INFONUCLEAR

SUPORT TEHNOLOGIC PENTRU DISEMINAREA INFORMAȚIEI DIN DOMENIUL NUCLEAR

Florin Hartescu
Mădălin Leauta
Valentin Cristea

Institutul Național de Cercetare – Dezvoltare în Informatică, ICI, București

Rezumat: Lucrarea prezintă arhitectura unui suport tehnologic pentru diseminarea informației, structurată pe trei niveluri, completată cu un al patrulea nivel care asigură o securitate sporită:

- nivelul interfeței cu utilizatorul rulează pe un browser de Web care permite accesul distribuit de la utilizatori;
- nivelul de comunicație se bazează pe un server Web. Acest nivel controlează comunicația dintre produsul software client și cel server corespunzător. Comunicația dintre programul client și server se realizează pe baza protocolului HTTP sau pe baza protocolului HTTPS, care prezintă un sistem de securitate mai ridicat. De remarcat faptul că ambele protocoale utilizează comunicații de tip connectionless. Acest lucru presupune ca la nivelul ambelor subsisteme (client și server) se dezvoltă funcții pentru împachetarea și despachetarea mesajelor schimbate între ele și implică utilizarea unui format de mesaj de comunicație cu structura standard la nivelul de aplicație pentru a putea suporta funcții și sisteme diferite;
- nivelul de stocare a datelor se constituie din trei componente. Acestea sunt sistemul de acces la baza de date, unul sau mai multe servere de baze de date și bazele de date propriu-zise. Sistemul de acces la baza de date include o colecție de clase pentru accesul la bazele de date sau programele necesare. Utilizarea mai multor tipuri de drivere de acces la baze de date impune o standardizare a limbajului de definire a bazelor de date și un instrument de conversie a tabelelor aflate în dependență din baze de date diferite, precum și posibilități de migrare ale acestor tabele între bazele de date.

Cuvinte cheie: bibliotecă virtuală, bază de date, sisteme de securitate, arhitectură client – server, Internet.

1. Introducere

Procesul de programare convențională folosește, de obicei, patru faze: analiza, proiectarea, implementarea și întreținerea.

În timpul analizei, s-a construit un model al aplicației în termenii domeniului nuclear. Această analiză s-a bazat, în special, pe problemele specifice ale domeniului din care face parte aplicația, nu pe considerente de limbaj software.

S-a urmărit obținerea unui model independent de constrângerile sau avantajele Web-ului, un sistem robust dar și securizat utilizând Apache, Php și Oracle, care să respecte cerințele aplicației din punct de vedere funcțional, dar, în același timp, să prezinte și un grad cât mai ridicat de abstractizare.

În privința bazelor de date, care, de obicei, au propriile sisteme de securizare, riscurile și vulnerabilitățile sunt cele create de o configurare greșită și de nerespectarea de către utilizatori a regulilor de accesare și abuzul asupra drepturilor și privilegiilor acordate.

ORACLE utilizează blocările pentru a controla accesul concurent la date.

Este foarte posibil într-un mediu multiutilizator, ca utilizatorii să își blocheze unii altora resursele. Este, de asemenea, posibil ca doi utilizatori să sfârșească prin a-și bloca unul altuia diferite resurse.

Sistemul de securitate oferit prin utilizarea ORACLE se refera la înregistrarea tuturor utilizatorilor și autentificarea lor la fiecare accesare a aplicației pentru a controla accesul la baza de date și pentru a înregistra utilizatori cu diferite niveluri de drepturi de acces. Când s-a creat un nou utilizator, un număr de drepturi se atribuie pentru a defini tipurile de activități permise pentru fiecare utilizator. Dacă se încerca executarea unei operații neautorizate, sistemul nu va permite ca operația să aibă loc.

Atunci când o bază de date acumulează un volum mare de date, securitatea datelor poate deveni o problemă importantă din cel puțin din două motive:

1. în primul rând, trebuie prevenită distrugerea datelor din cauza accidentelor hardware, cum ar fi defectarea echipamentelor. (Oracle oferă o soluție pentru acest tip de incidente.);
2. în al doilea rând, trebuie prevenită posibilitatea alterării datelor - prin distrugere sau modificare - de către un operator neautorizat, cu sau fără rea intenție.

Față de versiunile anterioare, Oracle 9*i* îmbunătățește securitatea, interoperabilitatea, performanța și ușurința utilizării prin suportul standard pentru Public Key Infrastucture (PKI) și alte noi funcționalități.

Oracle Advanced Security 9.0.1 asigură creșterea securității prin legătura cu serviciile de securitate pentru Oracle 9i prin integrarea Public Key Infrastructure (PKI).

Serverele Web disponibile în prezent oferă tipuri și niveluri diferite de securitate. Câteva caracteristici de securitate oferite de serverele web sunt:

- Configurări care permit schimbarea userului cu nume de user și parola;
- Suportul SSL (versiunea 2 și 3);
- Suportul S-HTTP;
- Suportul PCT;
- Accesul restricționat prin nume de domeniu;
- Accesul restricționat prin adrese IP;
- Configurarea unor grupuri de utilizatori;
- Posibilitatea de a schimba controlul accesului fără a restarta serverul;
- Ascunderea unor părți din documente, bazată pe reguli de securitate;
- Interzicerea accesului la fișierele sistem;
- Permisiuni acordate pe sistemul ierarhic pentru documentele de bază;
- Permiterea sau interzicerea accesului la toate fișierele în afară de cele aflate în lista de acces.

Serverul Oracle necesită autentificarea utilizatorului (prin parolă și host).

Serverele Web cele mai importante oferă caracteristici de securitate la niveluri diferite, prezentate de autorii serverului sau companiile care dețin drepturile de autor sau de vânzare.

În tabelul următor sunt comparate câteva dintre aceste caracteristici comune:

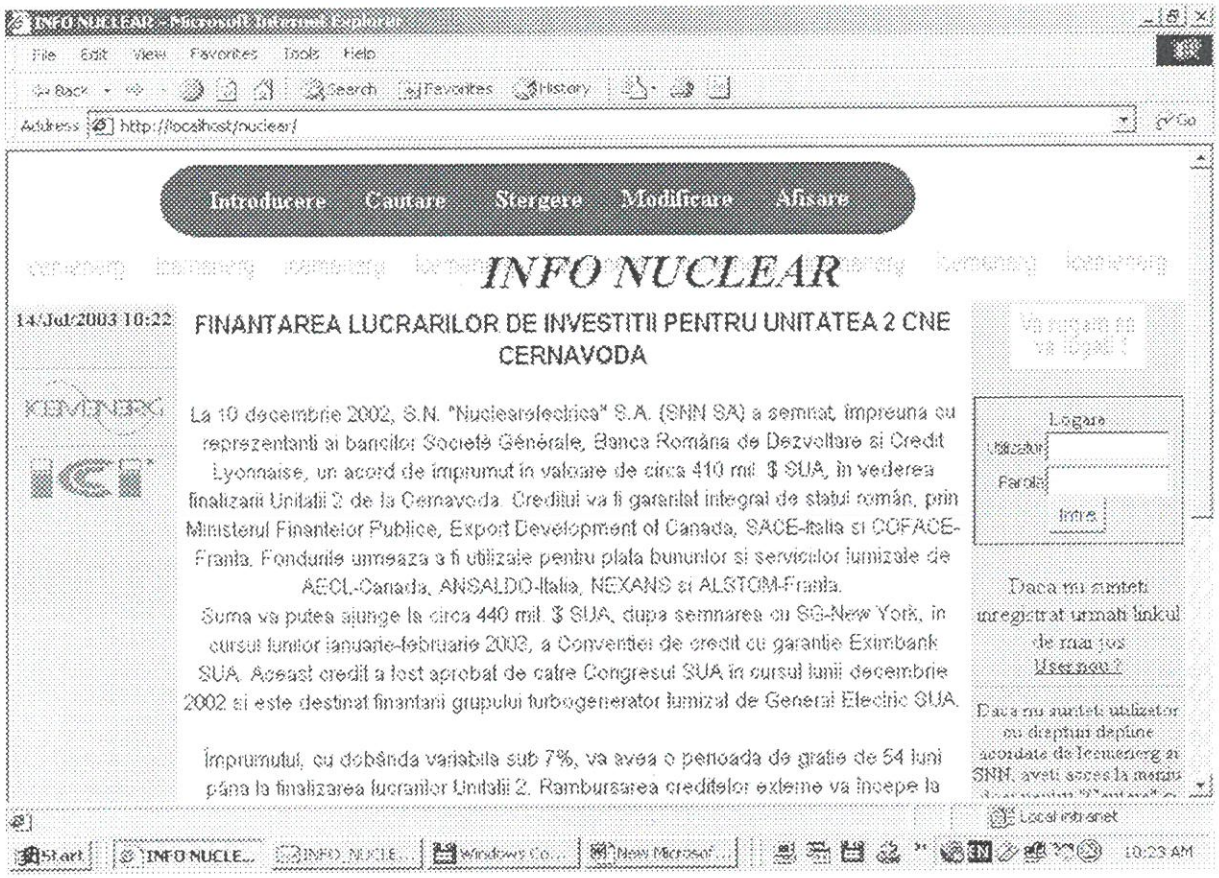
CARACTERISTICI	***SERVER WEB***
Pot cere parola pentru autorizare utilizator	Alibaba, Apache, ApacheSSL, CL-HTTP, Commerce Builder, DECthreads, EnterpriseWeb, Esplanade, Esplanade Secure, ExpressO, Fnord, FolkWeb, GNNserver, GoServe, IBM Connection, IBM Connection Secure, Jazz, MacHTTP, Microsoft IIS, NCSA, Netscape Enterprise, Netscape FastTrack, NetWare Web, Open Market Secure, Open Market WebServer, Oracle, Purveyor, Quarterdeck WebServer, Sioux, Spinnaker, Spinner, SPRY SafetyWeb, SPRYWeb, SuperWeb, TECWeb, W4, Web Commander, WebServer400, WebSite, WebSite Pro, WebSTAR 95/NT, WebSTAR Mac, Webware Comm, WN, Zeus
Suporta SSL v. 2	Alibaba, ApacheSSL, Commerce Builder, COSMOS, Esplanade Secure, GNNserver, IBM Connection Secure, Microsoft IIS, Netscape Enterprise, Netscape FastTrack, Open Market Secure, Oracle, Purveyor, Sioux, SPRY SafetyWeb, Web Commander, WebSTAR Mac, Zeus
Suporta SSL v. 3	Netscape Enterprise, Netscape FastTrack, Sioux
Suporta S-HTTP	IBM Connection Secure, Open Market Secure, Web Commander
Interzicerea prin nume de domeniu	Alibaba, Apache, ApacheSSL, CL-HTTP, Commerce Builder, DECthreads, EnterpriseWeb, Esplanade, Esplanade Secure, ExpressO, FolkWeb, GN, GNNserver, GoServe, IBM Connection, IBM Connection Secure, Jazz, MacHTTP, NCSA, Netscape Enterprise, Netscape FastTrack, NetWare Web, Open Market Secure, Open Market WebServer, Oracle, Purveyor, Quarterdeck WebServer, Sioux, Spinner, SPRY SafetyWeb, SPRYWeb, TECWeb, Web Commander, WebServer400, WebSite, WebSite Pro, WebSTAR 95/NT, WebSTAR Mac, Webware Comm, WN, Zeus
Interzicerea prin adresa IP	Alibaba, Apache, ApacheSSL, CL-HTTP, Commerce Builder, DECthreads, EnterpriseWeb, Esplanade, Esplanade Secure, ExpressO, Fnord, FolkWeb, GN, GNNserver, GoServe, IBM Connection, IBM Connection Secure, Jazz, MacHTTP, Microsoft IIS, NCSA, NetPresenz, Netscape Enterprise, Netscape FastTrack, NetWare Web, Open Market Secure, Open Market WebServer, Oracle, Purveyor, Quarterdeck WebServer, Sioux, Spinnaker, Spinner, SPRY SafetyWeb, SPRYWeb, SuperWeb, TECWeb, W4, Web Commander, WebServer400, WebSite Pro,

	WebSite, WebSTAR 95/NT, WebSTAR Mac, Webware Comm, WN, Zeus
Configurarea unor grupuri de useri	Alibaba, Apache, ApacheSSL, CL-HTTP, Commerce Builder, EnterpriseWeb, Esplanade, Esplanade Secure, ExpressO, Fnord, FolkWeb, GNNserver, GoServe, IBM Connection, IBM Connection Secure, Jazz, Microsoft IIS, NCSA, Netscape Enterprise, Netscape FastTrack, NetWare Web, Open Market Secure, Open Market WebServer, Oracle, Purveyor, Quarterdeck WebServer, Sioux, Spinnaker, Spinner, SPRY SafetyWeb, SPRYWeb, SuperWeb, TECWeb, Web Commander, WebServer400, WebSite, WebSite Pro, WebSTAR 95/NT, Zeus
Posibilitatea de a conecta userul fără restartarea serverului	Alibaba, Apache, ApacheSSL, CL-HTTP, Commerce Builder, DECthreads, EnterpriseWeb, Esplanade, Esplanade Secure, ExpressO, FolkWeb, GN, GNNserver, GoServe, IBM Connection, IBM Connection Secure, Jazz, MacHTTP, Microsoft IIS, NCSA, Netscape Enterprise, Netscape FastTrack, NetWare Web, Open Market Secure, Open Market WebServer, Purveyor, Sioux, Spinnaker, Spinner, SuperWeb, TECWeb, W4, Web Commander, WebServer400, WebSite, WebSite Pro, WebSTAR 95/NT, WebSTAR Mac, Webware Comm, WN, Zeus
Pot ascunde părți din document bazate pe reguli de securitate	CL-HTTP, Commerce Builder, GoServe, Microsoft IIS, Netscape Enterprise, Netscape FastTrack, Purveyor, Spinnaker, Spinner, TECWeb, W4, WebServer400, Webware Comm, WN, Zeus
Regulile de securitate pot fi bazate pe URL	Alibaba, CL-HTTP, Commerce Builder, Esplanade, Esplanade Secure, ExpressO, FolkWeb, GNNserver, GoServe, IBM Connection, IBM Connection Secure, Jazz, MacHTTP, Microsoft IIS, Netscape Enterprise, Netscape FastTrack, Open Market Secure, Open Market WebServer, Purveyor, Sioux, Spinnaker, Spinner, SPRY SafetyWeb, SPRYWeb, SuperWeb, TECWeb, W4, WebServer400, WebSite, WebSite Pro, WebSTAR Mac, Webware Comm, WN, Zeus
Modelul de securitate implicită pentru fișiere bazate pe documente	**Permit accesul la toate fișierele în afară de cele aflate în lista de acces:** Alibaba, Apache, ApacheSSL, Esplanade, Esplanade Secure, ExpressO, IBM Connection, IBM Connection Secure, Jazz, MacHTTP, Microsoft IIS, NCSA, NetWare Web, Netscape Enterprise, Netscape FastTrack, Open Market Secure, Open Market WebServer, Purveyor, SPRY SafetyWeb, SPRYWeb, Sioux, Spinner, SuperWeb, WebSTAR Mac, WebServer400; **Interzic accesul la toate fișierele în afară de cele aflate în lista de acces:** Commerce Builder, DECthreads, EnterpriseWeb, FolkWeb, GN, Spinnaker, W4, WN, Webware Comm, Zeus; **Nu permit accesul la fișiere sistem**: COSMOS, TECWeb.
Permisiuni de tip ierarhic pentru directoare și documente	Alibaba, Apache, ApacheSSL, CL-HTTP, Commerce Builder, EnterpriseWeb, Esplanade, Esplanade Secure, ExpressO, GN, GNNserver, Jazz, Microsoft IIS, NCSA, Netscape Enterprise, Netscape FastTrack, NetWare Web, Open Market Secure, Open Market WebServer, Oracle, Purveyor, Sioux, Spinner, SPRY SafetyWeb, SPRYWeb, W4, Web Commander, WebServer400, WebSite, WebSite Pro, WebSTAR Mac, Webware Comm, Zeus

2. Prezentarea Sistemului Info Nuclear

Aplicația Info Nuclear este disponibilă pe un site din ICI.

Pagina de primire permite logarea. Pentru a avea acces la meniu, toți utilizatorii sunt nevoiți să se logheze.



Dacă se introduce greşit un nume sau o parolă, se afişează un mesaj de culoare roşie "Utilizatorul sau parola introduse sunt greşite". După logare, în partea dreaptă, apare numele utilizatorului logat. Dacă cineva doreşte să se înregistreze pentru a accesa informaţiile Info Nuclear, trebuie să se logheze prin click pe linkul User nou?

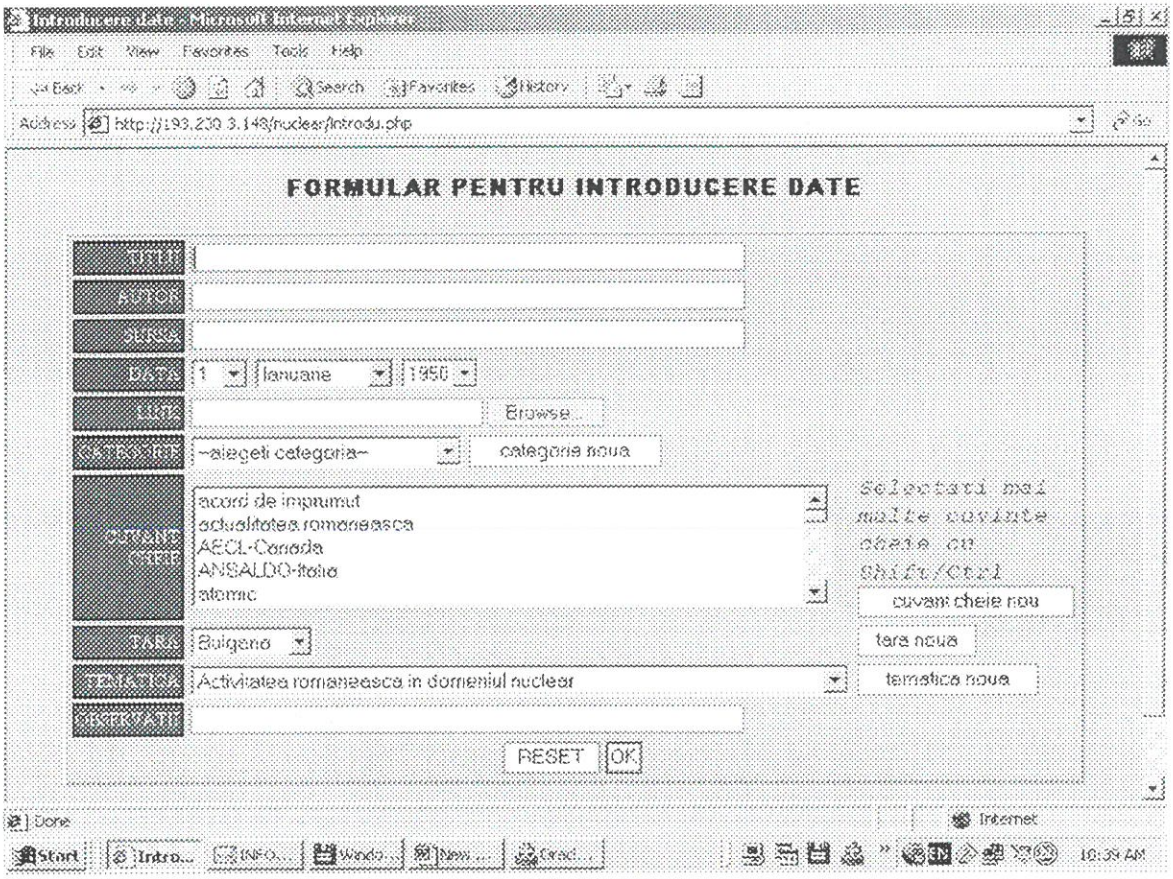
Va fi necesar să completeze formularul de înregistrare, în baza de date (toate câmpurile sunt obligatoriu de completat). Programul verifică dacă toate câmpurile formularului au fost completate, în caz contrar va afişa un mesaj "Vă rugăm să introduceţi prenumele (numele_câmpului)".

Meniul conţine 5 funcţii, 3 accesibile doar utilizatorilor autorizati de ICI:

- Introducere;
- Ştergere;
- Modificare;

şi 2 denumite Căutare şi Afişare, disponibile tuturor celor care s-au logat.

Pentru delogare, se poate apăsa pe Delogare şi se face redirecţionarea automat după o secundă la prima pagină. Formularul de Introducere date:



Pentru cuvinte cheie, ţară, tematică, se va alege din listă cele dorite. Pentru an sunt disponibile valori de la 1950 până la anul curent (2003), în anii care vor urma, lista se actualizează cu 2004, 2005 etc prin program, în mod automat. Pentru încărcarea pe server (de unde se va citi) a documentului se apasă browse pentru a se alege de pe calculatorul de unde se încarcă datele documentul dorit, care trebuie să fie tip permis, altfel se va avertiza (se poate întoarce pentru a alege un fişier valid). Se poate alege din lista disponibilă o categorie sau se poate introduce o categorie nouă, un cuvânt - cheie nou, o ţară nouă, o tematică nouă prin click pe butoanele corespondente.

Se pot alege mai multe cuvinte cheie (oricâte din listă) cu ajutorul tastelor Shift şi Ctrl şi a mouse-ului: dacă se ţine Shift apăsat prin click, se selectează cuvinte cheie consecutive; dacă se ţine Ctrl apăsat prin click, se selectează cuvinte cheie unul câte unul. Dacă nu se introduce nici un criteriu de căutare, utilizatorul este atenţionat prin mesaj. Există 2 criterii de căutare: TOATE şi ORICARE.

Pentru "Ştergere" accesibilă din meniu, se face căutarea ca mai sus a titlului care se doreşte a fi şters, se face click pe *Stergere*

Apare mesajul de avertizare:

Sunteţi sigur că doriţi să ştergeţi?

OK Cancel

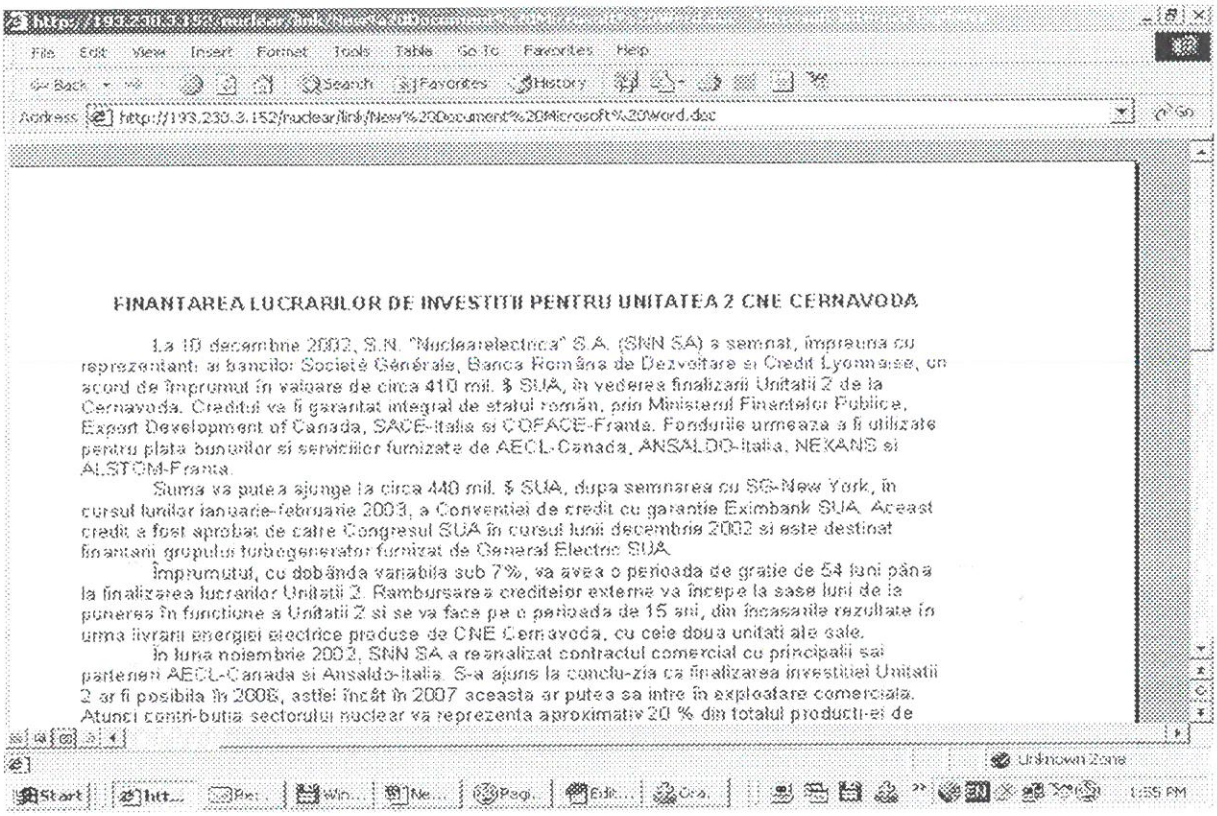
- dacă se apasă OK, se va şterge respectiva înregistrare şi se poate reîntoarce la cautare prin "Înapoi la căutare pentru ştergere";
- dacă se apasă Cancel, nu se va şterge.

Modificarea este disponibilă din meniu prin click pe modificarea dorită: "Modificare CUVÂNT CHEIE" sau "Modificare TEMATICĂ" sau "Modificare ŢARĂ" sau "Modificare CATEGORIE". Se va alege un cuvânt cheie care urmează a fi modificat din lista disponibilă şi un cuvânt modificat, altfel, veţi fi avertizat prin mesaj "Vă rugăm să alegeţi un cuvânt cheie care urmează a fi modificat".

Programul verifică dacă sunt introduse date în ambele câmpuri, altfel, avertizează prin mesaj "Vă rugăm să alegeţi Cuvântul Cheie care urmează a fi modificat". Dacă exista deja cuvântul cheie modificat se avertizează. Se

poate face întoarcere la modificare sau renunțare (redirectare la meniu). Similar pentru Tematică, Țară, Categorie, Afișare disponibil din meniu afișează titlurile disponibile.

Accesarea *"Citire document"* permite citirea propriu - zisă a respectivului document, de exemplu:



FINANTAREA LUCRARILOR DE INVESTITII PENTRU UNITATEA 2 CNE CERNAVODA

La 10 decembrie 2002, S.N. "Nuclearelectrica" S.A. (SNN SA) a semnat, impreuna cu reprezentanti ai bancilor Societe Generale, Banca Romana de Dezvoltare si Credit Lyonnaise, un acord de imprumut in valoare de circa 410 mil. $ SUA, in vederea finalizarii Unitatii 2 de la Cernavoda. Creditul va fi garantat integral de statul roman, prin Ministerul Finantelor Publice, Export Development of Canada, SACE-Italia si COFACE-Franta. Fondurile urmeaza a fi utilizate pentru plata bunurilor si serviciilor furnizate de AECL-Canada, ANSALDO-Italia, NEKANS si ALSTOM-Franta.

Suma va putea ajunge la circa 440 mil. $ SUA, dupa semnarea cu SG-New York, in cursul lunilor ianuarie-februarie 2003, a Conventiei de credit cu garantie Eximbank SUA. Acest credit a fost aprobat de catre Congresul SUA in cursul lunii decembrie 2002 si este destinat finantarii grupului turbogenerator furnizat de General Electric SUA.

Imprumutul, cu dobanda variabila sub 7%, va avea o perioada de gratie de 54 luni pana la finalizarea lucrarilor Unitatii 2. Rambursarea creditelor externe va incepe la sase luni de la punerea in functiune a Unitatii 2 si se va face pe o perioada de 15 ani, din incasarile rezultate in urma livrarii energiei electrice produse de CNE Cernavoda, cu cele doua unitati ale sale.

In luna noiembrie 2002, SNN SA a realizat contractul comercial cu principalii sai parteneri AECL-Canada si Ansaldo-Italia. S-a ajuns la concluzia ca finalizarea investitiei Unitatii 2 ar fi posibila in 2008, astfel incat in 2007 aceasta ar putea sa intre in exploatare comerciala. Atunci contri-butia sectorului nuclear va reprezenta aproximativ 20 % din totalul productiei de

Bibliografie

1. **MIKULA, N.**: Schemas take DTDs to the next level, 2000.
2. **PILAT, V. ş. a.**: Introducere în Internet, Editura Teora, Bucureşti, 1995.
3. **MURRY, W.H. III, PAPPAS, C.**: Application Programming for Windows NT, Osborne McGraw-Hill.
4. * * * Tehnica programării calculatoarelor. Căutare şi Sortare.
5. **PATRICIU, V. V.:** Criptografia şi securitatea reţelelor de calculatoare cu aplicaţii în C şi Pascal, Editura Tehnică, Bucureşti, 1994.
6. **PATRICIU, V., ENE-PIETROŞANU, M., CRISTEA, C., BICA, C.**: Securitatea în UNIX şi Internet, Editura Tehnică, Bucureşti.
7. * * * Random Oracles are Practical: a paradigm for designing efficient protocols. În: Proc. of the 1st ACM Conference on Computer and Communications Security, 1993, pp. 62-73.
8. **POINTCHEVAL, D.**: Security Proofs for Signature Schemes. În: Proc. of EUROCRYPT'96, vol 1070, Springer-Verlag, 1996, pp. 387-398.
9. **STERN, J.:** Advances in Cryptology. În: Proc. of EUROCRYPT'96, vol 1070, Springer Verlag, 1996, pp. 387-398.
10. **VAUDENAY, S.**: Hidden Collissions on DSS, Advances in Cryptology. În: Proc. of CRYPTO'96, Springer Verlag, 1996.
11. **CRISTEA, V., GODZA, G., ZABALAN, V., BELEA, E., ACHIM, O., ISPIR, T.:** Platforme Web pentru comerț electronic, Modele conceptuale de comert electronic.
12. **BULÂCEANU, C.**: Rețele locale de calculatoare, Editura Tehnică, Bucuresti 1995.