Invenţia se referă la tehnologiile informaţionale şi poate fi utilizată pentru protecţia contra falsificării documentelor de hârtie.

Sunt cunoscute documentele protejate printr-un cod numeric [1]. Cu toate acestea, documentul dat din cauza lipsei protecţiei informaţionale prin numeric, este uşor falsificat de către tructurile interesate.

Este cunoscut un document [2] selectat în calitate de prototip şi care conţine un semn de protecţie sub forma unui set de perforaţii obţinute printr-un proces cu descărcare electrică stocastic şi un cod numeric.

Cu toate acestea, documentul dat posedă un dezavantaj seminificativ. Pentru confirmarea autenticităţii acestuia este necesara adresare permanentă la baza de date centrală, în care fiecare set de perforaţii cu descărcare electrică este stocat cu numărul individual propriu.

Documentul de hârtie protejat criptografic propus conţine un semn de protecţie sub forma unui set de perforaţii produse printr-un proces cu descărcare electrică stocastic şi un cod numeric.

Drept particularitate a documentului de hârtie propus poate fi recunoscut faptul că acesta conţine suplimentar un cod de bare bidimensional conţine informaţii despre setul de perforaţii de pe semn, o informaţie succintă privind textul documentului şi codul numeric, semnate cu o semnătură digitală.

Este cunoscută utilizarea semnăturii digitale la protejarea documentelor electronice verticale. Cu toate acestea, abordarea dată a fost considerată inaplicabilă pentru protecţia documentelor de hârtie [3]. Aplicarea semnăturii electronice efemere pe obiectul material – un document de hârtie – este o chestiune separată.

Este cunoscut un procedeu de protecţie a documentelor [4] fără adresarea la baza de date centrală. Procedeul dat se bazează pe compararea documentului cu imaginea holografică a acestuia.

În calitate de prototip la examinarea procedeului de creare a documentului protejat criptografic este selectat procedeul de creare a documentului de hârtie protejat prin aplicarea pe acesta a unui semn fizic, obţinut printr-un proces cu descărcare electrică stocastic şi un cod numeric, scanarea şi, în caz de necesitate, introducerea acestei informaţii în baza de date [5].

Drept particularitate a procedeului propus poate fi faptul că imaginea digitală binară comprimată a semnului, şi informaţia succintă privind textul şi codul numeric sunt semnate cu o semnătură digitală (cheie închisă), imaginea semnată se transformă într-un cod de bare bidimensional şi se imprimă pe documentul dat în apropierea semnului.

În fig. 1, este prezentat un exemplu tipic al documentului 1, executate pe suport de hârtie şi conţinând, în afară de conţinutul principal (text, imagine, semnătură; imprimare), următoarele elemente de protecţie suplimentare:

- o zonă specială 2 pe documentul de hârtie 1; semnul de identificare 3, care reprezintă un set de orificii (perforaţii) de dimensiuni şi configuraţii arbitrare, executate prin perforarea electrică necontrolată (stocastică) multiplă a suportului de hârtie într-o zonă a documentului desemnată special pentru aceasta; semnul 3 este prevăzut cu un număr de identificare (4) care simplifică procesele de recuperare şi de identificare a acestuia;
- un cod de bare bidimensional (5), care conţine informaţii cu privire la parametrii distinctivi ai semnului 3, semnat cu semnătura digitală a emitentului – părţii autentificatoare P.

Emitent – partea care produce (editează, publică) un document legal.

În fig. 2 este prezentată schematic procedura de creare a documentului de hârtie protejat criptografic. Procedura se efectuează pe partea emitentului P, care doreşte să autentifice documentul de ieşire şi să-l protejeze contra posibilităţii de redactare (modificare) ulterioară neautorizată.

În schemă sunt reprezentate următoarele elemente:

1. Documentul, care urmează să fie protejat. Acesta poate fi orice doment cu conţinut arbitrar (text, desen, foto, etc.), executat pe suport de hârtie. De exemplu, acesta poate fu un document financiar, certificat, buletin de identitate, paşaport, etc.

6. Un dispozitiv cu descărcare electrică de înaltă tensiune pentru aplicarea unui semn de identificare pe suportul de hârtie al documentului (1) prin metoda perforării electrice necontrolate (stocastice).

7. Documentul, care conţine un semn de identificare, obţinut prin perforarea cu descărcare electrică necontrolată multiplă a suportului de hârtie în zona prestabilită. Semnul de protecţie 3 reprezintă un set de orificii de mărime şi configuraţie arbitrară. Fiecare semn 3 obţinut astfel este unic şi ireproductibil, deoarece procesul de creare a acestuia are un caracter necontrolabil (stocastic).

8. Un dispozitiv de scanare şi prelucrare. În calitate de astfel de dispozitiv poate fi unul dintre smartphone-urile, planşetele, calculatoarele de buzunar (PDA), produs în serie şi echipat cu o cameră digitală cu rezoluţia necesară şi un set de programe de aplicaţie pentru citirea şi prelucrarea imaginilor. De asemenea, este posibilă varianta de utilizare a unui calculator personal cu un scanner staţionar produs în serie conectat la acesta.

În componenţa dispozitivului de scanare şi prelucrare (8) intră următoarele elemente:

8.1. Procedura de scanare a semnului de protecţie, care asigură citirea semnului – obţinerea imagini binare codificate a semnului şi stocarea în memoria dispozitivului (8).

8.2. Imaginea binară digitalizată a semnului, stocată în memoria dispozitivului (8).

8.3. Procedura de comprimare a imaginii binare a semnului, care transformă imaginea binară iniţială a semnului (8.2), care posedă o anumită redundanţă informaţională într-un cod numeric mai compact X (8.4). Procedura de comprimare este realizată în scopul de a economisi memoria necesară pentru stocarea semnului în dispozitivul de prelucrare (8) şi accelerarea procedurilor de prelucrare ulterioare. Procedura de comprimare se efectuează fără pierderea informaţiilor cu privire la parametrii unui semn concret 3.

8.4. Codul compact H. Acesta poartă informaţii importante cu privire la parametrii semnului concret 3, dar, spre deosebire de imaginea binară a acestuia (8.2), posedă o redundanţă mult mai mică.
8.5. Procedura de semnare a codului numeric compact X (8.4) cu semnătura digitală a părţii autentificatoare P. Semnătura digitală certifică autenticitatea codului digital compact X.
(8.4) şi, prin urmare autenticitatea imaginii binare iniţiale a semnului de protecţie (8.2). Procedura de semnare digitală este descrisă prin următoarea expresie matematică:
S=DP (X)
unde X - este codul numeric compact, a cărui autenticitate este certificată; DP – transformarea criptografică asimetrică închisă, efectuată cu ajutorul cheiei închise a părţii autentificatoare P; S - rezultatul transformării criptografice; secvenţa binară.
8.6. Signatura S, care reprezintă rezultatul semnării codului numeric compact X cu cheia închisă a părţii autentificatoare P.
8.7. Procedura de codificare de bare, care asigură, transformarea signaturii obţinute S (8.6.) într-unul dintre codurile de bare convenţionate (5), de exemplu, într-un QR-cod bidimensional utilizat pe scară largă. Codificarea de bare este utilizată pentru a asigura posibilitatea reproducerii şi citirii ulterioare a acestei informaţii prin mijloace convenţionale.
9. Codul de bare, care poartă informaţii despre imaginea binară a semnului de protecţie (8.2), a cărui autenticitate este certificată de semnătura digitală a părţii autentificatoere P. Acesta este creat în dispozitivul de prelucrare (8) şi transmis la dispozitivul de imprimare (10).
10. Orice dispozitiv de imprimare produs în serie (imprimantă), care poate reproduce pe suportul de hârtie un cod de bare (5).
11. Documentul final, executat pe suport de hârtie, care conţine un semn de protecţie 3 şi codul de bare corespunzător 5, care confirmă autenticitatea originii semnului de protecţie 3.
La etapa iniţială, pe suportul de hârtie al documentului (1) care este supus protecţiei, prin intermediul unui dispozitiv cu descărcare electrică (6) se aplică un semn de protecţie unic şi ireproductibil 3. Apoi, semnul obţinut 3 este scanat cu ajutorul dispozitivului (8), prelucrat şi codificat prin acest dispozitiv efectuând secvenţa de proceduri descrise mai sus (8.1, 8.3, 8.5, 8,7). Drept rezultat se creează un cod de bare (5), care poartă informaţii despere parametrii caracteristici ai unui semn concret, a cărui autenticitate este certificată de partea autentificatoare.
P. Codul de bare obţinut (5) se imprimă de documentul de hârtie cu ajutorul dispozitivului de imprimare (10).
Documentul obţinut astfel (11), în afară de conţinutul aplicabil (text, desen, foto), conţine elemente de protecţie suplimentare aplicate pe suportul de hârtie al acestuia – semnul de identificare de protecţie ireproductibil unic 3 cu perforaţii, numărul de identificare 4 şi codul de bare corespunzător 5, care atestă autenticitatea originii semnului dat 3.
În fig. 3 este reprezentată schematic procedura de verificare a autenticităţii documentului protejat 11, care se efectuează pe partea verificatoare V (utilizatorul documentului).
În schemă sunt reprezentate următoarele elemente:
11. Documentul protejat, executat pe suport de hârtie. Documentul conţine în structura s-a următoarele elemente:
- conţinutul principal (text, desen, fotografii, etc.),
- semnul de identificare de protecţie unic 3, cu perforaţii,
- numărul de identificare 4,
- codul de bare 5, care corespunde semnului dat 3 şi atestă autenticitatea acestuia.
12. Dispozitivul de scanare şi prelucrare. În calitate de un astfel de dispozitiv poate servi unul dintre smartphone-urile, planşetele, calculatoarele de buzunar (PDA) produse în serie, echipat cu o cameră digitală cu rezoluţia necesară şi un set de programe de aplicaţie pentru citirea şi prelucrarea imaginilor. De asemenea, este posibilă varianta utilizării unui calculator personal cu un scanner staţionar produs în serie conectat la acesta.
În componenţa dispozitivului de scanare şi prelucrare (12) intră următoarele elemente:
12.1 Procedura de scanare a semnului de protecţie, similară cu procedura (8.1) din fig. 2. Aceasta asigură citirea mărcii – obţinerea imaginii binare codificate a semnului şi stocarea în memoria dispozitivului (12).
12.2. Imaginea binară digitalizată a semnului 3, stocată în memoria dispozitivului (12 şi similară cu elementul (8.2) din fig. 2.
12.3. Procedura de comprimare a imaginii binare a semnului, care transformă imaginea binară iniţială a semnului (12.2) într-un cod numeric mai compact X* (12.4). Similar cu procedura (8.3) din fig. 2.
12.4. Codul numeric compact X*, similar cu elementul (8.4) din fig, 2. Autenticitatea acestui cod este echivalentă cu autenticitatea semnului scanat 3. Autenticitatea codului numeric compact X* şi, prin urmare, autenticitatea semnului citit 3, este verificată în procesul efectuării procedurilor ulterioare.
12.5. Scanarea codului de bare, care poartă informaţii cu privire la imaginea binară a semnului de protecţie autentic 33, a cărui autenticitate este certificată de semnătură digitală a părţii autentificatoare P. Similar cu elementul (8.5) din fig. 2.
12.6. Procedura de decodare a codului de bare. Aceasta asigură citirea codului de bare şi stocarea lui în memoria dispozitivului (12).
12.7. In formaţia semnată digital de decodare a codului de bare, car asigură obţinerea signaturii S.
12.8. Signatura S, similară cu elementul (8.6) din fig. 2). conţine informaţia privind codul numeric autentic X semnată de către partea autentificatoare P.

12.9. Procedura de verificare (dezvăluire) a semnăturii digitale, care este descrisă prin următoarea expresie matematică:
X= EP (S).
unde X – este codul numeric compact autentic; EP – transformarea criptografică asimetrică deschisă, realizată cu ajutorul cheie deschise a părţii autentificatore P; S – signatura.
12.10. Codul numeric autentic obţinut C.
12.11. Operaţiunea de comparare bit cu bit (reaptă) a codului numeric compact X*, obţinut în urma citirii şi prelucrării semnului de pe document, cu codul numeric compact autentic X, care a fost semnat de către partea autentiticatoare P.
13. Decizia cu privire la autenticitatea documentului. Dacă codurile X* şi X coincid până la bit, atunci documentul este considerat autentic. Se realizează sub forma unui mesaj format de dispozitivul (12) şi destinat verificarea V.
La etapa iniţială partea verificatoare V (utilizatorul) primeşte un document 11 executat pe suport de hărtie şi având în afară de conţinutul principal un semn de protecţie 3, constând într-un set stocastic de perforaţii, un cod numeric 4 şi un cod de bare 5.
Cu ajutorul dispozitivului (12) utilizatorul scanează semnul de protecţie (12.1). Informaţia obţinută cu privire la semnul de protecţie se prelucrează cu ajutorul secvenţei de proceduri descrise mai sus (12.2, 12.3), realizate în componenţa dispozitivului 12. Drept rezultat cu ajutorul dispozitivului (12) se calculează şi se stochează în memorie codul numeric compact X* corespunzător semnului citit.
Apoi, cu ajutorul dispozitivului (12), utilizatorul scanează codul de bare (5). Informaţia obţinută privind codul de bare se prelucrează cu ajutorul secvenţei de proceduri descrise mai sus (12.5; 12.7, 12.9), realizare în dispozitivul (12). Drept rezultat, cu ajutorul dispozitivului (12) se calculează şi se stochează în memorie codul numeric compact X, autenticitatea cărui a fost anterior certificată de către partea P.
Codurile X* şi X se compară bit cu bit (treptat). Dacă acestea coincid, atunci documentul se consideră autentic şi se adoptă decizia cu privire la autenticitatea documentului 13.