



MD 1871 G2 2002.02.28

REPUBLICA MOLDOVA



(19) Agenția de Stat
pentru Protecția Proprietății Industriale

(11) 1871⁽¹³⁾ G2
(51) Int. Cl.⁷: G 06 F 12/14;
H 04 K 1/00

(12) BREVET DE INVENȚIE

(21) Nr. depozit: a 2000 0155 (22) Data depozit: 2000.07.28	(45) Data publicării hotărârii de acordare a brevetului: 2002.02.28, BOPI nr. 2/2002
(71) Solicitant: Compania DEKART, S.R.L., MD (72) Inventatori: OLEINIK Weacheslaw, MD; ANESTIADI Valerii, MD; PETROVA Olga, MD (73) Titular: Compania DEKART, S.R.L., MD (74) Reprezentant: JENICOVSCAIA Galina, MD	

(54) Procedeu de protecție contra copierii bazelor de date și a programelor
pentru calculator

(57) Rezumat:

1
Protecția bazelor de date și a programelor
pentru calculator se obține prin asigurarea fiecărui
utilizator al pachetului de programe pentru
calculator sau al bazelor de date cu un dispozitiv
5 electronic de protecție extern, care trebuie conectat
la calculatorul utilizatorului. Acest dispozitiv
electronic extern se folosește pentru păstrarea unei
părți a codului (și/sau datelor) programului sau al
10 bazei de date care se protejează. Partea codului
(datelor) care se păstrează în dispozitivul electronic
extern se execută de procesorul propriu, totodată
executarea (transmiterea) codului nu poate fi

2
începută înainte de introducerea în dispozitivul
extern a unui cod-cheie special. Codul-cheie
special este creat de program în memoria de lucru a
calculatorului prin transformarea criptografică a
datelor aleatorii, create de dispozitivul extern și
transmise de el în memoria de lucru a
calculatorului.
10 Rezultatul invenției constă în sporirea fiabili-
tății protecției bazelor de date și a programelor
pentru calculator contra copierii lor neautorizate.
Revendicări: 3

MD 1871 G2 2002.02.28

3

Descriere:

Invenția se referă la dispozitive electronice de protecție a programelor și a bazelor de date pentru calculator contra copierii nesancționate. În invenție figurează următorii termeni:

5 **descifrare** – transformare criptografică, scopul căreia este deschiderea conținutului unui volum de date cifrat mai înainte;

cifrare – transformare criptografică, scopul căreia este ascunderea conținutului unui volum de date;

10 **cheie** – succesiune a simbolurilor, care determină starea unor parametri ai algoritmului transformării criptografice și care asigură alegerea unei transformări din totalitatea transformărilor criptografice posibile pentru algoritmul dat al transformării;

transformare criptografică – transformarea unui volum dat de informație, scopul căreia este ascunderea conținutului acestei informații, prevenirea schimbării ei sau a folosirii ei nesancționate;

15 **criptoanaliză** – calcularea cheii secrete pentru obținerea accesului nesancționat la informația cifrată sau elaborarea procedurii, care asigură accesul la informația cifrată fără calcularea cheii secrete;

criptoanalist – persoană, care îndeplinește criptoanaliza;

smart – cartelă – cartelă cu circuit integrat, care include microprocesor.

20 Este cunoscut procedeul de protecție a programelor pentru calculator contra folosirii lor fără autorizare, declarat în brevetul [1]. Procedeul include faze de cifrare, cel puțin a unei părți a programelor pentru calculator, care se protejează. Totodată cifrarea se efectuează conform algoritmului unu, iar descifrarea părții cifrate a programelor pentru calculator se efectuează conform algoritmului doi. Algoritmul doi împreună cu cheia, care se folosește pentru descifrarea părții programelor pentru calculator care a fost cifrată, se păstrează într-un dispozitiv extern, adaptat pentru conectare cu calculatorul, totodată dispozitivul extern conține cel puțin un mediu de memorizare, care se citește de către calculator și un procesor propriu. O particularitate distinctivă a procedurii este aceea că descifrarea conform algoritmului doi (g2) se efectuează cu ajutorul cheii doi (k2), care se păstrează în dispozitiv extern, totodată cheia doi se deosebește de cheia unu (k1), care se folosește în procesul cifrării părții programelor pentru calculator indicate conform algoritmului unu (g1).

30 Cifrarea părții programelor pentru calculator indicate conform algoritmului unu (g1) se efectuează prin cifrarea codului inițial al programelor pentru calculator corespunzătoare până la compilarea și redactarea legăturilor, sau în procesul fazelor analogice de prelucrare, care formează un program executabil, și în același timp la biblioteca datelor se adaugă un cod de obiect, care se referă la procesul schimbului cu dispozitiv extern.

35 Descifrarea părții programelor de calculator cifrate, care se efectuează conform algoritmului doi (g2), se realizează atunci, când calculatorul în procesul executării programelor pentru calculator indicate găsește consecutivitatea apelului sau o comandă analogică, care provoacă trecerea în punct corespunzător de intrare în cod de obiect adăugat indicat, cu care se instalează un canal de schimb între calculator și dispozitivul extern cu folosirea codului de obiect adăugat. Prin acest canal de schimb partea cifrată a programelor pentru calculator se transmite în prima fază de transmitere în dispozitivul extern pentru descifrarea cu ajutorul procesorului propriu al dispozitivului, după ce partea descifrată a programelor pentru calculator se prelucrează în dispozitivul extern, iar rezultatul prelucrării se transmite în a doua fază a transmiterii în direcția opusă pentru folosirea ulterioară în calculator.

45 Procedeul dat asigură protecția programelor pentru calculator, însă are un șir de dezavantaje. Mai întâi, el nu este practic, fiindcă efectuarea cifrării codului programului este necesar de a se realiza înainte de compilarea și redactarea legăturilor sau în timpul îndeplinirii acestor procese.

50 Dezavantajul principal al procedurii este acela că în procesul executării programelor pentru calculator sunt introduse două faze de transmitere a părții programelor pentru calculator (de la calculator în dispozitiv și de la dispozitiv în calculator) și descifrarea acestei părți în dispozitivul extern, ceea ce în măsură semnificativă reduce viteza executării programelor pentru calculator care se protejează.

55 Este cunoscut de asemenea și un alt procedeu și dispozitiv de protecție a programelor pentru calculator contra copierii, care folosesc apel și răspuns pentru prevenirea executării neautorizate a programelor pentru calculator [2], care include mijloace de interpelare, legate cu programe pentru calculator protejate și mijloace pentru răspuns, în care cheia secretă a utilizatorului se păstrează în siguranță și în care:

MD 1871 G2 2002.02.28

4

a) mijloacele de interelare nu au acces la cheia secretă a utilizatorului și includ mijloace de generare a interelării și de transmitere a interelării menționate mijloacelor de răspuns;

b) mijloacele de răspuns includ mijloace de semnare a interelării menționate cu folosirea cheii secrete a utilizatorului și întoarcere a interelării semnate mijloacelor de interelare, și

5 c) mijloacele de interelare includ mijloace de verificare a interelării semnate menționate cu folosirea cheii deschise a utilizatorului și prevenire a executării unor sau tuturor unităților de programe pentru calculator, dacă verificarea menționată nu a fost reușită.

Însă acest procedeu are un dezavantaj semnificativ, care constă în aceea că mijloacele de interelare, verificare și luare a deciziei se găsesc în modulul de program ca atare și pot fi găsite și „neutralizate” de către infractor. De fapt, aceste mijloace reprezintă o parte a programului (codului) și, din această cauză, ascunderea lor cu o siguranță suficientă în realitate nu este posibilă.

10 Cel mai apropiat după esența tehnică de procedeu solicitat de protecție contra copierii bazelor de date și a programelor pentru calculator este procedeu și dispozitivul [3], în care protecția programelor pentru calculator se obține prin asigurarea fiecărui utilizator al pachetului de programe cu un dispozitiv electronic de protecție, care trebuie să fie conectat la calculatorul utilizatorului. Programul protejat trimite semnale codificate de interelare la dispozitivul electronic de protecție care prelucrează semnalele de interelare și transmite semnale codificate de răspuns programului. Programul nu va fi executat până ce nu va identifica semnalele de răspuns în conformitate cu criteriul de protecție ales în prealabil. Acest procedeu folosește memoria de lucru și programul, 15 păstrat în memoria menționată, totodată procedeu include în combinație următoarele acțiuni:

20 a) încărcarea programului în memoria de lucru menționată, totodată programul include comenzi pentru:

1) generarea semnalelor codificate de interelare alese în prealabil,

2) evaluarea semnalelor de răspuns, și

25 3) generarea semnalelor de comandă în conformitate cu criteriul de protecție ales în prealabil;

b) inițializarea executării programului menționat;

30 c) transmiterea semnalelor codificate de interelare menționate din memoria menționată în dispozitivul electronic de protecție menționat, care prelucrează semnalele primite în mod automat și, în afară de aceasta, generează răspuns codificat;

d) transmiterea semnalelor codificate de răspuns menționate în memoria menționată; și generarea semnalelor de comandă din memoria menționată, care forțează calculatorul menționat de a opri executarea programului menționat numai în cazul în care semnalul de răspuns menționat nu satisface criteriul de protecție ales în prealabil.

35 Însă și acest procedeu posedă același dezavantaj semnificativ ca și procedeu [2], care constă în aceea că mijloacele de interelare, verificare și primire a deciziei se găsesc în modulul programului care se protejează ca atare și pot fi găsite și „neutralizate” de către infractor.

Problema pe care o rezolvă invenția este elaborarea unui procedeu care ar permite asigurarea protecției sigure a bazelor de date și a programelor pentru calculator contra copierii și folosirii lor neautorizate cu reducerea minimă a vitezei de executare a programelor care se protejează.

40 Esența invenției constă în aceea că procedeu de protecție contra copierii bazelor de date și a programelor pentru calculator ce include conectarea unui dispozitiv electronic extern de protecție la calculator, care conține memorie de lucru și program ce se păstrează în memoria menționată, încărcarea programului în memoria de lucru a calculatorului, inițierea executării programului menționat, transmiterea semnalelor codificate de interogare din memoria de lucru a calculatorului în dispozitivul extern de protecție, prelucrarea în mod automat a semnalelor recepționate, generarea și transmiterea semnalelor codificate de răspuns în memoria de lucru a calculatorului, în care o parte a codului (și/sau a datelor) programului sau bazei de date care se protejează se păstrează în memoria dispozitivului electronic extern de protecție și este inaccesibilă 45 până la introducerea în dispozitivul extern a unui cod-cheie special.

50 Problema constă de asemenea în asigurarea unui sistem de protecție de așa fel, în care fiecărui utilizator se permite crearea unui număr nelimitat de copii ale pachetului de programe cumpărate legitim, însă în care aceste copii nu pot fi folosite în calculatoare, care aparțin părților terțe neautorizate.

55 Problema se soluționează prin aceea că în procedeu de protecție contra copierii bazelor de date și a programelor pentru computer, care constă în aceea că se folosește un dispozitiv extern de protecție, care se conectează cu calculatorul, ce are memoria de lucru și program, care se păstrează în memoria menționată, și include următoarele acțiuni:

MD 1871 G2 2002.02.28

5

- încărcarea programului în memoria menționată;
 - inițializarea executării programului menționat;
 - transmiterea semnalelor codificate de interpelare din memoria de lucru menționată în dispozitivul extern de protecție menționat, care prelucrează în mod automat semnalele recepționate și generează semnale codificate de răspuns;
 - transmiterea semnalelor codificate menționate în memoria de lucru menționată;
- o parte a codului (și/sau a datelor) programului (sau bazei de date) care se protejează se păstrează în memoria dispozitivului extern menționat și este inaccesibilă înainte de introducerea în dispozitivul extern menționat a unui cod-cheie special.

Problema în privința protecției programelor pentru calculator se rezolvă de asemenea prin aceea că partea codului programului menționat, care se găsește în dispozitivul extern menționat, totodată executarea nu poate fi începută înainte de introducerea în dispozitivul extern menționat a codului-cheie special menționat.

Problema se rezolvă de asemenea prin aceea că în calitate de cod-cheie special menționat se folosește un cod, care se creează de către programul menționat în memoria de lucru a calculatorului menționată prin mijlocul transformării criptografice a datelor aleatorii, care se creează de către dispozitivul extern menționat și sunt transmise de către el în memoria de lucru a calculatorului menționată.

Rezultatul invenției solicitate este asigurarea protecției bazelor de date și programelor pentru calculator contra copierii și folosirii lor neautorizate cu reducerea minimă a vitezei executării programelor care se protejează.

Procedul se realizează în felul următor.

În procedeul de protecție contra copierii bazelor de date și a programelor pentru calculator conform invenției solicitate fiecare pachet de programe cumpărat legitim este aprovizionat cu un dispozitiv electronic de protecție extern.

În timpul executării programului, încărcat în memoria de lucru a calculatorului, el generează semnale codificate de interpelare, care se transmit în dispozitivul extern de protecție.

Dispozitivul electronic extern de protecție se folosește pentru păstrarea unei părți a codului programului, care se găsește în memoria de lucru a dispozitivului. Dispozitivul extern menționat posedă un procesor propriu, care poate fi folosit pentru executarea părții codului programului, care se găsește în memoria de lucru a procesorului menționată.

Dacă dispozitivul electronic extern de protecție este corect, adică livrat utilizatorului împreună cu programul, atunci el identifică semnalele de interpelare, prelucrează datele primite în interpelare sau execută partea codului programului, care se găsește în memoria de lucru a dispozitivului de protecție și transmite datele răspunsului convenite în memoria de lucru a calculatorului.

Accesul la memoria de lucru a dispozitivului extern este limitat și se permite după introducerea unui cod-cheie special în dispozitivul extern. Acest cod-cheie special se introduce de către utilizator – posesorul legitim al programelor pentru calculator. După aceasta partea codului programului menționat și datele, amplasate în memoria de lucru a dispozitivului, devin accesibile pentru executarea și prelucrarea cu ajutorul procesorului propriu al dispozitivului extern.

În calitate de cod-cheie special menționat poate fi folosit de asemenea un cod, care se creează de către program, care se păstrează în memoria de lucru a calculatorului, prin mijlocul transformării criptografice a datelor aleatorii, care se creează de către dispozitivul extern și sunt transmise în memoria de lucru a calculatorului pentru transformare. După transformarea criptografică a datelor aleatorii în memoria calculatorului ele se transmit în calitate de cod-cheie special menționat în dispozitivul extern.

Și numai în cazul în care programele pentru calculator în memoria de lucru o să primească date convenite de la dispozitivul extern, executarea programului va evolua pe cale corectă. În cazul în care datele convenite de răspuns nu vor fi primite de către memoria de lucru a calculatorului, care conține programul, atunci programul nu va fi executat de către calculator.

În cazul în care obiectul care se protejează este baza de date pentru calculator, dispozitivul extern se folosește pentru păstrarea codului, care realizează transformarea criptografică a datelor de indice (fișiere) ale bazei protejate. Baza de date trebuie să fie construită în așa fel, încât lipsa datelor de indice (fișierelor) să nu dea posibilitate de a folosi baza de date și numai datele de indice (fișiere) primite de la dispozitivul extern să asigure această posibilitate.

Deoarece producătorul programului livrează dispozitivul extern fiecărui utilizator împreună cu fiecare program cumpărat aparte, fiecare utilizator poate să creeze copii de rezervă ale programului

MD 1871 G2 2002.02.28

6

cumpărat legitim și să le folosească pe calculator cu dispozitivul de protecție extern, care a fost livrat împreună cu pachetul de programe cumpărat, conectat cu el.

5 La calculatorul, care nu este conectat la dispozitivul electronic de protecție extern, nu pot fi executate copii. Deși teoretic este posibil de a crea o copie nelegitimă (emulator) a dispozitivului electronic de protecție extern, prețul, consumul de timp și dificultatea “extragerii” programului și cheilor din dispozitiv sunt o dificultate mai mare decât cumpărarea programului de la producător. Mai mult decât atât, fiecare dispozitiv extern, legat cu pachetul de programe dat, este unic și falsificarea lui (emularea) nu este utilă pentru un alt pachet de programe ale aceluiași producător.

10

(57) Revendicări:

15 1. Procedeu de protecție contra copierii bazelor de date și a programelor pentru calculator ce include conectarea unui dispozitiv electronic de protecție extern la calculator, care conține memorie de lucru și program ce se păstrează în memoria menționată, încărcarea programului în memoria de lucru a calculatorului, inițierea executării programului menționat, transmiterea semnalelor codificate de interogare din memoria de lucru a calculatorului în dispozitivul extern de protecție, prelucrarea în mod automat a semnalelor recepționate, generarea și transmiterea
20 semnalelor codificate de răspuns în memoria de lucru a calculatorului, **caracterizat prin aceea că** o parte a codului (și/sau a datelor) programului sau bazei de date care se protejează se păstrează în memoria dispozitivului electronic extern de protecție și este inaccesibilă până la introducerea în dispozitivul extern a unui cod-cheie special.

25 2. Procedeu, conform revendicării 1, **caracterizat prin aceea că** partea de cod al programului se execută de către procesorul care se conține în dispozitivul electronic extern.

30 3. Procedeu, conform revendicărilor 1 și 2, **caracterizat prin aceea că** în calitate de cod-cheie special se folosește codul care se creează de către program în memoria de lucru a calculatorului prin transformarea criptografică a datelor aleatorii create de dispozitivul electronic extern și transmise de el în memoria de lucru a calculatorului.

(56) Referințe bibliografice:

1. WO 97/03398 A
2. US 5935246 B
3. US 4446519 B

Șef Secție:

COZMA Valeriu

Examinator:

NASTAS Xenia

Redactor:

CANȚER Svetlana

RAPORT DE DOCUMENTARE

(21) Nr. depozit: a 2000 0155	(85) Data fazei naționale PCT:
(22) Data depozit: 2000.07.28	(86) Cerere internațională PCT:
Prioritatea invocată : (31) nr.: 32) data : 33) țara : (51) Int. Cl. (7) : G 06 F 12/14; H 04 K 1/00 Alți indici de clasificare: (54) Titlul : Procedeu de protecție contra copierii bazelor de date și a programelor pentru calculator. (71) Solicitantul : Compania DEKART, S.R.L., MD Termeni caracteristici : procedeu de protecție contra copierii bazelor de date și a programelor pentru calculator	
I. Minimul de documente consultate (sistema clasificării și indicii de clasificare)	
C.I.B. 7: MD 1994-2000 EA 1996-2000	
II. Documente considerate ca relevante	
Categoria*	Date de identificare ale documentelor citate si indicarea pasajelor pertinente
-	-
☐ Documentele următoare sunt indicate în continuare a rubricii II	
☐ Informația referitoare la brevete paralele se anexează	
* categoriile speciale ale documentelor consultate:	
A - document care definește statutul general al tehnicii	P - document publicat înainte de data depozitului național reglementat dar după data priorității invocate
E - document anterior dar publicat la data de depozit național reglementar sau după aceasta data	T - document publicat după data depozitului sau a priorității invocate, care nu aparține stadiului pertinent al tehnicii, dar care este citat pentru a pune în evidența principiul sau teoria care conține baza invenției
L - document care poate pune în discuție data priorității invocate, poate contribui la data publicării altor divulgări sau pentru un motiv expres (se va indica motivul)	X - document de relevanță deosebită: invenția revendicată nu poate fi considerată nouă sau implicând activitate inventivă
O - document referitor la o divulgare orală, un act de folosire, la o expunere sau orice altă	Y - document de relevanță deosebită: invenția revendicată nu poate fi considerată ca implicând activitate inventivă când documentul este asociat cu unul sau mai multe alte documente de aceeași natură, aceasta combinație fiind evidentă pentru o persoană de specialitate
	& - document care face parte din aceeași familie de documente
Data efectuării documentării 2001.08.13	
Examinatorul Xenia Nastas	

ANEXĂ la RAPORTUL DE DOCUMENTARE

Informația referitoare la brevete paralele		(21) Nr. depozit:	
Date de identificare ale documentelor citate în raport	Data publicării	Brevete paralele	Data publicării
1	2	3	4