GENERAL INFORMATION ON THE IMPERATIVE, EVOLUTION AND CONCORDANCE OF THE MEANS AND METHODS OF PROTECTING ECONOMIC INFORMATION AND INFORMATION RESOURCES

GENERALITĂȚI PRIVIND IMPERATIVUL, EVOLUȚIA ȘI CONCORDANȚA MIJLOACELOR ȘI METODELOR DE PROTEJARE A RESURSELOR INFORMAȚIONALE ȘI INFORMATICE ECONOMICE

Leahu Tudor
Doctor în științe economice, conferențiar universitar
Universitatea Liberă Internațională din Moldova
e-mail: leahu.ts@mail.ru

Abstract
The imperative factors are elucidated, characterized the circumstances and environments of current and future economic information and informatics systems, which objectively contributed to the urgent need for invention, elaboration and using of various means and methods of protection of information resources. The functional value of the field in question in the market economy environment and in integrated informatics systems is emphasized. The content of the material is structured and rendered from the positions of the unitary process of economic management, which performs not only information, but also and the materials activities, in interconnection and direct interaction in real time. Its subdivisions are also specified and in this basis - determined the field of application of the above-mentioned means and methods in the existing conditions of processing the informational values of economic content.
In this context, the subdivisions of the previously nominated process, its constituents, are systematized and analyzed. The general scheme of the interconnection and interaction between the parameters of protection and efficiency of the functioning of economic integrated informatics systems is established and elaborated. Depending on the application environments, the categories of protection of information units, physically made in the form of data elements, on manual and informatics storage media are highlighted. At the same time, in terms of mutual influence with information resources, some aspects of the protection of other informatics resources are elucidated. Tangentially, the terminology is examined and the concordance of the means and methods of organizing and carrying the data protection processes is performed. The problems of this department of economic informatics and the possible ways to solve them are formulated.

Keywords: *categories, concordance, data protection means and methods, explanation terminology, imperative factors, integrated economic informatics systems, problems, systematization, ways to solve*

JEL Classification: *C55, D85, E47, L63, L86*

INTRODUCERE

Anticipat oricăror activități de cercetări sau de asigurare a evoluției lor în direcția anterior bine determinată, obiectiv se impune formularea, cunoașterea și aplicarea exactă a anumitor termeni specifici pentru domeniul concret al utilizării lor. Neglijarea acestei teze face imposibile inițierea, elaborarea, implementarea și funcționarea cotidiană a obiectului (procesului) gestionat.

În acest sens, și procesele de protejare a resurselor informatice au solicitat și permanent au înaintat cerințe tot mai stringente față de realizarea procedurilor, operațiunilor de prelucrare și păstrare a componenței, structurii și conținutului (valorilor) unităților de resurse anterior nominalizate. De constatat faptul că pentru a satisface și respecta aceste exigențe primordial apare necesitatea în formarea anumitei terminologii concordante cu compoziția, configurația și logica evoluției ariei de aplicare. De aceea, pornind de la complexitatea componenței resurselor, se cer elaborate și aplicate noțiuni referitoare la toată sfera de preocupări informatice, sector, sub-sector, compartiment,

resursă şi componentă constituantă a lor. În conformitate cu astfel de deziderat, pot fi evidenţiaţi termeni de ordin general, intermediar şi particular.

În contextul celor expuse până aici, raportat la protecţia sistemelor informaţionale şi informatice economice, se observă un număr relativ sporit de termeni, uneori cu conţinut contradictoriu, fără orientare spre mediul real ce a provocat formularea şi întrebuinţarea lor. Din motivul dat, atât pentru teoria, cât şi pentru practica elaborării şi funcţionării sistemelor în cauză, de importanţa deosebită dispune clarificarea esenţei şi conţinutului funcţional al unor termeni de bază referitor la acest domeniu.

CONŢINUTUL CERCETĂRII

În sursele bibliografice [1-4] şi activităţile practice de asigurare a protecţiei datelor cele mai frecvent utilizate sunt noţiunile „fiabilitate", „securitate", „protecţie", „confidenţialitate", „integritate", „risc (pericol)". Deşi fiecare din ele dispun de un anumit grad de sinonimitate, nu toate pot ft utilizate în măsură egală pentru un element ori altul al sistemului informaţional (informatic). Aşa, de exemplu, „securitatea" se interpretează drept minimalizare a vulnerabilităţii elementelor sistemului, iar „pericolul" - drept încălcare potenţiala a securităţii. Odată cu majorarea performanţei sistemelor de procesare a datelor, devine tot mai evidenta valoarea pericolelor neintenţionate şi intenţionate.

Cea mai vastă se considera noţiunea de „protecţie", care se referă la orice resursă a sistemului informatic. De aceea, privind resursele informaţionale, ea include în sine asigurarea confidenţialităţii datelor, protejarea informaţiei de modificări şi falsificări, de lichidare (ştergere) a ei şi excluderea „acaparării" resurselor sistemului cu stăpânirea lor monopolistă „Protecţia informaţională" se referă la tot sistemul de organizare, transformare şi utilizare a datelor şi la fiecare componentă (resursă, activitate) a lui în particular. De aceea în fiecare caz aparte ea se determină divers, în dependenţă de obiectele şi acţiunile, pentru care ea trebuie să fie asigurată.

De asemenea, „protecţia informaţională" include o totalitate de acţiuni, metode şi mijloace ce asigură soluţionarea a aşa probleme principale ca verificarea integrităţii informaţiilor; excluderea accesului neautorizat la resursele calculatoarelor, la programele şi datele informaţionale, excluderea utilizării neautorizate a programelor (protecţie de copiere a programelor).

Fiabilitatea caracterizează gradul de siguranţă a unui sistem ori componentă a lui în conformitate cu scopul conceput şi realizat; capacitatea funcţionării lui timp cât mai îndelungat. De aceea, noţiunea se referă mai mult la partea fizică (materială) a sistemului, măcar că la nivel general ea poate fi utilizată şi în sens de trăinicie, temeinicie, siguranţă şi chiar securitate a oricărui element al sistemului.

În acelaşi timp, „confidenţialitatea" are atribuţie mai cu seamă la sensul conţinutului resurselor informaţionale şi constă în asigurarea nedestăinuirii conţinutului, componenţei, numărului, structurilor şi valorilor unităţilor informaţionale.

De asemenea, şi „integritatea" ca termen se referă preponderent la partea informaţională a sistemului. Din acest motiv esenţa ei se reduce la asigurarea deplinătăţii şi exactităţii valorilor datelor prin excluderea modificării lor ocazionale sau intenţionate, anularea lor prin ştergere.

După cum a fost afirmat anterior, protecţia se raportează la orice resursă a sistemelor informatice şi de aceea termenul se consideră de cel mai general nivel, din ce cauză este justificată includerea parametrilor ce contribuie la realizarea ei. În aşa aspect, în dependenţă de categoria resurselor şi scopul protejării lor, termenul elucidat înglobează noţiunile de fiabilitate şi securitate. Deci, prin intermediul asigurării unui anumit grad de fiabilitate şi securitate, se atinge o anumită eficacitate a funcţionării sistemului. În această

bază, interconexiunea și concordanța dintre noțiunile parametrilor elucidați ai sistemelor nominalizate schematic poate fi prezentată prin interrnediul figurii 1.

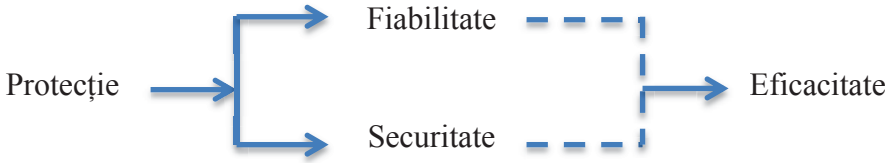

Figura 1. Schema interconexiunii și concordanței termenilor parametrilor protecției și eficacității funcționării sistemelor informatice economice (S.Ic.E.)

De menţionat că fiabilitatea se referă, mai cu seamă, la funcţionarea resurselor S.I$_c$.E., pe când securitatea are atribuţie preponderent la existenţa („păstrarea") lor. Prin urmare, prima asigură funcţionalitatea resurselor tehnice şi tehnologice, iar cea secundă - accesul şi confidenţialitatea celorlalte resurse. Însă, orice nu s-ar efectua în acest domeniu totul este orientat spre un singur scop - asigurarea calităţii resurselor informaţionale, ceea ce şi caracterizează integral eficienţa S.I$_c$.E. Sunt cunoscute aşa date că în S.U.A. (conform afirmării şi datelor companiei C.N.N.) valoarea pierderilor de la încălcările securităţii şi neasigurării fiabilităţii S.Ic.E. au atins cifre de zeci de miliarde de dolari [1, pp.311-312; 3, pp.33-35] .

Important este şi faptul că pentru economia de piaţă este caracteristică aplicarea cât mai frecventă a principiului selectiv de aplicare a resurselor informaţionale în activităţile de gestiune. El se reduce la acel concept că varietatea selectării se găseşte în dependenţă directă de complexitatea, componenţa şi plenitudinea conţinutului acestor resurse. De aceea cu cât mai variate şi mai voluminoase sunt informaţiile păstrate pe mediul fizic memorar al mijloacelor tehnice informatice, cu atât mai operativă şi mai aleatoare este selecţia lor în orice moment oportun.

În aşa context actualmente se constată noian de informaţii economice, ceea ce fără conştientizarea necesităţii formării şi afişării nu numai a celor rezultative, dar şi a celor iniţiale, de asemenea, complică şi acutizează problemele protecţiei şi eficienţei S.I$_c$.E.

SPECIFICUL FUNCȚIONĂRII DOMENIULUI EXISTENT DE APLICARE – IMPERIOZITATE DE PROTEJARE

Situația creată la moment și premisele evoluției posibile a managementului economic tot mai impunător confirmă faptul necesității transformării lui treptate, ca unitate organizatorică, într-un nucleu material – informațional de acțiune analoagă automată. În astfel de circumstanțe nu este exclusă influența decisivă nemijlocită și temporar imediată a activităților materiale și spirituale umane de starea proceselor informaționale.. Ca urmare a formării acestei conjuncturi, protecția unităților informaționale, operațiunilor și procedurilor de manipulare cu ele va dispune de valoare gestională extremă, deoarece "alterarea" lor prompt se va răsfrânge asupra activităților în cauză. Din motivul dat, abordarea sistemică și tratarea integrată vor deveni iminente pentru orice teren managerial economic, indiferent de dimensiunile razelor spațiale și temporale existențiale și evoluționiste ale lui.

În acest context preliminar apare necesitatea stringentă în analiza nivelului integrării sistemului actual de gestiune economică și implicit a sub-sistemului lui informațional. Ambele se caracterizează prin izolare spațială și evoluția discretă a proceselor materiale și informaționale, care virtual și în interpretare analogică formează un tot întreg. De aici - : multiplele discordanțe dintre activitățile acestor două categorii de procese, fărâmițarea sistemului managerial pe nivele (organisme) de gestiune (primare,

intermediare, superioare), perioade de funcționare (operative, curente, de pronostic) și a sistemului informațional pe subsisteme, complexe de probleme și probleme particulare.

Astfel de situație a condus la efecte cât mai expresive, mai cu seamă, la nivelele intermediare și superioare de gestiune, a rolului influențabil al subiectului asupra evenimentelor materiale și spirituale atât a societății umane în ansamblu, cât și a fiecărei subdiviziuni, individ al ei. S-au creat condiții de favorizare a înrăuririi precumpănitor negative tendențioase a sistemului managerial asupra obiectului (procesului) condus, precum și la predominarea metodelor și mijloacelor administrative aplicate practic în orice spațiu și moment de gestiune. De pe poziții unitare, toate aceste momente, cu prevalență, sunt provocate de necorespunderea nivelului de performanță a sub-sistemului managerial comparativ cu sub-sistemul condus de el. Formarea rupturii menționate s-a produs odată cu instituirea caracterului social al activităților materiale umane, ea fiind consecința penuriei accentuate de informații calitative.

Analiza desfășurării cursului acestor două constituente ale procesului unitar de gestiune economică scoate în transparență mersul obiectiv spre lichidarea izolării teritoriale și funcționării discrete a lor. În prezent și de la începutul socializării activităților subiectului așa înaintare se observă și este realizată prin inventarea, elaborarea și aplicarea diverselor mijloace tehnice, programate, metode tehnologice, etc., considerate drept resurse informatice. Trasând o paralelă între progresul dezvoltării resurselor elucidate, devine sesizabil faptul că cele enumerate anterior au avansat esențial, pe când, din punct de vedere a cuprinderii totale a fenomenului informațional ca unitate integrală, aplicarea lor în domeniile informativ și decizional economice este insuficientă. În sensul dat, se atestă o acoperire satisfăcătoare de către mijloacele și metodele informatice numai a unei etape transformative a informațiilor – a etapei de prelucrare (informațională, structurală, de calcul), celelalte două etape – inițială și de utilizare rămânând efectuate preponderent în mod manual de subiect. În rezultat, s-a format o discordanță substanțială dintre nivelele performanței metodelor și mijloacelor informatice și domeniul aplicării lor. Așa situație poate fi calificată drept nepregătire a resurselor informaționale pentru implicarea resurselor nominalizate în procesarea lor.

Circumstanțele create sunt provocate de extinderea spațială și vitezele inimaginabile de realizare a preocupărilor materiale umane. Despre aceasta mărturisește formularea evolutivă a concepției globalizării activităților în cauză, obiectiv fiind împinși de imperativul integrării material – informaționale. Altfel afirmând, globalizarea materială a provocat și nu poate fi realizată și funcționa fără globalizarea informațională.

De menționat că în prezent și permanent, în procesarea datelor pe bună dreptate și justificat se consideră decisive resursele informatice, enumerate mai sus. Însă, nu mai puțin valoroasă pentru această modalitate este și adecvarea structurării și organizării resurselor informaționale, interconexiunilor procesuale și funcționale ale lor. Prin realizarea consecutivă a acestor două categorii de interconexiuni se asigură continuitatea tuturor proceselor informaționale. În cazul, în care continuitatea este susținută de mijloace și metode tehnice, ea este automată. Prin urmare, nu numai factorii informatici, dar și însăși domeniul – resursele informaționale, prin interconexiunile sale structurale raționale, de organizare și prelucrare eficientă, contribuie direct la procesarea mașinală a lor. De aceea, de importanță decisivă în spriginirea funcționării automate a sistemului integrat de management economic dispun identificarea, respectarea, punerea în funcțiune și garantarea funcționării tehnice a interconectărilor de orice varietate în cadrul sistemului.

Din cele elucidate până aici, din punct de vedere științific și proiectant, rezumă justificarea imperativului elaborării concepției unitare de creare și asigurare a funcționarii fiabile și eficiente a unui sistem informatic, care ar integra într-un tot indivizibil resursele

și procesele (materiale + informaționale) apartenente lui. Așa sistem se solicită să fie nu numai unitar în plan compozițional și structural, dar și totalmente interconectat și procesual integrat.

Pornind de la considerentele menționate, concepția sistemului informatic integrat rezidă în cuprinderea cu procese informatice nu numai a activităților informaționale, dar și materiale în interconexiune și interacțiune nemijlocită. Unitatea acestui sistem se referă atât la organizarea, cât și structurarea și funcționarea tuturor elementelor constitutive ale lui de pe poziții unitare.

Astfel de abordare impune efectuarea elaborării, implementării și asigurarea evoluției lui cotidiene prin stabilirea și realizarea tuturor constituantelor, interconectărilor și interacțiunilor dintre ele, indiferent de razele teritoriale și temporale în baza principiului motivației, conform căruia materia cauzează informația, ultima fiind de predestinație informativă și decizională.

Pe lângă cele menționate mai sus, odată cu determinarea exactă și deplină a caracteristicilor menționate, respectarea întocmai și realizarea lor prin intermediul factorului informatic, se creează condiții de constituire a unui sistem de mansagement economic de acțiune analoagă, adică, automata și nu automatizată, ceea ce este propriu pentru asemenea sisteme în present. În așa situație sistemul va funcționa conform schemei din figura 2 [4, pp.251-253].

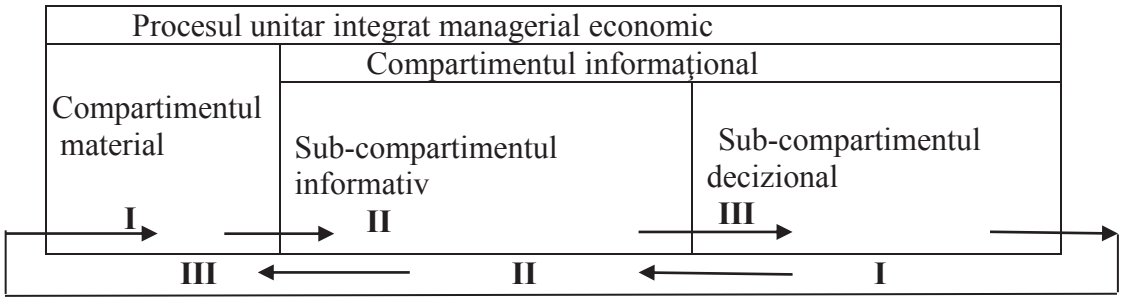

Figura 2. Schema conceptuală de funcționare a procesului unitar integrat de gestiune economică

Schema concepției succesiunii interconexiunii și interacțiunii compartimentelor și sub-compartimentelor procesului unitar integrat economic din figura 2 este bazată pe principiul motivației și pentru varianta inițierii evoluției lui. În cazul, în care procesul deja funcționează, astfel de ordine se inversează, adică deciziile formulate afectează procesele materiale, ultimele – procesele informative, iar ultimele – formularea repetată exactă, luarea autentică și realizarea eficientă a proceselor materiale, conform noilor valori decizionale, etc. până la încetarea funcționării acestui proces. După cum se vede, în ambele situații, în cadrul acestui ciclu material-informațional unitar, randamentul compartimentului **I și c**alitatea produselor sub-compartimentului **III** (varianta I → II → III) decisiv depind de nivelul autenticității produselor sub-compartimentului **II,** ceea ce și fondează imperativul asigurării unei protecții cât mai fiabile a lui.

De avut în ve4dere și acea circumstanță, conform căreia formarea (apariția) unei activități sau a unui complex de activități noi este motivată atât de rezultatele anumitor experimente (practici) impuse, cât și de consecințele evoluției proceselor. În acest sens, în prezent evoluția sistemelor informatice economice (S.I$_c$.E.) a condus la apariția și acumularea multiplelor și tot mai variatelor și voluminoaselor probleme ce necesită soluționare cotidiană, eforturi și resurse semnificative. Printre ele de prim ordin de valorificare și conceptual se consideră cele ce asigură gradul necesar de fiabilitate,

securitate şi eficacitate a acestor sisteme. Preponderent, practica funcţionării lor treptat a solicitat domeniului ciberneticii şi informaticii economice formarea anumitor ramuri de cunoştinţe teoretice şi deprinderi practice privind efectuarea activităţilor nominalizate (fiabilitate, securitate, eficacitate) [4, pp.205-208].

Aşa cum procesele economice materiale şi informaţionale se realizează spaţial şi temporal, există necesitatea coordonării lor în cadrul acestor raze. Din motivul dat, orice acţiuni şi activităţi ce se referă la ele solicită abordare sistemică de ordin ştiinţific. Pe lângă cele menţionate, e necesar de avut în vedere faptul că S.Ic.E. este o unitate destul de complexă, fiind compusă din diverse resurse, din care de bază sunt cele tehnice, informaţionale, matematice, programate, tehnologice, economice, socio-juridice, ş.a.

Aşa specific esenţial obiectiv a condus la luarea în considerare a interconexiunilor şi interacţiunilor dintre aceste componente în aşa mod ca sistemul în cauză să funcţioneze cât mai eficient, obţinând cele mai calitative produse informaţionale informative cu cele mai reduse consumuri.

Importanţa protecţiei datelor este, de asemenea, motivată şi de particularităţile mediului economiei de piaţă, care amplifică valoarea funcţională a asigurării acestor parametri calitativi ai S.Ic.E. E cunoscută situaţia că în acest mediu practic este nelimitată solicitarea informaţională a oricărui obiect ori activitate, ceea ce permanent sporeşte volumul şi complică componenţa resurselor informaţionale. Drept urmare se solicită atenţie deosebită protecţiei celor din urmă, care, la rândul sau, se realizează prin intermediul fiabilităţii şi securităţii tuturor celorlalte resurse (tehnice, programate, tehnologice, economice, socio-juridice), ultimele contribuind la eficacitatea generală a funcţionării S.Ic.E. în ansamblu.

EVOLUŢIA, FACTORII ŞI PROBLEMELE ASIGURĂRII PROTEJĂRII RESURSELOR INFORMAŢIONALE ŞI INFORMATICE ECONOMICE

Pe măsura evoluţiei practicii funcţionării S.I$_c$.E. tot mai insistent se solicită specializarea evidentă a serviciilor informatice sub formă de anumite subdiviziuni organizatorice în cadrul unităţilor economice, rareori fiind realizate sub formă de servicii de protecţie a datelor preponderent în sectoarele bancar, statal, afacerilor interne.

După cum se ştie, sistemele informaţionale economice se caracterizează prin volume considerabile, componenţă compusă şi repartizare spaţială extinsă a elementelor sale. Din acest motiv există necesitatea de a asigura o anumită concordanţă dintre diverse nivele şi compartimente ale lor în aşa mod ca obiectele şi procesele economice deservite de ele să dispună de evoluţie prosperă continuă.

În contextul dat conexiunea informaţională contribuie la integrarea activităţilor economice. sub formă de sistem unitar de efectuare a lor, ceea ce în realitate şi e necesar să se producă.

La începuturi, când producerea, distribuirea şi consumarea bunurilor materiale şi spirituale erau de caracter particular şi practic nu se realizau în anumite perioade de timp îndelungate şi pe scară spaţială extinsă, şi informaţiile respective privind aceste activităţi, de regulă, erau „dobândite”, memorizate, prelucrate şi utilizate de un individ sau de un grup redus de indivizi (gospodărie individuală) în mod oral şi în termene operative (pe parcursul activităţilor economice, într-o zi ori câteva zile), fără a implica în aceste procese anumite suporturi şi mijloace auxiliare speciale.

Pe măsura extinderii razei manifestării economice materiale umane tot mai pronunţat devine caracterul social al informaţiei în cauză, iar procesele informaţionale necesită organizarea şi efectuarea lor în mod conştient. De aceea, dacă la faza iniţială a activităţilor materiale economice umane fluxurile informaţionale spaţial se formau şi se

realizau acolo, unde şi cele materiale, apoi treptat, în mod evolutiv, ele tot mai esenţial şi-au majorat atât termenele, cât şi scara de acţiune.

În aşa circumstanţe funcţionarea eficientă a sistemului informaţional economic este bazată nu numai pe concordanţa spaţială şi temporală a proceselor informaţionale, dar în măsură egală şi pe asigurarea protecţiei valorilor unităţilor informaţionale funcţionale. Aceasta din urmă îşi găseşte explicarea în faptul, că odată cu integrarea activităţilor materiale economice în parametrii nominalizaţi, automat se produce şi integrarea fluxurilor informaţionale, ce le însoţesc. În consecinţa fenomenului produs e suficient ca o singură valoare a unităţii informaţionale să fie „alterată", sau pierdută şi sistemul informaţional în ansamblu poate să nu corespundă solicitărilor sistemului de gestiune concret, aşa cum unitatea informaţională respectivă dispune de mulţime de conexiuni cu o mulţime de alte aşa unităţi şi „pierderea" („alterarea") ei, firește, influenţează negativ sistemul informaţional integral. De aceea conceptul organizării resurselor informaţionale sub formă de fişiere separate nu accentuează în mod evident valoarea protecţiei datelor, aşa cum neasigurarea ei se referă la fiecare fişier în parte şi nu afectează tot sistemul informaţional în întregime sau o bună parte a lui.

Totodată, organizarea integrată a datelor înaintează probleme stringente privind securitatea lor din cauza că realizarea ei este condiţionată de conexiunile informaţionale dintre problemele soluţionate. În aşa condiţii „deteriorarea" unei unităţi de date poate să se răsfrângă asupra calităţii sistemului informaţional în ansamblu.

Aşadar, integrarea datelor în procesele de organizare şi transformare obiectiv acutizează necesitatea asigurării stricte a protejării tor. Pornind de la acest considerent, sporirea importanţei activităţilor de protecţie a datelor este condiţionată şi de următorii factori de bază:

1) evoluţia conceptului de organizare a datelor odată cu trecerea de la fişiere separate la baza informaţională unitară integrată, ce deserveşte tot obiectul economic şi fiecare subdiviziune, participant (activitate) şi resursă ale lui;
2) coordonarea şi reglarea proceselor informaţionale economice în spaţiu şi timp;
3) sporirea continuă a numărului şi volumelor unităţilor informaţionale funcţionale;
4) majorarea complexităţii structurale a acestor unităţi;
5) complexitatea varietăţii compoziţionale a unităţilor în cauză;
6) complicarea efectuării proceselor de organizare, transformare şi utilizare a valorilor unităţilor informaţionale în cadrul sistemului de gestiune a unităţii economice.

La rândul său, aceşti factori contributivi la protecţia datelor au condus la necesitatea:

1) evidenţierii, ordonării şi integrării funcţionale a unitaţilor structurale informaţionale, condiţionate de interconexiunea informaţională a problemelor soluţionate şi de utilizarea cât mai economă a spaţiului memorar al sistemului informatic;
2) scoaterii în vileag, sistematizării şi integrării structurale a unităţilor informaţionale cu scopul unificării structurii lor;
3) profilării, clasificării şi integrării procedurilor informaţionale, de prelucrare şi de utilizare a unităţilor structurale de date pentru a exclude dublarea şi iterativitatea lor nejustificată;

În prezent utilizatorii sistemelor informatice economice în mare măsură sunt conştienţi de actualitatea şi necesitatea stringentă a asigurării protecţiei informaţiilor de a fi accesate şi utilizate în mod neautorizat. Însă, deşi se dispune de număr considerabil de publicaţii, anumită experienţă în acest domeniu şi interes major faţă de tematica dată, rămân nesoluţionate următoarele probleme principale:

1) elaborarea unui mod unitar de abordări privind determinarea scopurilor de asigurare a protecţiei informaţionale a sistemului informatic (informaţional) economic;

2) interpretarea neunivocă a terminologiei;

3) elaborarea modului unitar de abordare a clasificării factorilor de influenţă asupra securităţii informaţionale cu evidenţierea şi sistematizarea riscurilor (pericolelor) intenţionate şi potenţiale;

4) compunerea şi respectarea riguroasă a modalităţii unitare de abordare a conceptului de protecţte a sistemului informaţional în ansamblu şi a componentelor lui în particular;

5) elaborarea modului unitar de abordare a evaluării (estimării) protecţiei resurselor sistemului informaţional;

6) întocmirea metodologiei unitare ştiinţifice şi variatelor metodici de realizare a ei în ceea ce privește determinarea dimensiunii pierderilor din cauza abuzurilor programatice;

7) elaborarea unui sistem unitar de criterii (indicatori) de determinare a dimensiunilor riscului şi eficienţei sistemului de securitate informaţională [4, pp.207-210].

ANALIZA MEDIILOR, MIJLOACELOR ŞI METODELOR DE PROTEJARE A RESURSELOR INFORMATICE

Protejarea datelor se efectuează divers în funcţie de mediul formării şi transformării lor. Se evidenţiază două medii de aşa natură – sistemul informaţional şi sistemul informatic. Primul include toate informaţiile ce sunt organizate, prelucrate şi utilizate conform cerinţelor şi în cadrul sistemului de gestiune concret în ansamblu, atât în baza metodelor manuale, cât şi a celor automate. De reamintit că sistemul informatic este nu altceva decât sistemul informaţional realizat prin intermediul mijloacelor tehnice. De atenţionat, de asemenea, că în economie până în prezent încă nu s-a reuşit ca sistemul informaţional să fie realizat pe deplin în mod automat.

În dependenţă de aceste două medii au fost inventate, elaborate şi aplicate diverse mijloace şi metode de protecţie a datelor caracteristice pentru fiecare din ele, ce pe parcurs au evoluat. Varietăţile lor sunt predeterminate de tipurile de suporturi, pe care se înregistrează în mod diferit informaţia. În aşa caz se observă două grupe de mijloace şi metode de securitate a datelor, una referindu-se la documente, iar alta - la suporturile informatice (tehnice). Primele se consideră manuale, iar cele secunde - preponderent automate. La rândul său, mijloacele şi metodele manuale sunt de caracter fizic, aşa cum ele depind de proprietăţile şi de „posibilităţile” fizice ale acestei categorii de suporturi (documente) de a proteja informaţia. Ele se elaborează şi se implementează în sistemele informaţionale bazate pe organizarea şi transformarea informaţiei în mod manual integral sau parţial.

Mijloacele şi metodele de protecţie a datelor caracteristice pentru suporturi tehnice (informatice) sunt atât de categorie fizică, cât şi programatică. În cadrul ambelor grupe de aşa mijloace şi metode (manuale şi informatice), de asemenea, pot fi realizate diverse procedee organizatorice de securitate a datelor. Metodele fizice sunt condiţionate nu numai de particularităţile fizice ale suporturilor, dar şi a dispozitivelor mijloacelor tehnice, a tehnologiilor informaţionale şi informatice. În acest sens se poate presupune că odată cu performanţa construcţiei elementelor constructive şi „duritatea” fizică a mijloacelor tehnice, ponderea şi valoarea mijloacelor programatice de securitate a datelor, posibil, vor scădea.

În general raportul dintre mijloacele şi metodele fizice şi cele organizatorice depinde de calitatea şi performanţa celor dintâi şi valoarea sociala a informaţiilor. Cu cât

primele sunt mai imperfecte cu atât componenţa metodelor organizatorice este mai variată, concomitent cu performanţa lor continuă.

Afară de cele menţionate, e necesar de atenţionat asupra faptului că, fiind inventată şi utilizată de subiect, informaţia economică se consideră produs artificial şi cu acest prilej aspectul subiectiv al mijloacelor şi metodelor de formare şi protejare a ei este decisiv. Din motivul dat asigurarea protecţiei acestei informaţii depinde nu numai de performanţa metodelor şi mijloacelor, dar şi de valoarea şi caracterul ei social. De aceea, cu cât valoarea funcţională şi socială a informaţiilor economice este în ascensiune, ce este firesc şi continuu pentru ea, cu atât mai complicate şi mai variate sunt tentativele de a o „altera" şi a o „lichida" ca produs de importanţă primordială în societatea umană. În contrariu acestor tentative se dezvoltă mijloacele şi metodele de protecţie a datelor.

După cum s-a stabilit anterior, metodele şi mijloacele de asigurare a protejării datelor în sistemul informaţional sunt de caracter manual şi limitate de proprietăţile unui singur tip de suporturi - documentul. Din acest motiv preponderent ele sunt de ordin fizic şi se realizează în mod organizatoric. Unele din ele se referă la protecţia sistemului informaţional în ansamblu (localurile, mijloacele auxiliare, mobilă specială şi alte echipamente de păstrare, organizare şi manipulare a documentelor), iar altele - la protecţia conţinutului funcţional al acestui sistem (diverse cartoteci, mape, dulapuri şi stelaje de păstrare a documentelor). De regulă, documentele completate sunt organizate în pachete după termenele de formare (perfectare) a lor (o zi, cinci zile, decadă, lună, trimestru, semestru, an, etc.) şi pe obiecte şi activităţi (de exemplu, documente pe intrările valorilor materiale, ieşirile lor, ori pe îndeplinirea anumitor volume de lucrări etc.). Protecţia conţinutului informational al documentaţiei elaborate este asigurată de semnăturile persoanelor responsabile de deplinătatea şi autenticitatea valorilor datelor înregistrate.

Accesul la informaţii este protejat prin intermediul diverselor documente reglementative (regulamente, acte normative, juridice, administrative, instrucţiuni de serviciu ş.a.) a activităţilor informaţionale, a obligaţiunilor funcţionale ale utilizatorilor, etc.

În aşa mod, afară de mijloacele si metodele fizice şi organizatorice, protejarea datelor este asigurată şi de metode şi mijloace juridice. Odată cu elaborarea, implementarea şi funcţionarea sistemelor informatice economice s-a schimbat şi componenţa mijloacelor şi metodelor de protecţie specifice lor. De exemplu, mijloacele tehnice de calcul trebuie să fie repartizate şi exploatate în aşa zone ale clădirilor, care ar asigura ferirea lor de diverse intenţii destructive. Locurile, unde se găsesc aceste mijloace, de asemenea, trebuie sa fie amenajate şi echipate conform cerinţelor ştiinţifice de asigurare a condiţiilor de menţinere fizica a tehnicii nominalizate în starea de funcţionare eficientă şi de excludere a posibilităţilor de a le distruge ori a le fura (uşi de fer. lacăte complicate, etc.).

De asemenea, e necesar de luat un şir de măsuri organizatorice privind excluderea accesului utilizatorilor neautorizaţi la fişiere şi programe sau a cauzelor generatoare de distrugere a lor. În acest scop se poate organiza eliberarea suporturilor (benzi, dischete, C.D.) cu fişiere numai în baza unor aprobări speciale ale persoanelor autorizate. Sălile calculatoarelor şi locurile de depozitare a fişierelor trebuie să fie protejate împotriva focului, prafului, excesului de temperatura şi umiditate, precum şi a altor cauze ce pot afecta datele păstrate.

În mediul sistemelor informatice economice pe larg este aplicată etichetarea fişierelor (internă, externă), care se consideră drept mijloc de protejare a datelor de utilizări eronate.

Protejarea fişierelor poate fi efectuată şi prin intermediul soft-ului, prin introducerea anumitor parametri (parole), care să ofere posibilitatea numai de citire sau citire şi înregistrare.

Pot fi utilizate anumite proceduri de restaurare a fişierelor de date sau de specificare a efectuării asupra lor a operaţiunilor de distrugere ori păstrare. De importanţă semnificativă dispun copiile fişierelor de date şi a resurselor programate pe suporturi păstrate în alte localuri, decât cele ale calculatoarelor.

În cazul prelucrării datelor în loturi se recomandă procedura de protecţie sub denumirea convenţională „bunic - tată – fiu" şi modificările ei. O procedura similara trebuie realizată şi în cazul, când fişierele sunt actualizate on - line. În cazul utilizării sistemelor de gestiune a bazelor de date, de administratorul bazei de date pot fi luate măsuri suplimentare prin utilizarea dicţionarelor de date şi a unor forme specifice de control confidenţial. Dacă datele sunt strict confidenţiale, se recomandă distrugerea (chiar şi prin ardere) a listelor iniţiale ori aplicarea protecţiei criptografice prin utilizarea codurilor secrete de transformare a datelor. Criptarea se recomandă pentru datele transmise prin linii de telecomunicaţii [2, 126- 135; 4, 207-210].

Protejarea datelor se asigură şi prin intermediul verificării deplinătăţii, clarităţii şi autenticităţii lor în cadrul fiecărei operaţiuni tehnologice de organizare, perfectare, păstrare şi prelucrare a lor. Controlul lor se efectuează de anumite mijloace, metode şi procedee.

La nivel de sistem informatic economic, în baza următoarelor criterii (principii) de clasificare, toate aceste metode şi mijloace pot fi sistematizate în următoarele grupe:

1) complexitatea încadrării (cuprinderii) – mijloace şi metode locale şi complexe;
2) predestinare funcţională – mijloace şi metode de anticipare (avertizare), depistare şi neutralizare a riscurilor, de restituire (recuperare) a sistemului interpretat drept unitate organizatorică de activitate;
3) natura categoriilor lor – mijloace şi metode juridice, organizatorico - administrative şi tehnico-programatice;
4) aria spaţială de acţiune - mijloace şi metode pentru zone necontrolate (externe), zone teritoriale controlate, pentru localurile funcţionării sistemului informatic, resursele lui;
5) etapele operaţionale de funcţionare a sistemului nominalizat - mijloace şi metode pentru controale la intrări, pe parcursul funcţionării (reglementării şi constrângerii redundanţei, reviziei, restituirii), la ieşiri din sistem;
6) obiectivele protecţiei - mijloace şi metode de protecţie de la acces neautorizat, de asigurare a valorii juridice, a conţinutului informaţional, de protecţie de la scurgere a informaţiei prin canalele sistemului, de protecţie de la abuzuri programatice, de la copieri neautorizate, difuzări a programelor şi informaţiilor confidenţiale computerizate;
7) caracterul opunerii - mijloace şi metode de protecţie activă şi pasivă.

Din cele enumerate, devine evident că componenţa metodelor şi mijloacelor de securitate a datelor este destul de variată şi depinde de scopurile aplicării lor, domeniile de realizare, modalităţile de efectuare ş.a. Despre conţinutul şi esenţa unora din ele se poate uşor de judecat în baza denumirilor lor. Altele, însă, necesită explicare, ultima fiind motivată şi de valoarea lor funcţională.

De pe aceste poziţii, metodele şi mijloacele de anticipare sunt predestinate pentru a crea aşa condiţii, în mediul cărora posibilitatea apariţiei şi realizării factorilor (riscurilor) de destabilizare să fie nulă sau minimă. Metodele şi mijloacele de depistare sunt orientate spre evidenţierea pericolelor apărute ori a posibilităţilor apariţiei lor şi colectarea informaţiilor suplimentare în acest sens. Metodele şi mijloacele de neutralizare contribuie

la neutralizarea pericolelor apărute, pe când cele de restituire (recuperare) - la restabilirea funcţionarii normale a sistemului informatic.

Metodele şi mijloacele tehnico-programatice de asigurare a securităţii datelor pot fi active şi pasive. Primele (cele active) sunt predestinate pentru delimitarea accesului la toate resursele sistemului informatic (tehnice, programatice, informaţionale ş.a.); transformarea datelor autentice în informaţii inutile (false) pentru infractor (acoperirea criptografică); restabilirea funcţionării normale a sistemului. Printre cele pasive de bază se consideră metodele şi mijloacele de monitoring a funcţionării sistemului informatic, de prelucrare şi analiză a datelor colectate pe parcursul monitoringului, de revizie şi audit a efectivului şi utilizării optime a resurselor sistemului, precum şi stabilirea (verificarea) integrităţii şi accesibilităţii acestor resurse.

Componenţa metodelor şi mijloacelor de securitate a datelor este condiţionată de varietăţile pericolelor ce pot avea loc în sistem. Posibilitatea realizării pericolelor depinde de locurile înguste (punctele vulnerabile) ale sistemului.

Drept pericol se consideră orice acţiune ce contribuie la dereglarea funcţionării sistemului. Se evidenţiază două tipuri de pericole de violare a securităţii datelor:

1) neintenţionate sau ocazionale;
2) acţiuni intenţionate.

Primul tip de pericole sunt de ordin extern şi intern. La cele externe se referă calamităţile naturale, factorii tehnogenici, politici, economici, sociali, extinderea tehnologiilor informaţionale şi comunicaţionale ş.a. În cadrul celor interne se includ pericolele provocate de stoparea funcţionării mijloacelor tehnice, erori în resursele programate, în activitatea personalului ş.a.

Cele mai răspândite acţiuni intenţionate de violare a securităţii resurselor sistemului informatic se consideră următoarele:

1) acces neautorizat la informaţii;
2) elaborarea resurselor programate specializate cu scopul accesului neautorizat;
3) elaborarea şi difuzarea viruşilor computeriali;
4) neglijenţă în elaborarea, susţinerea şi exploatarea resurselor programate;
5) furt de informaţii;
6) manipulare nejustificată a datelor;
7) încălcarea (nerespectarea) confidenţialităţii datelor;
8) negarea violării securităţii resurselor sistemului ş.a.

Cunoaşterea bazelor teoretice, dispunerea de anumită experienţă în activităţi de elaborare, implementare şi funcţionare a sistemelor de protejare a informaţională în economie va contribui în mod decisiv la majorarea calităţii resurselor informaţionale, ceea ce, la rândul său, va conduce la performarea sistemului de gestiune, iar ultimul - ia îmbunătăţirea rezultatelor activităţilor unităţilor materiale economice.

Actualmente de importanţă semnificativă dispune securitatea resurselor informaţionale ale reţelelor informatice – cele mai adecvate realizării automate a proceselor informative economice.

Aşa securitate este de valoare extremă pentru fiecare computer conectat la Internet, sau aflat într-o reţea de tip Intranet, Extranet şi chiar o reţea locală. Mai mult, chiar si pentru un P.C. stand-alone securitatea informaţiei poate fi o problemă serioasă, atunci, când acesta conţine informaţii personale, secrete, de anumit grad de confidenţialitate.

Prin intermediul acestei securităţi se protejează informaţiile de o paletă extinsă de pericole legate de asigurarea continuă a activităţilor, de minimizarea pagubelor şi de maximizarea recuperării investiţiilor şi a oportunităţilor de afaceri.

Indiferent, se află calculatorul în birou sau pe pupitru acasă, asigurarea securităţii informaţiilor poate dispune de aceeaşi acuitate. Evident, în cazul reţelei, asigurarea securităţii reprezintă o problemă mult mai stringentă şi, totodată, mult mai dificilă. Multe din atacurile recente de tip denial-of-service, care au pus în real pericol câteva site-uri de Web foarte populare, unele chiar guvernamentale, au reuşit să provoace situaţie de panică la autorităţile din mai multe ţări, chiar şi puternic dezvoltate. Unele voci au ajuns până la aceea că aşa pericole au devenit mult mai acute decât se credea până acum prin consecinţele sale, uneori inimaginabile.

Au existat suficiente dovezi, care susţineau poziţia acelora ce credeau că atacurile hackerilor au fost posibile din cauză că s-a reuşit obţinerea accesului doar la calculatoarele slab protejate. Cu alte cuvinte, spărgătorii de coduri au succes doar acolo, unde nu se asigură o securitate riguroasă tehnogenică.

Pericolul sabotajului prin calculator bazat pe viruşi, care pot face distrugeri extraordinare, este astăzi bine cunoscut şi de necontestat, nemaivorbind despre viruşi, care pot prelua controlul complet asupra unui calculator dintr-o reţea, precum periculosul cal troian "Back Orifice".

În pofida unor sisteme legislative destul de bine puse la punct, furtul de informaţii prin intermediul calculatorului s-a extins foarte mult, mai ales, în unele ţări, care deţin tehnologii avansate. El reprezintă un domeniu extrem de delicat, iar pentru protecţia si securitatea datelor se fac eforturi uriaşe.

Cele enumerate mai sus ar putea însemna doar o mică parte din numeroasele motive, pentru care este necesar să se acorde atenţie deosebită securităţii informaţiilor din calculatoare.

S-ar putea spune că majoritatea utilizatorilor din cele mai mari si mai importante instituţii din lume se află sub acoperirea unor firewall-uri de companie sau personale si că, în cazul lor, securitatea este complet asigurată. În realitate, însă, lucrurile nu stau chiar aşa. Şi dovezi în acest sens, desigur, există. Aproape zilnic apar pe Internet informaţii privind spargerea unor site-uri de Web importante, furturi de informaţii din diverse reţele, unele dintre cele mai bine puse la punct, iar dacă se mai ia în considerare că mulţi dintre cei păgubiţi refuză să-şi facă publice accidentele de această natură, chiar şi din simplul motiv de a nu risca pierderea credibilităţii sau a prestanţei, atunci, desigur, se poate confirma că statisticile nu oferă dimensiunea reală a fenomenului, iar acesta este cu mult mai îngrijorător.

În contextul afacerilor informaţiile şi procesele, pe care se sprijină sistemele si reţelele informatice, sunt subiecte deosebit de importante. Cele trei caracteristici de bază ale informaţiei (confidenţialitatea, integritatea si disponibilitatea) sunt esenţiale pentru menţinerea competitivităţii, profitabilităţii, legalităţii si imaginii comerciale ale unei organizaţii.

Din ce în ce mai mult, organizaţiile, sistemele si reţelele lor informatice se confruntă cu ameninţarea securităţii informaţiilor provocate de un larg spectru de surse, incluzând frauda, spionajul, sabotajul, vandalismul, incendiile şi inundaţiile. O sursă comună de pericol este prezentată de atacurile virusilor electronici, care pot provoca daune şi distrugeri considerabile. Aceste mijloace devin din ce în ce mai agresive şi mai sofisticate.

Unii oameni de afaceri şi profesionişti au ajuns la concluzia că un hacker suficient de competent poate pătrunde în aproape orice sistem de calcul, inclusiv în cele care au fost protejate prin metode bazate pe parole şi criptarea datelor. Alţii, mai sceptici, susţin că, chiar si atunci, când un sistem este bine protejat împotriva atacurilor din exterior, rămâne întotdeauna alternativa trădării din interior. Multe date secrete, cum ar fi listele de clienţi,

salariile angajaţilor, investiţii şi bugete, referate confidenţiale ş.a., pot fi copiate pur si simplu pe o dischetă sau USBFlash, iar aceasta poate fi scoasă de la locul de muncă, deseori chiar fără să se sesizeze ceva.

Calculatoarele de tip mainframe rezolvă problema furtului prin această sursă păstrând încuiate calculatorul şi suporturile mari de stocare a datelor. În cazul mainframe-urilor, singura cale de a putea folosi datele este cea oferită de terminalele aflate la distanţă, şi care sunt dotate cu un ecran, o tastatură, dar nu si cu unităţi de disc. Din cauza acestei siguranţe suplimentare oferite de sistemele de tip mainframe, unii experţi susţin că reţelele locale de calculatoare personale ar trebui configurate la fel, uitând că centralizarea excesivă a mainframe-urilor a fost unul din principalele motive, pentru care s-au dezvoltat calculatoarele personale.

Orice conectare obişnuită la Internet nu este întotdeauna lipsită de riscuri. Conexiunea propriu zisă, absolut inocentă la prima vedere, ar putea fi însoţită prin partaj fraudulos de un parazit sau un program spion, care dispune de rol foarte bine definit: de a fura o parte din informaţiile manipulate, unele din ele, desigur, de caracter strict confidenţial pentru proprietar. În acest sens, cu siguranţă există mare doză de neâncredere în aprecierile de natură pesimistă a unora, si de multe ori, cu sau fără voie, sunt exagerate.

În lumea specialiştilor I.T. se obişnuieşte să se spună că un P.C. este complet protejat de un produs firewall si de un program antivirus. Exista produse informatice ce pot asigura protecţie foarte bună pentru grupurile mici sau pentru P.C. - urile individuale. De exemplu, firewall-uri precum ZoneAlarm (www.zonelabs.com) sau BlackICE Defender (www.netice.com), sunt foarte la modă astăzi, iar produsele antivirus sunt foarte multe şi foarte eficace.

Tranziţia la societatea informaţională implică nevoia de informaţii credibile, iar progresul tehnologic are implicaţii de ordin exponenţial asupra evoluţiei lor. Din acest punct de vedere, necesitatea securizării informaţiilor păstrate şi procesate prin intermediul calculatoarelor decurge pur şi simplu din necesitatea de conectare si de comunicare, iar globalizarea şi Internetul au schimbat complet faţa lumii la confluenţa dintre milenii.

Calculatoarele personale prezintă vulnerabilităţi pentru că în general nu există protecţie hardware a memoriei interne şi externe: un program executabil poate avea acces oriunde în memoria internă sau pe hard-disk. În orice sistem informatic protecţia presupune asigurarea programelor şi datelor împotriva următoarelor acţiuni:

1) pierderi accidentale, cauzate de căderile de tensiune, defectarea unităţilor de hard disk;
2) accesare neautorizată a datelor şi programelor, prin acţiuni de parolare şi criptare;
3) fraudă pe calculator (sustragerea sau alterarea datelor, furturi de servicii);
4) virusarea software-ului.

Pentru o protecţie eficientă este necesar să fie cunoscute şi asigurate următoarele elemente:

1) identificarea accesului prin reguli şi relaţii între utilizatori şi resurse;
2) evidenţa accesului pentru urmărirea utilizării resurselor sistemului, precum şi pentru posibilitatea refacerii unor date în caz de distrugere;
3) integritatea şi confidenţialitatea datelor;
4) funcţionalitatea programelor.

Mijloacele prin care se poate asigura protecţia sunt:

1) măsuri organizatorice contra distrugerii datorate catastrofelor naturale, măsuri referitoare la selecţia profesională a personalului, organizarea unui sistem de control a accesului, organizarea păstrării si utilizării suporturilor de informaţii;

2) măsuri juridice, care cuprind documente normative ce controlează şi reglementează procesul prelucrării şi folosirii informaţiilor;

3) mijloace informatice constituite din programe de protecţie şi tehnici de criptare a informaţiilor.

Cele mai cunoscute şi utilizate modele de asigurare a protecţiei (autorizare a accesului) sunt:

1) Modelul Hoffman, constă dintr-un set de reguli referitoare la 4 tipuri de obiecte - utilizatori, programe, terminale şi fişiere, fiecare cu 4 caracteristici de securitate:

a) autoritatea (nesecret, confidenţial, secret, strict secret);
b) categoria (compartimente specifice de grupare a datelor (acces limitat, acces cu aprobare));
c) dreptul (grupa de utilizatori, care au acces la un anumit obiect);
d) regimul (mulţimea modurilor de acces la obiect: citire, actualizare, execuţie program).

2) Modelul Kent, are 5 dimensiuni: împuterniciri, utilizatori, operaţii, resurse, situaţii. El conţine un proces de organizare a accesului bine definit printr-un algoritm. Accesul la date este considerat drept serie de cereri ale utilizatorilor pentru operaţii la resurse într-un moment, în care sistemul se află în anumită stare [2, pp.176-183; 4, pp.220-224].

În final e necesar de accentuat că activitatea problemei protecţiei resurselor informatice este cauzată în primul rînd de masivitatea implementării şi utilizării celor de pe urmă practic în orice domeniu al activtăţii umane şi, mai cu seamă, a lucrărilor informaţionale economice, proprii pentru orice categrie de ocupaţii.

Aşa cum funcţionarea eficientă S.I$_c$.E. este asigurată prin interconexiunea şi interacţiunea corectă a constituantelor sale, astfel de preocupare devine iminamente imposibilă. Complicarea şi imperiositatea ei devin şi mai evidente în cazul aplicării mijloacelor şi metodelor informtice ce solicită îndeplinirea acţiunilor în mod automat. În aşa situaţie nu e exclus că în unele cazuri o singură eroare să conducă la alterarea şi prăbuşirea sistemului.

Din motivele enumerate mai sus şi menţionate de la începutul articolului prezent se impun conştientizarea convingătoare a rolului imperios al protejării componentelor informatice, cunoaşterea profundă a evoluţiei, distincţiei dintre fiabilitatea şi securitatea lor, categoriilor şi concordanţei mijloacelor şi metodelor acestor procese, ceea ce va contribui la performanţe notorii a lucrărilor legate de obţinerea produselor informaţionale în mediul informatic

CONCLUZII

1. Locul, rolul și valoarea funcțională în cadrul procesului unitar de gestiune economică dictează preocuparea primordială de protejare a informațiilor de conținut informativ.
2. Astfel de abordare este justificată de faptul că datele informative constituie consecința evoluției proceselor materiale și baza obținerii produselor decizionale. De aceea, de calitatea lor depinde formularea și luarea deciziilor, care direct influențează compartimentul material.
3. Totodată, protejarea izolată numai a unităților informaționale nu asigură nivelul performant deplin al calității lor, deoarece pe lângă protecție, asupra acestui parametru esențial influențează mijloacele, metodele și resursele implicate în procesarea valorilor acestor unități.

4. Din motivul dat protecția informațională integrală solicită elucidarea ei în interconexiune și interacțiune cu mijloacele și metodele de protejare a celorlalte resurse informatice.
5. Complexitatea compoziţională, volumele inimaginabile a resurselor informaționale și informatice, provocate de mersul obiectiv al proceselor globalizării activităților umane materiale și spirituale, au condus la complicarea şi acutizarea problemelor protejării şi eficientizării S.I$_c$.E.
6. Pe lângă acest fenomen, problemele în cauză sunt provocate şi de următorii factori de influenţă semnificativă:
   a) nivelul nesatisfăcător al parametrilor exploatativi ai mijloacelor tehnice informatice, de valoare decisivă dispunând suporturile informaţionale şi informatice, precum şi dispozitivele de afişare;
   b) tendinţa spre proprietatea privată a informaţiilor, aşa cum fiecare utilizator pretinde la resursele informaţionale proprii;
   c) valoarea juridică a informaţiilor economice, ceea ce solicită grad major de autenticitate a lor;
   d) ca şi orice alte informaţii, cele economice nu se consumă, din ce cauză pierderea poate conduce la imposibilitatea recuperării lor;
   e) primitivismul activităţilor de fiabilitate şi securitate a S.I$_c$.E., organizarea sistemică a cărora se găseşte la etapa iniţială.
7. Pe măsura evoluţiei practicii funcţionării S.I$_c$.E. în cadrul unităţilor economice,, tot mai insistent se impune specializarea evidentă a serviciilor informatice sub formă de anumite subdiviziuni organizatorice, rareori fiind realizate sub formă de servicii de protecție a resurselor informaționale și informatice, preponderent în sectoarele bancar, statal, afacerilor interne.
8. De pe pozițiile integrării într-un tot unitar și funcționării analoage, structurarea existentă a procesului managerial economic (fig.2) este provocată de următorii factori esențiali:
   a) dispersarea excesivă în spațiu și funcționarea expresiv discretă în timp, aceasta din urmă fiind cauzată în primul rând de gradul insuficient și primitivismul efectuării activităților materiale și informaționale umane;
   b) extinderea semnificativă a dimensiunilor teritoriale și scurtarea termenelor temporale ale preocupărilor materiale umane;
   c) respectiv, și ocupațiile informaționale, care sunt obiectiv impuse, deci, indetașabile de cele materiale, în evoluția sa s-au transformat din domeniu de preocupări a unui subiect (grup de subiecte) în domeniu de interes al societății în ansamblu.
9. Ieșirea din situația creată și perspectiva performanței permanente a domeniului elucidat pot avea loc prin crearea și aplicarea mijloacelor și metodelor bazate pe principiul integrării.

BIBLIOGRAFIE

1. Considerations on challenges and future directions in cybersecurity. Romanian Association Information Security, Romania, 2019, 333 p.
2. Ivan, I., Toma, C., Constantinescu, R. Information Security Handbook – Second Edition, Bucurежti Ed. ASE, 2009, 257-280 p..
3. Войтик А. И.,. Прожерин В.Г.Экономика информационной безопасности. Санкт-Петербург, Национальный Исследовательский Университет, 2012, 120 с.
4. Leahu T. Organizarea, structurarea și transformarea informațiilor sistemului managerial economic. Chișinău, CEP USM, 2009, 431 p.