MD 1871 F1 2002.02.28

REPUBLICA MOLDOVA

(19) Agenţia de Stat
pentru Protecţia Proprietăţii Industriale

(11) 1871 (13) F1
(51) Int. Cl.[7]: G 06 F 12/14;
H 04 K 1/00

(12) BREVET DE INVENŢIE

Hotărârea de acordare a brevetului de invenţie poate fi revocată în termen de 6 luni de la data publicării

(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 Weaceslaw, MD; ANESTIADI Valerii, MD; PETROVA Olga, MD
(73) Titular: Compania DEKART, S.R.L., MD
(74) Reprezentant: JENICICOVSCAIA Galina, MD

(54) Procedeu de protecţie contra copierii bazelor de date şi a programelor pentru calculator

(57) Rezumat:

1

Protecţia bazelor de date şi a programelor pentru calculator se obţine prin asigurarea fiecărui utilizator al pachetului de programe pentru calculator sau al bazelor de date cu un dispozitiv electronic de protecţie extern, care trebuie conectat la calculatorul utilizatorului. Acest dispozitiv electronic extern se foloseşte pentru păstrarea unei părţi a codului (şi/sau datelor) programului sau al 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 începută înainte de introducerea în dispozitivul

2

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 şi transmise de el în memoria de lucru a calculatorului.

Rezultatul invenţiei constă în sporirea fiabilităţii protecţiei bazelor de date şi a programelor pentru calculator contra copierii lor neautorizate.

Revendicări: 3

MD 1871 F1 2002.02.28

Descriere:

Invenţia se referă la dispozitive electronice de protecţie a programelor şi a bazelor de date pentru calculator contra copierii nesancţionate. În invenţie figurează următorii termeni:

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

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

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

transformare criptografică – transformarea unui volum dat de informaţie, scopul căreia este ascunderea conţinutului acestei informaţii, prevenirea schimbării ei sau a folosirii ei nesancţionate;

criptoanaliză – calcularea cheii secrete pentru obţinerea accesului nesancţionat la informaţia cifrată sau elaborarea procedeului, care asigură accesul la informaţia cifrată fără calcularea cheii secrete;

criptoanalist – persoană, care îndeplineşte criptoanaliza;

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

Este cunoscut procedeul de protecţie a programelor pentru calculator contra folosirii lor fără autorizare, declarat în brevetul [1]. Procedeul include faze de cifrare, cel puţin a unei părţi a programelor pentru calculator, care se protejează. Totodată cifrarea se efectuează conform algoritmului unu, iar descifrarea părţii cifrate a programelor pentru calculator se efectuează conform algoritmului doi. Algoritmul doi împreună cu cheia, care se foloseşte pentru descifrarea părţii programelor pentru calculator care a fost cifrată, se păstrează într-un dispozitiv extern, adaptat pentru conectare cu calculatorul, totodată dispozitivul extern conţine cel puţin un mediu de memorizare, care se citeşte de către calculator şi un procesor propriu. O particularitate distinctivă a procedeului 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 deosebeşte de cheia unu (k1), care se foloseşte în procesul cifrării părţii programelor pentru calculator indicate conform algoritmului unu (g1).

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

Descifrarea părţii programelor de calculator cifrate, care se efectuează conform algoritmului doi (g2), se realizează atunci, când calculatorul în procesul executării programelor pentru calculator indicate găseşte 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 şi 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 direcţia opusă pentru folosirea ulterioară în calculator.

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

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

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

a) mijloacele de interpelare nu au acces la cheia secretă a utilizatorului şi includ mijloace de generare a interpelării şi de transmitere a interpelării menţionate mijloacelor de răspuns;

b) mijloacele de răspuns includ mijloace de semnare a interpelării menţionate cu folosirea cheii secrete a utilizatorului şi întoarcere a interpelării semnate mijloacelor de interpelare, şi

c) mijloacele de interpelare includ mijloace de verificare a interpelării semnate menţionate cu folosirea cheii deschise a utilizatorului şi prevenire a executării unor sau tuturor unităţilor de programe pentru calculator, dacă verificarea menţionată nu a fost reuşită.

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

Cel mai apropiat după esenţa tehnică de procedeul solicitat de protecţie contra copierii bazelor de date şi a programelor pentru calculator este procedeul şi dispozitivul [3], în care protecţia programelor pentru calculator se obţine prin asigurarea fiecărui utilizator al pachetului de programe cu un dispozitiv electronic de protecţie, care trebuie să fie conectat la calculatorul utilizatorului. Programul protejat trimite semnale codificate de interpelare la dispozitivul electronic de protecţie care prelucrează semnalele de interpelare şi transmite semnale codificate de răspuns programului. Programul nu va fi executat până ce nu va identifica semnalele de răspuns în conformitate cu criteriul de protecţie ales în prealabil. Acest procedeu foloseşte memoria de lucru şi programul, păstrat în memoria menţionată, totodată procedeul include în combinare următoarele acţiuni:

a) Încărcarea programului în memoria de lucru menţionată, totodată programul include comenzi pentru:
   1) generarea semnalelor codificate de interpelare alese în prealabil,
   2) evaluarea semnalelor de răspuns, şi
   3) generarea semnalelor de comandă în conformitate cu criteriul de protecţie ales în prealabil;

b) iniţializarea executării programului menţionat;

c) transmiterea semnalelor codificate de interpelare menţionate din memoria menţionată în dispozitivul electronic de protecţie menţionat, care prelucrează semnalele primite în mod automat şi, în afară de aceasta, generează răspuns codificat;

d) transmiterea semnalelor codificate de răspuns menţionate în memoria menţionată; şi generarea semnalelor de comandă din memoria menţionată, care forţează calculatorul menţionat de a opri executarea programului menţionat numai în cazul în care semnalul de răspuns menţionat nu satisface criteriul de protecţie ales în prealabil.

Însă şi acest procedeu posedă acelaşi dezavantaj semnificativ ca şi procedeul [2], care constă în aceea că mijloacele de interpelare, verificare şi primire a deciziei se găsesc în modulul programului care se protejează ca atare şi pot fi găsite şi „neutralizate" de către infractor.

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

Esenţa invenţiei constă în aceea că procedeul de protecţie contra copierii bazelor de date şi a programelor pentru calculator ce include conectarea unui dispozitiv electronic extern de protecţie la calculator, care conţine memorie de lucru şi program ce se păstrează în memoria menţionată, încărcarea programului în memoria de lucru a calculatorului, iniţierea executării programului menţionat, transmiterea semnalelor codificate de interogare din memoria de lucru a calculatorului în dispozitivul extern de protecţie, prelucrarea în mod automat a semnalelor recepţionate, generarea şi transmiterea semnalelor codificate de răspuns în memoria de lucru a calculatorului, în care o parte a codului (şi/sau a datelor) programului sau bazei de date care se protejează se păstrează în memoria dispozitivului electronic extern de protecţie şi este inaccesibilă până la introducerea în dispozitivul extern a unui cod-cheie special.

Problema constă de asemenea în asigurarea unui sistem de protecţie de aşa 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 aparţin părţilor terţe neautorizate.

Problema se soluţionează prin aceea că în procedeul de protecţie contra copierii bazelor de date şi a programelor pentru computer, care constă în aceea că se foloseşte un dispozitiv extern de protecţie, care se conectează cu calculatorul, ce are memoria de lucru şi program, care se păstrează în memoria menţionată, şi include următoarele acţiuni:

- încărcarea programului în memoria menţionată;
- iniţializarea executării programului menţionat;
- transmiterea semnalelor codificate de interpelare din memoria de lucru menţionată în dispozitivul extern de protecţie menţionat, care prelucrează în mod automat semnalele recepţionate şi generează semnale codificate de răspuns;
- transmiterea semnalelor codificate menţionate în memoria de lucru menţionată;

o parte a codului (şi/sau a datelor) programului (sau bazei de date) care se protejează se păstrează în memoria dispozitivului extern menţionat şi este inaccesibilă înainte de introducerea în dispozitivul extern menţionat a unui cod-cheie special.

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

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

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

Procedeul se realizează în felul următor.

În procedeul de protecţie contra copierii bazelor de date şi a programelor pentru calculator conform invenţiei solicitate fiecare pachet de programe cumpărat legitim este aprovizionat cu un dispozitiv electronic de protecţie 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 protecţie.

Dispozitivul electronic extern de protecţie se foloseşte pentru păstrarea unei părţi a codului programului, care se găseşte în memoria de lucru a dispozitivului. Dispozitivul extern menţionat posedă un procesor propriu, care poate fi folosit pentru executarea părţii codului programului, care se găseşte în memoria de lucru a procesorului menţionată.

Dacă dispozitivul electronic extern de protecţie 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 găseşte în memoria de lucru a dispozitivului de protecţie şi transmite datele răspunsului cuvenite în memoria de lucru a calculatorului.

Accesul la memoria de lucru a dispozitivului extern este limitat şi 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 menţionat şi datele, amplasate în memoria de lucru a dispozitivului, devin accesibile pentru executarea şi prelucrarea cu ajutorul procesorului propriu al dispozitivului extern.

În calitate de cod-cheie special menţionat 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 şi 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 menţionat în dispozitivul extern.

Şi numai în cazul în care programele pentru calculator în memoria de lucru o să primească date cuvenite de la dispozitivul extern, executarea programului va evolua pe cale corectă. În cazul în care datele cuvenite de răspuns nu vor fi primite de către memoria de lucru a calculatorului, care conţine 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 foloseşte pentru păstrarea codului, care realizează transformarea criptografică a datelor de indice (fişiere) ale bazei protejate. Baza de date trebuie să fie construită în aşa fel, încât lipsa datelor de indice (fişierelor) să nu dea posibilitate de a folosi baza de date şi numai datele de indice (fişiere) 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

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

La calculatorul, care nu este conectat la dispozitivul electronic de protecţie extern, nu pot fi executate copii. Deşi teoretic este posibil de a crea o copie nelegitimă (emulator) a dispozitivului electronic de protecţie extern, preţul, consumul de timp şi dificultatea "extragerii" programului şi 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 şi falsificarea lui (emularea) nu este utilă pentru un alt pachet de programe ale aceluiaşi producător.

(57) Revendicări:

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

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

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

(56) Referinţe bibliografice:

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

Şef Secţie: COZMA Valeriu

Examinator: NASTAS Xenia

Redactor: CANŢER Svetlana

RAPORT DE DOCUMENTARE

(21) Nr. depozit: a 2000 0155	(85) Data fazei naţionale PCT:
(22) Data depozit: 2000.07.28	(86) Cerere internaţională PCT:

Prioritatea invocată :
(31) nr.: 32) data : 33) ţara :
(51) Int. Cl. (7) : G 06 F 12/14; H 04 K 1/00
Alţi indici de clasificare:
(54) **Titlul** : Procedeu de protecţie contra copierii bazelor de date şi a programelor pentru calculator.
(71) Solicitantul : Compania DEKART, S.R.L., MD
Termeni caracteristici : procedeu de protecţie contra copierii bazelor de date şi a programelor pentru calculator

I. Minimul de documente consultate (sistema clasificării şi 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	Numărul revendicării vizate
-	-	-

☐ **Documentele următoare sunt indicate în continuare a rubricii II**	☐ **Informaţia referitoare la brevete paralele se anexează**
*** categoriile speciale ale documentelor consultate:**	**P** - document publicat înainte de data depozitului naţional reglementat dar după data priorităţii invocate
A - document care defineşte statutul general al tehnicii	**T** - document publicat după data depozitului sau a priorităţii invocate, care nu aparţine stadiului pertinent al tehnicii, dar care este citat pentru a pune în evidenţa principiul sau teoria care conţine baza invenţiei
E - document anterior dar publicat la data de depozit naţional reglementar sau după aceasta data	**X** - document de relevanţă deosebită: invenţia revendicată nu poate fu considerată nouă sau implicând activitate inventivă
L - document care poate pune în discuţie data priorităţii invocate, poate contribui la data publicării altor divulgări sau pentru un motiv expres (se va indica motivul)	**Y** - document de relevanţă deosebită: invenţia revendicată nu poate fu considerată ca implicând activitate inventivă când documentul este asociat cu unul sau mai multe alte documente de aceiaşi natură, aceasta combinaţie fiind evidentă pentru o persoană de specialitate
O - document referitor la o divulgare orală, un act de folosire, la o expunere sau orice altă	**&** - document care face parte din aceiaşi 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 in raport	Data publicării	**Brevete paralele**	Data publicării
1	2	3	4