardurile de certificare (*token)* de la KM pentru a realiza anumite sarcini. Aceste token-uri sunt stocate în sistemul de raportare a fluxului de lucru. Cu toate acestea, un număr limitat de analize încrucişate ale KM şi ale fişierelor raport ale fluxului de lucru pot oferi informații privind autentificarea şi nonautentificarea.

4. Software pentru rețele de comunicație

FaceTime Communications (www.facetime.com), pionierii în utilizarea productivă şi în siguranță a comunicațiilor unificate şi a Web 2.0 au introdus o soluție de management de securitate şi conformitate pentru rețelele sociale numită *Socialité*. Socialité oferă un control granular al unor aplicații precum Facebook, LinkedIn şi Twitter şi este disponibil ca software, drept serviciu de implementare (SaaS) sau ca soluție-premisă ca un modul al gateway-ului de securitate FaceTime. Socialité este, de asemenea, prima soluție care poate fi implementată ca o soluție hibrid pentru a oferi posibilitatea de a defini o politică de rețea şi o politică de roaming pentru oamenii din afara rețelei. Acum organizațiile pot oferi controlul asupra caracteristicilor şi comunicațiilor media-sociale atât pentru utilizatorii dintr-o rețea corporatistă cât şi pentru cei situați la distanță.

Aplicațiile media de socializare utilizate la locul de muncă au devenit un lucru obişnuit pentru angajații din toate departamentele şi tinde să se dezvolte pentru canale suplimentare în vederea extinderii lor pentru alte categorii de oameni cum ar fi: clienți, parteneri, prospecți, furnizori etc. De fapt, din 2010 Annual Collaborative Internet Survey, sponsorizat de FaceTime, relevă că 61% dintre lucrători utilizează rețelele sociale zi de zi în rețeaua corporației. Facebook, LinkedIn şi Twitter au devenit deosebit de populare din cauza eficienței lor în contactarea prospecților, vizualizarea candidaților pentru diverse locuri de muncă, a promovării evenimentelor şi pentru extinderea comunicațiilor de afaceri. Cu toate acestea, utilizarea acestor rețele de socializare de către vânzători, de căte serviciul de marketing, cel de resurse umane şi de către alte departamente presupune noi cerințe din partea organizațiilor, pentru a satisface solicitările de securitate, management şi conformitate în această situație.

Schimbările recente de reglementări, stipulate în publicații cum ar fi Financial Industry Regulatory Advisory (FINRA) sau Regulatory Notice 10-06, reprezintă ghiduri de îndrumare în această problemă pentru securizarea comunicațiilor firmelor şi brokerilor cu publicul prin intermediul site-urilor de rețele sociale.

Cu *Socialité*, clienții beneficiază de un set extins de funcții pentru mai mult de 1.000 de rețele de socializare în scopul asigurării conformității cu o varietate de reguli şi reglementări. În Facebook, LinkedIn şi Twitter, cele trei rețele de socializare esențiale, *Socialité* permite un control pentru 95 de activități distincte şi caracteristici de conținut. *Socialié* poate, de asemenea

modera şi arhiva conținut partajat pe Facebook, LinkedIn şi Twitter pentru a se asigura că numai conținutul pre-aprobat este împărtăşit şi celorlați participanți.

5. Concluzii

Cooperarea implică o comunicare şi un anumit tip de coordonare. Din aceste două elemente rezultă dezvoltarea unei noi paradigme a activităților de colaborare. [6]

Colaborarea poate avea succes dacă toți membrii participanți arată bunăvoință şi responsabilitate. Colaborarea este necesară pentru a face față la proiecte mari. Caracterul colaborativ este social, esențial pentru munca ce trebuie să fie apreciată în întreprinderile interactive de proiectare a sistemelor.

Dezvoltarea de sisteme colaborative conduce la creşterea complexității lor şi caracterul global al economiei este proiectat pentru a determina de asemenea un caracter global pentru cele mai multe dintre sistemele colaborative. Din punct de vedere al infomației acestor sisteme globale de colaborare trebuie să le corespundă indicatori globali de performanță, procedurilor de conversie de date, şi trebuie definite matricile sistemelor colaborative. Pe baza acestor indicatori de agregare ar trebui să decidă adecvat nivelul global, nivelul intermediar şi nivelul de execuție a oricărui sistem colaborativ organizat pe niveluri ierarhice.

Un sistem colaborativ creează un mediu în care oamenii pot lucra mai bine împreună, pot partaja informații fără constrângerile de timp şi spațiu, deoarece acesta este caracterizat prin trei aspecte fundamentale: activități comune, schimbul de mediu şi modul de interacțiune.

Pentru a face față constrângerilor C-Business (a se citi collaborative business), întreprinderile / firmele trebuie să ia în considerare cerințele de securitate în timp ce-şi reproiectează procesele de afaceri şi sistemele de informații. Tehnologiile care au la bază Internet-ul oferă un suport simplu de schimb de date. Cu toate acestea, amenințările de pe internet aduc constrângeri consistente în ceea ce priveşte proiectarea infrastructurilor. Mai mult decât atât, amenințările la adresa organizațiilor legate de deschiderea infrastructurii presupun definirea cu precizie a profilurilor de colaborare pentru ca un BP (business proccess) să poate fi adaptat cu uşurință atât pentru utilizare internă cât şi pentru cea externă.

BIBLIOGRAFIE

1. **CIUREA, C.:** A Metrics Approach for Collaborative Systems, ASE.
2. **BENABEN, F.; TOUZI, J.; RAJSIRI, V.; PINGUAD, H.:** Collaborative Information System Design. Centre de Genie Industriel.
3. **IVAN, I.; CIUREA**., **C.:** Using Very Large Volume Data Sets for Collaborative Sys-tems Study. Informatica Economică Journal [Online] http://revistaie.ase.ro/content/49/003%20-%20Ivan, %20Ciurea.pdf
4. **IVAN, I.; CIUREA, C.:** Quality characteristics of collaborative systems. În Proc., The Second Interna-tional Conferences on Advances in Computer-Human Interactions, vol. I, Cancun, Mexico, 2009, pp. 164-168.
5. **SILAGHI, G. C.:** Collaborative Multi-Agent Systems - Conception, design and development. Cluj-Napoca: Risoprint Publishing House, 2005.
6. **NIȚCHI, Ş.; NIȚCHI, R.; MIHĂILĂ, A.:** Some Remarks on Collaborative Systems Framework. Informatica Economică Journal, http://revistaie.ase.ro/content/43/20-nitchi.pdf
7. ISO Standards for Interoperability: a Comparison proceedings of INTEROP-ESA'05, Kosanke, K, Geneva, Swiss, February 21-25 2005, Springer-Verlag; pp. 55-64.
8. **BERNUS, P.; SCHMIDT, G.:** Architectures of information systems. Springer Verlag, 1998.
9. **MORLEY, C:** La modélisation des processus : typologie et proposition utilisant UML.

Actes des journées ADELI : processus et systèmes d'information, Paris, France, 2002.

10. **LAURAS, M.; PARROD, N.; TELLE, O.:** Proposition de référentiel pour la notion d'entente industrielle: trois approches dans le domaine de la gestion des chaînes logistiques. Revue Française de Génie Industrie l, 2003, vol. 22, nr. 4, pp. 5-29.
11. **REIX, R.:** Systèmes d'information et management des organisations, 4th éd., Vuibert 2002.
12. **VERNADAT, F.:** Techniques de modélisation en entreprise: application aux processus opérationnels. Edition Economica, 1999.
13. **AUBERT, B.; DUSSART, A.:** Systèmes d'Information Inter-Organisationnels. Rapport Bourgogne: march 2002, CIRANO.
14. **BERTHIER, D.; MORLEY, C.; MAURICE-DEMOURIOUX, M.:** Enrichissement de la modélisation des processus métiers par le paradigme des systèmes multi-agents: Revue Systèmes d'information, 2005, vol. 10, no. 3, pp. 25-45.
15. **TOUZI, J.; BÉNABEN, F.; PINGAUD, H.:** Une approche de la conception d'un système d'information d'entreprise par la représentation des processus. GDR MACS Congress groupe de travail ECI, Paris, France, March 2005.
16. **VERWOERD, T., HUNT, R.:** Intrusion detection techniques and approaches. Computer Communications, 25, 2002, pp. 1356–1365.
17. Safe VPN: IPSec Virtual Private Networks in depth, CISCO Corp., Cisco, 2001 White paper avialable at http://www.cisco.com/application/pdf/en/us/guest/netsol/ns128/c654/cdccont_0900aecd800b05ad.pdf.
18. **HUNT, R.:** Internet/intranet firewall security – Policy, architecture and transaction services. Computer Communications, 21, 1998. pp. 1107–1123.
19. **MC HUGH, J.; CHRISTIE, A.; ALLEN, J.:** Defending yourself: the role of intrusion detection systems. IEEE Software, September/October 2000, 2000, pp. 42–51.
20. **HUNT, R.:** Technological infrastructure for PKI and digital certification. Computer Communication, 24, 2001, pp. 1460–1471.
21. **NEUMAN, B. C.; TS'O, T.:** Kerberos: An Authentication Service for Computer Networks., IEEE Commnication, September 1994, 32, 9, 1994, pp. 33–38.
22. IBM Tivoli Access Manager for e-business, IBM Corp., 2003. Available at http://www.redbooks.ibm.com/redpapers/pdfs/redp3677.pdf
23. Access Master SSO – Technical overview, Evidian Corp., 2001. Available at http://www.evidian.com/evifiles/edocs/SSOTechnicalOverview.pdf
24. **SAMARATI, P., AMMANN, P., JAJODIA, S.:** Maintaining replicated authorizations in distributed database systems. Data & Knowledge Engineering, February 1996, pp. 55–84.
25. **LEVITIN, A. V.; REDMAN, T. C.; SLOAN:** Data as a resource: properties, implications and prescriptions, Management Review, fall 1998, 1998, pp. 89–101.
26. SAFE: A Security Blueprint for Enterprise Networks, CISCO Corp, 2000 White paper avilable at http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safe_wp.htm
27. Privacy online: a report to congress, FTC (Federal Trade Commission), 1998. Report. Available at http://www.ftc.gov/reports/privacy3/priv-23.htm
28. **BIENNIER, F., FAVREL, J.:** Secure collaborative information system for enterprise alliances: a workflow based approach. ETFA'01 Proceedings, 2, 2001, pp. 33–41.
29. **FISHER-HÜBNER, S.:** IT-security and privacy. Lecture Notes in Computer Science, 1958, 2001, pp. 35-106.