



MD 956 Y 2015.09.30

REPUBLICA MOLDOVA



(19) Agenția de Stat
pentru Proprietatea Intelectuală

(11) **956** (13) **Y**
(51) Int.Cl: *H04L 9/00* (2006.01)
H04L 29/06 (2006.01)
H04K 1/00 (2006.01)

(12) BREVET DE INVENȚIE
DE SCURTĂ DURATĂ

În termen de 6 luni de la data publicării mențiunii privind hotărârea de acordare a brevetului de invenție de scurtă durată, orice persoană poate face opoziție la acordarea brevetului	
(21) Nr. depozit: s 2015 0017 (22) Data depozit: 2015.02.17	(45) Data publicării hotărârii de acordare a brevetului: 2015.09.30, BOPI nr. 9/2015
(71) Solicitant: SOCIETATEA CU RĂSPUNDERE LIMITATĂ "SIGURANȚĂ TRANZACȚII", MD (72) Inventatori: FLORESCU Alexandru-Ion, RO; DUDUICA Simon, RO (73) Titular: SOCIETATEA CU RĂSPUNDERE LIMITATĂ "SIGURANȚĂ TRANZACȚII", MD (74) Mandatar autorizat: JENICICOVSCAIA Galina	

(54) Metodă de prevenire a infracțiunii la solicitarea prestării de servicii prin intermediul rețelei Internet

(57) Rezumat:

1

Invenția se referă la metode de prevenire a fenomenului infracțional potențial existent la solicitarea din partea unui utilizator către furnizorul ce prestează servicii prin rețeaua Internet.

Metoda de prevenire a infracțiunii la solicitarea prestării de servicii prin intermediul rețelei Internet constă în aceea că la recepționarea semnalului-solicitare de la dispozitivul utilizatorului de către serverul furnizorului pentru descoperirea infractorului, serverul realizează o verificare activă,

2

solicitând de la utilizator datele accountului și suma de control a fișierului, de asemenea determinând datele specifice ale dispozitivului utilizatorului. În cazul imposibilității de identificare a datelor sus-numite, se stabilește o conexiune suplimentară între serverul furnizorului și dispozitivul utilizatorului, care execută o verificare pasivă, solicitând date suplimentare de autentificare.

Revendicări: 1

Figuri: 5

MD 956 Y 2015.09.30

(54) Method for offence prevention at the request of providing services by means of the Internet network

(57) Abstract:

1

The present invention relates to methods for preventing the potentially existing offence phenomenon at user's request to the service provider by means of the Internet network.

The method for offence prevention at the request of providing services by means of the Internet network consists in that upon entry of signal-request from the user device to the server of the provider to disclose the intruder, the server performs an active testing,

2

prompting the account data and fingerprint from the user, as well as identifying the specific data of user device. In case of failure to identify the above data, it is established a bypass connection between the server of the provider and the user device, which performs a passive testing, prompting additional authentication data.

Claims: 1

Fig.: 5

(54) Метод предотвращения правонарушения при запросе о предоставлении услуг посредством сети Интернет

(57) Реферат:

1

Изобретение относится к методам предотвращения потенциально существующего явления правонарушения при запросе со стороны пользователя к поставщику услуг посредством сети Интернет.

Метод предотвращения правонарушения при запросе о предоставлении услуг посредством сети Интернет состоит в том, что при поступлении сигнала-запроса с устройства пользователя на сервер провайдера для раскрытия злоумышленника, сервер осуществляет активную проверку, запрашивая у

2

пользователя данные аккаунта и контрольную сумму файла, а также определив специфические данные устройства пользователя. В случае невозможности идентификации вышеперечисленных данных, устанавливается дополнительное соединение между сервером провайдера и устройством пользователя, которое выполняет пассивную проверку, запрашивая дополнительные данные аутентификации.

П. формулы: 1

Фиг.: 5

Descriere:

Invenția se referă la metode de prevenire a fenomenului infracțional potențial existent la solicitarea din partea unui utilizator către furnizorul ce prestează servicii prin rețeaua Internet.

- 5 Metoda poate fi utilizată în cadrul prestării următoarelor servicii, fără a se limita la acestea:
- servicii care presupun autentificarea clientului prin intermediul unei metode de autentificare alese de furnizorul de servicii;
 - servicii care presupun autentificarea clientului prin intermediul unei metode de autentificare alese de furnizorul de servicii și necesită o limitare cantitativă a serviciului prestat (exemplu: free trial);
 - 10 • servicii care nu presupun autentificarea clientului și necesită o limitare cantitativă a serviciului prestat (exemplu: accesul trebuie să fie restricționat la un număr maxim de accesări zilnice de către un singur utilizator);
 - din punct de vedere al bunului oferit, servicii exclusiv online din tipurile de mai sus;
 - 15 • servicii care presupun furnizarea unui bun tangibil ca urmare a unei comenzi efectuate prin intermediul interfeței electronice a serviciului.

Este cunoscută o metodă de prevenire a infracțiunii la solicitarea prestării de servicii prin intermediul rețelei Internet, care constă în aceea că la recepționarea semnalului-solicitare de la dispozitivul utilizatorului de către serverul furnizorului pentru descoperirea infractorului, serverul realizează o verificare activă, solicitând de la utilizator datele accountului, ID-ul atribuit de sistemul de prevenire a fraudei pentru dispozitivul client al utilizatorului (device ID), amprenta digitală a dispozitivului client (generată de către sistemul antifraudă pe baza informațiilor specifice ale dispozitivului client la accesarea serviciului), suma de control a fișierului, de asemenea determinând datele specifice ale dispozitivului utilizatorului, cookie, ID-ul sesiunii și introducându-le pe acestea în memoria sa [1].

Dezavantajele acestei metode constau în aceea că astfel de metode de verificare a datelor utilizatorului pot fi vulnerabile, deoarece există situații, când serverul furnizorului nu poate identifica ID-ul utilizatorului, cum ar fi situații în care dispozitivul nu permite stocarea ID-ului sau când utilizatorul a șters acest ID ca urmare a unei operațiuni de mentenanță a dispozitivului sau situații în care furnizorul de servicii nu dorește stocarea ID-ului datorită contextului în care oferă serviciu. În cazul în care serverul furnizorului nu poate identifica ID-ul utilizatorului, sistemul refuză de a presta utilizatorului serviciul solicitat. Însă în cazul în care utilizatorul, care a solicitat serviciul, este un utilizator de bună credință, iar sistemul furnizorului nu poate identifica ID-ul calculatorului acestuia, apare situația, în care furnizorul refuză prestarea serviciului unui utilizator de bună credință.

Problema pe care o rezolvă invenția constă în crearea unei metode, care ar asigura autentificarea securizată pentru utilizator și optimizarea interacțiunii utilizator-furnizor în ceea ce privește eficacitatea și siguranța.

Metoda, conform invenției, înlătură dezavantajele menționate mai sus prin aceea că la recepționarea semnalului-solicitare de la dispozitivul utilizatorului de către serverul furnizorului pentru descoperirea infractorului, serverul realizează o verificare activă, solicitând de la utilizator datele accountului și suma de control a fișierului, de asemenea determinând datele specifice ale dispozitivului utilizatorului, cookie, ID-ul sesiunii și introducându-le pe acestea în memoria sa, în cazul imposibilității de identificare a datelor accountului utilizatorului sau sumei de control a fișierului utilizatorului, se stabilește o conexiune suplimentară între serverul furnizorului și dispozitivul utilizatorului, care execută o verificare pasivă, solicitând date suplimentare de autentificare.

Invenția se explică prin desenele din figurile 1-5, care reprezintă:

- fig. 1, schema legăturilor între dispozitivul utilizatorului și furnizor;
- 50 - fig. 2, schema generală de parcurs a semnalului solicitării din start până la accesul serviciului, sau refuzul definitiv de prestare a serviciului, incluzând detalii pentru investigarea preliminară;
- fig. 3, schema parcursului semnalului solicitării în cadrul verificării pasive;
- fig. 4, schema parcursului semnalului solicitării în cadrul verificării active a unui dispozitiv cu indicator dispozitiv prezent;
- 55 - fig. 5, schema parcursului semnalului solicitării în cadrul verificării active a unui dispozitiv fără identificator dispozitiv prezent, cu recurs la investigarea pasivă.

Lista semnelor convenționale:

DC : dispozitiv client

CD1 : context dispozitiv 1 - de exemplu referrer și informații de genul acesta

CD2 : context dispozitiv 2 - de exemplu dacă ADC a putut fi salvată pe dispozitiv

5 CD3 : context dispozitiv 3 - de exemplu adresa IP, resursa (URL)

ADD : amprenta digitală dispozitiv (calcularea ei se face pe baza caracteristicilor dispozitivului)

ID: identificator dispozitiv - este un identificator unic generat de către SPF și salvat pe DC

ADC : aplicație detecție client

10 SP : sistem prevenire

BD-SP : baza de date - sistem prevenire

ADF : aplicație de detecție furnizor

FS : furnizor de servicii

FS-CPC : furnizor de servicii - configurare punct de control

15 RDFS : reguli definite de către furnizorul de servicii

AC : aplicație cadru a furnizorului de servicii (javascript)

ICU : informații comportament utilizator

DIU : datele introduse de către utilizator - setul de date ce trebuie introduse de către
utilizatorul care accesează un anume serviciu/resursă. Pot fi datele de acces (login) sau de
20 înscriere

DRDA : Date Relevante pentru Domeniul de Activitate.

Metoda propusă constă în aceea că la recepționarea semnalului-solicitare de la dispozitivul
infractorului presupus (1) (în figura 1) de serverul furnizorului (2), serverul solicită de la
utilizator informația privind contul acestuia și amprenta digitală a dispozitivului client
25 (fingerprint) și introduce aceste date în memoria sa, după care utilizatorul completează
formularul de solicitare a serviciului, în cazul în care modalitatea de acces a serviciului stabilită
de furnizor prevede acest pas. În această etapă se realizează o verificare activă a
conștiințiozității utilizatorului prin determinarea datelor specifice ale dispozitivului
utilizatorului, cum ar fi modul cookie, sesiunea ID, etc. În cazul în care dispozitivul
30 utilizatorului nu a trecut verificarea activă, adică serverul furnizorului nu a reușit citirea
informației cu privire la contul sau la amprenta digitală a dispozitivului client al utilizatorului,
se conectează automat legătura suplimentară între serverul furnizorului și dispozitivul
utilizatorului, care execută o verificare pasivă, folosind datele disponibile la momentul
respectiv.

35 Schema legăturilor între dispozitivul utilizatorului și furnizor (figura 1)

Diagrama reprezintă schematic interacțiunea dintre un utilizator și un formular al unui
furnizor de servicii. Utilizatorul accesează o pagină web, unde furnizorul de servicii prezintă
niște câmpuri care trebuie completate. În pagina web este prezentă și aplicația detectare
40 infractor client (denumită în cele ce urmează "aplicație de detecție client") servită de către
sistemul de prevenire a infracționalității din cadrul invenției (denumit în cele ce urmează
"sistem de prevenire") care face o sumă de verificări pe dispozitiv client. Odată făcute aceste
verificări, clientul contactează sistemul de prevenire și-i trimite datele de amprentare digitală
pasivă bazate pe datele culese de pe dispozitivul client. De asemenea se transmit și date de
55 genul cookies sau identificator de device, acesta din urmă în cazul în care verificarea activă
este posibilă. În momentul în care utilizatorul trimite formularul completat pe dispozitivul
client, datele completate de către utilizator împreună cu amprenta digitală dispozitiv sunt
trimise la furnizorul de servicii. Furnizorul de servicii trimite mai departe la sistemul de
prevenire date cum ar fi amprenta digitală, dispozitiv și informații de identificare și primește
înapoi un scor pe baza căruia este evaluată credibilitatea clientului.

50 Procedura de verificare pe etape se realizează în modul ce urmează.

Etapă investigării preliminare (figura 2)

De la dispozitivul utilizatorului se expediază o solicitare spre serverul furnizorului. Serverul
furnizorului răspunde acestei solicitări transmițând aplicația cadru (denumită în cele ce
urmează "aplicație cadru") pentru furnizarea serviciului. Aplicația cadru este o aplicație
55 specifică furnizorului de servicii care permite utilizatorului să acceseze serviciul într-o etapă
ulterioară. Această aplicație cadru este integrată cu aplicația detecție client furnizată de
sistemul de prevenire. Aplicația cadru lansează aplicația de detecție client pe dispozitivul
utilizatorului. Dacă lansarea a eșuat, sistemul de prevenire nu va putea realiza verificarea și, prin
urmare, accesul utilizatorului la serviciul respectiv va fi refuzat. Dacă lansarea este reușită, în

funcție de configurările specifice realizate de furnizorul de servicii pentru punctul de control, se va proceda în felul următor: (a) dacă punctul de control este configurat ca punct de control cu verificare doar pasivă, se va proceda la realizarea identificării pasive (figura 3); și (b) dacă punctul de control necesită verificare completă, se va proceda la citirea identificatorului dispozitiv și la generarea amprentei dispozitiv. Ca o continuare la opțiunea descrisă la litera (b) din propoziția precedentă, dacă identificatorul dispozitiv este găsit, se va continua cu pașii descriși în figură (figura 4), iar dacă identificatorul dispozitiv nu este găsit, se va continua cu pașii descriși în figură (figura 5).

Etapa investigării complete, varianta investigării pasive pentru prevenirea fraudei (figura 3)

- Se continuă din figura 2. Pe dispozitivul clientului se generează amprenta dispozitivului, pe baza datelor specifice disponibile pe dispozitiv, cum ar fi, dar nelimitându-se la: tip de browser, limbă, sistem de operare, tipuri de caractere, module instalate, etc. Dacă nu este necesar ca utilizatorul să introducă date de acces într-un formular, atunci amprenta dispozitivului se trimite la furnizorul de servicii. Dacă este nevoie ca utilizatorul să introducă date suplimentare, atunci aplicația cadru va afișa un formular pe dispozitivul client. În timp ce clientul introduce datele, aplicația de detecție client colectează informațiile de comportament ale utilizatorului care apoi împreună cu datele introduse de utilizator și amprenta dispozitiv sunt trimise la furnizorul de servicii. Furnizorul de servicii validează mai întâi datele introduse de către utilizator; dacă nu sunt valide/bune și este permisă o nouă încercare de introducere a datelor, utilizatorului îi va fi afișat din nou formularul pe dispozitivul client. Dacă însă datele introduse de către utilizator sunt valide, atunci aplicația de detecție pentru furnizorul de servicii (denumită în cele ce urmează "aplicația de detecție furnizor") adună datele din contextul dispozitiv 3 (de exemplu adresa IP, resursa (URL) denumită în cele ce urmează "context dispozitiv 3") și le trimite la sistemul de prevenire, împreună cu informațiile de comportament și amprenta dispozitiv primite de la aplicația de detecție client. Aplicația de detecție furnizor este o aplicație furnizată de sistemul de prevenire și integrată cu sistemul furnizorului de servicii. Sistemul de prevenire determină, pe baza algoritmului de investigare pasivă și a datelor primite, dacă există înregistrări care atestă, cu o probabilitate prestabilită, faptul că dispozitivul este identic cu dispozitive conectate anterior. Sistemul de prevenire evaluează datele disponibile (informațiile dispozitivelor determinate a fi identice, datele introduse de către utilizator, amprenta dispozitiv, informațiile comportament utilizator, contextul dispozitiv 1, contextul dispozitiv 3, datele de identificare domeniu de activitate) pe baza regulilor definite de către furnizorul de servicii în interfața de administrare a sistemului de prevenire și pe baza datelor relevante pentru domeniul de activitate respectiv, adunate de sistemul de prevenire de la ceilalți furnizori de servicii. În urma evaluării datelor de mai sus de către sistemul de prevenire, acesta răspunde către furnizorul de servicii transmițând o recomandare (acceptă, respinge sau analizează), un scor, precum și informații despre regulile care au fost aplicate pentru obținerea scorului. În cazul recomandării acceptă, furnizorul de servicii va pune la dispoziție resursa pe care utilizatorul dorește s-o acceseze, prin intermediul aplicației cadru de pe dispozitivul client. În cazul recomandării respinge sau analizează, furnizorul de servicii poate afișa informații privitoare la accesul restricționat prin intermediul aplicației cadru de pe dispozitivul client. În cazul recomandării analizează, administratorul furnizorului de servicii este notificat și va putea ulterior accepta sau respinge manual cererea din interfața de administrare a sistemului de prevenire. La o accesare ulterioară de către utilizator a resursei sau serviciului, sistemul de prevenire va emite recomandarea acceptă sau respinge, corespunzător cu acțiunea manuală a administratorului.

Etapa investigării complete, varianta investigării active pentru prevenirea fraudei, a unui dispozitiv cu identificator dispozitiv prezent (figura 4)

- Se continuă din figura 2. Dacă nu este necesar ca utilizatorul să introducă date de acces într-un formular, atunci amprenta dispozitivului, împreună cu identificatorul de dispozitiv se trimite la furnizorul de servicii. Dacă este nevoie ca utilizatorul să introducă date suplimentare, atunci aplicația cadru va afișa un formular pe dispozitivul client. În timp ce clientul introduce datele, aplicația de detecție client colectează informațiile de comportament ale utilizatorului care apoi împreună cu datele introduse de utilizator, identificatorul de dispozitiv și amprenta dispozitiv sunt trimise la furnizorul de servicii. Acesta validează mai întâi datele introduse de către utilizator; dacă nu sunt valide/bune și este permisă o nouă încercare de introducere a datelor, utilizatorului îi va fi afișat din nou formularul pe dispozitivul client. Dacă însă datele introduse de către utilizator sunt valide, atunci aplicația de detecție client pentru furnizorul de servicii adună datele context dispozitiv 3 și le trimite sistemului de prevenire, împreună cu informațiile

de comportament și amprenta dispozitiv primite de la aplicația de detecție client. Aplicația de detecție client pentru furnizorul de servicii este o aplicație furnizată de sistemul de prevenire și integrată cu sistemul furnizorului de servicii. Sistemul de prevenire evaluează datele disponibile (datele introduse de către utilizator, identificatorul dispozitiv, amprenta dispozitiv, informațiile comportament utilizator, contextul dispozitiv 1, contextul dispozitiv 3, datele de identificare domeniu de activitate) pe baza regulilor definite de către furnizorul de servicii în interfața de administrare a sistemului de prevenire și pe baza datelor relevante pentru domeniul de activitate respectiv, adunate de sistemul de prevenire de la ceilalți furnizori de servicii. În urma evaluării datelor de mai sus de către sistemul de prevenire, acesta răspunde către furnizorul de servicii transmițând o recomandare (acceptă, respinge sau analizează), un scor, precum și informații despre regulile care au fost aplicate pentru obținerea scorului. În cazul recomandării acceptă, furnizorul de servicii va pune la dispoziție resursa pe care utilizatorul dorește s-o acceseze, prin intermediul aplicației cadru de pe dispozitivul client. În cazul recomandării respinge sau analizează, furnizorul de servicii poate afișa informații privitoare la accesul restricționat prin intermediul aplicației cadru de pe dispozitivul client.

Etapă investigării complete, varianta investigării active pentru prevenirea fraudei, a unui dispozitiv fără identificator dispozitiv prezent, cu recurs la investigarea pasivă (figura 5)

Se continuă din figura 2. Pe dispozitivul clientului se generează amprenta dispozitivului, pe baza datelor specifice disponibile pe dispozitiv, la fel ca la figura 3. Se transmite această amprentă către sistemul de prevenire, opțional prin intermediul unui serviciu de redirecție furnizor (proxy) care are rolul de a face posibilă tranzacționarea integrală prin intermediul furnizorului de servicii. Sistemul de prevenire, la primirea amprentei dispozitiv va genera identificatorul dispozitiv, va stoca amprenta dispozitiv împreună cu identificatorul dispozitiv și informațiile din contextul dispozitiv 1 (cum ar fi referrer și informații de acest gen) și va transmite către aplicația de detecție client identificatorul dispozitiv. Aplicația de detecție client va încerca stocarea identificatorului de dispozitiv pe dispozitiv, marcând în contextul dispozitiv 2, dacă această stocare s-a efectuat cu succes. Dacă nu este necesar ca utilizatorul să introducă date de acces într-un formular, atunci amprenta dispozitivului, împreună cu identificatorul de dispozitiv, se trimite la furnizorul de servicii. Dacă este nevoie ca utilizatorul să introducă date suplimentare, atunci aplicația cadru va afișa un formular pe dispozitivul client. În timp ce clientul introduce datele, aplicația de detecție client colectează informațiile de comportament ale utilizatorului care apoi împreună cu datele introduse de utilizator, identificatorul de dispozitiv și amprenta dispozitiv sunt trimise la furnizorul de servicii. Ultimul validează mai întâi datele introduse de către utilizator; dacă nu sunt valide/bune și este permisă o nouă încercare de introducere a datelor, utilizatorului îi va fi afișat din nou formularul pe dispozitivul client. Dacă însă datele introduse de către utilizator sunt valide, atunci aplicația de detecție furnizor adună datele pentru contextul dispozitiv 3 și le trimite sistemului de prevenire, împreună cu contextul dispozitiv 2 (cum ar fi dacă de exemplu aplicație detecție client a putut fi salvată pe dispozitiv), informațiile de comportament și amprenta dispozitiv primite de la aplicația de detecție client. Sistemul de prevenire determină, pe baza algoritmului de investigare pasivă și a datelor primite, dacă există înregistrări care atestă, cu o probabilitate prestabilită, faptul că dispozitivul este identic cu dispozitive conectate anterior. Acest pas este practic recursul la investigarea pasivă pentru un dispozitiv căruia i-a fost eliminat identificatorul dispozitiv de la ultima verificare. Apoi, sistemul de prevenire a fraudei evaluează datele disponibile (informațiile dispozitivelor determinate a fi identice, datele introduse de către utilizator, amprenta dispozitiv, informațiile comportament utilizator, contextul dispozitiv 1, contextul dispozitiv 3, date de relevanțe domeniu de activitate) pe baza regulilor definite de către furnizorul de servicii în interfața de administrare a sistemului de prevenire și pe baza datelor relevante pentru domeniul de activitate respectiv, adunate de sistemul de prevenire de la ceilalți furnizori de servicii. În urma evaluării datelor de mai sus de către sistemul de prevenire, acesta răspunde către furnizorul de servicii transmițând o recomandare (acceptă, respinge sau analizează), un scor, precum și informații despre regulile care au fost aplicate pentru obținerea scorului. În cazul recomandării acceptă, furnizorul de servicii va pune la dispoziție resursa pe care utilizatorul dorește s-o acceseze, prin intermediul aplicației cadru de pe dispozitivul client. În cazul recomandării respinge sau analizează, furnizorul de servicii poate afișa informații privitoare la accesul restricționat prin intermediul aplicației cadru de pe dispozitivul client.

În continuare se prezintă două exemple de folosire a metodei de prevenire a fraudei.

Primul exemplu se referă la o situație în care furnizorul de servicii online dorește o identificare preferabil prin metoda activă a utilizatorului, acesta accesând serviciul pe baza

- unui cont, folosind login și parola pentru autentificare. Astfel furnizorul oferă un serviciu online (denumit în cele ce urmează "SO") care pune la dispoziția utilizatorilor facilități de procesare în cloud. Utilizatorul are avantajul că în loc să aibă nevoie de câteva săptămâni să genereze un film de animație poate face acest lucru în câteva ore/o zi. Folosind metoda care
- 5 face obiectul invenției, un utilizator care încearcă să se înscrie a doua oară va fi identificat chiar și în cazul în care folosește un alt cont sau chiar un alt dispozitiv de rețea din aceeași
- 10 locație. Pe baza regulilor stabilite de către administratorii SO înscrierea/accesarea repetată a unui asemenea utilizator a site-ului poate genera o alertă în sistem. De asemenea în cazul în care dispozitivul utilizatorului nu permite stocarea unui identificator de dispozitiv sau acest
- 15 identificator a fost eliminat, în urma investigării pasive, sistemul poate decide să îi permită accesul în cont, dar să nu-i ofere niciun beneficiu sau alternativă, să nu-i blocheze accesul, dacă este cunoscut de sistemul de prevenire ca un utilizator care a făcut fraudă prin intermediul
- 20 cardurilor de credit în alte împrejurări. În felul acesta SO nu suferă pierderi din cauza utilizatorilor fraudulenți și își poate mări în același timp vânzările.
- 25 Al doilea exemplu se referă la o publicație online care funcționează pe bază de abonament, dar permite accesul neautentificat al unui vizitator la un articol pe zi. Această politică este implementată în scopul de a atrage cititorii și a-i convinge prin calitatea materialelor să dorească să citească mai mult și, prin urmare, să își facă abonament. Însă această politică implică posibilitatea limitării accesului fără a recurge la un cont de utilizator. Folosind sistemul
- de prevenire prin metoda pasivă a acestuia, în condițiile în care nu se dorește stocarea unui identificator de dispozitiv pe un dispozitiv cu al cărui posesor nu este într-o relație contractuală, publicația online poate identifica în mod unic un dispozitiv sau chiar cu o
- probabilitate suficient de bună un utilizator care folosește dispozitive din aceeași locație și, prin urmare, poate limita accesul la un articol pe zi și astfel obține venituri din abonamente în timp
- ce implementează politica de mai sus pentru atragerea clienților.

(56) Referințe bibliografice citate în descriere:

1. US 7330871 B2 2008.02.12

(57) Revendicări:

Metodă de prevenire a infracțiunii la solicitarea prestării de servicii prin intermediul rețelei Internet, care constă în aceea că la recepționarea semnalului-solicitare de la dispozitivul utilizatorului de către serverul furnizorului pentru descoperirea infractorului, serverul realizează o verificare activă, solicitând de la utilizator datele accountului și suma de control a fișierului, de asemenea determinand datele specifice ale dispozitivului utilizatorului, cookie, ID-ul sesiunii și introducându-le pe acestea în memoria sa, **caracterizată prin aceea că** în cazul imposibilității de identificare a datelor accountului utilizatorului sau sumei de control a fișierului utilizatorului, se stabilește o conexiune suplimentară între serverul furnizorului și dispozitivul utilizatorului, care execută o verificare pasivă, solicitând date suplimentare de autentificare.

Șef Secție Examinare:

GROSU Petru

Examinator:

GHIȚU Irina

Redactor:

CANȚER Svetlana

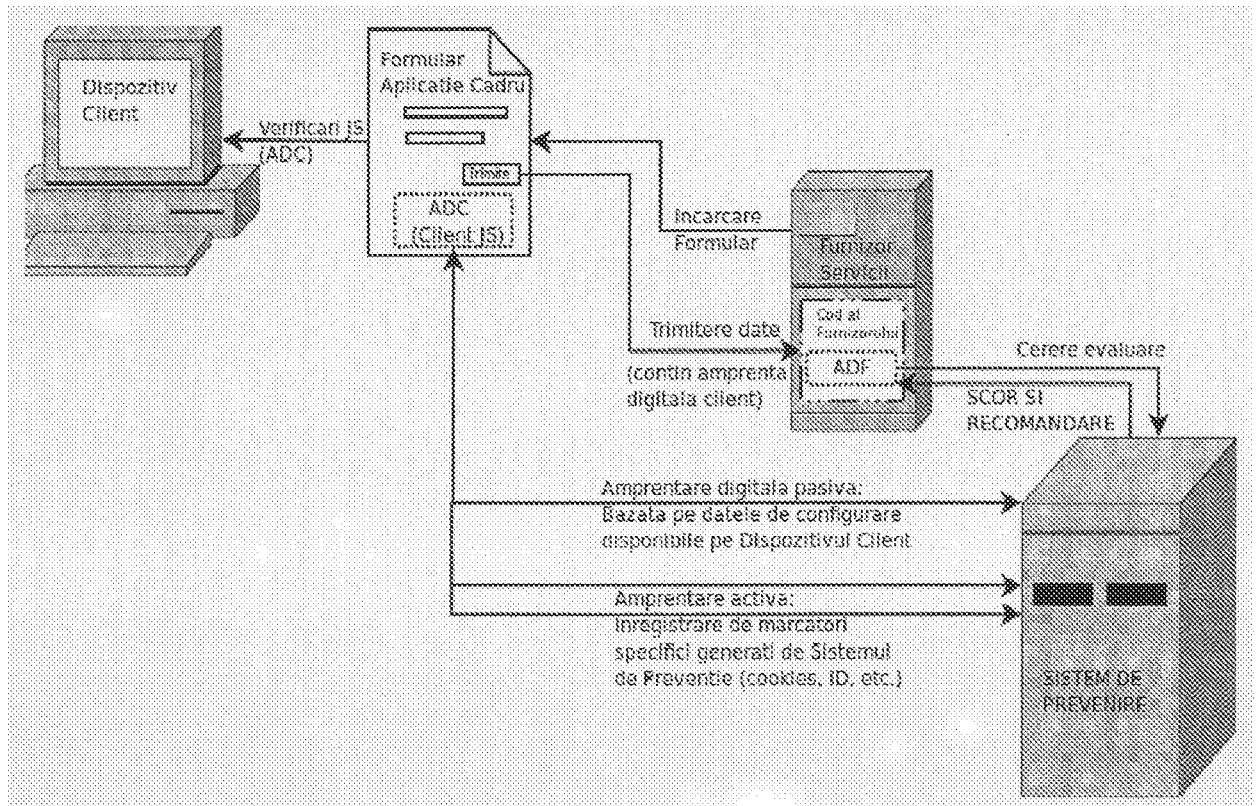


Fig. 1

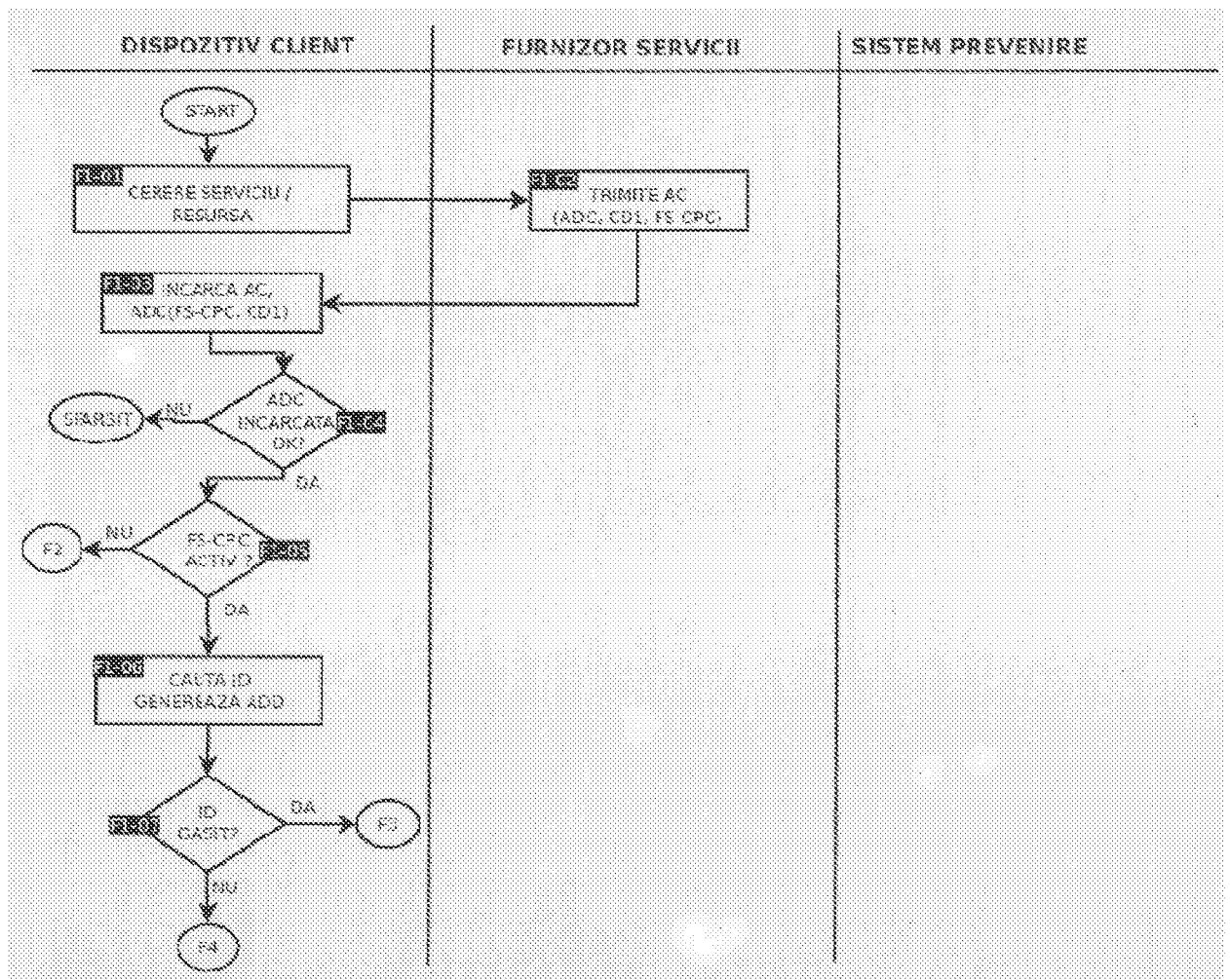


Fig. 2

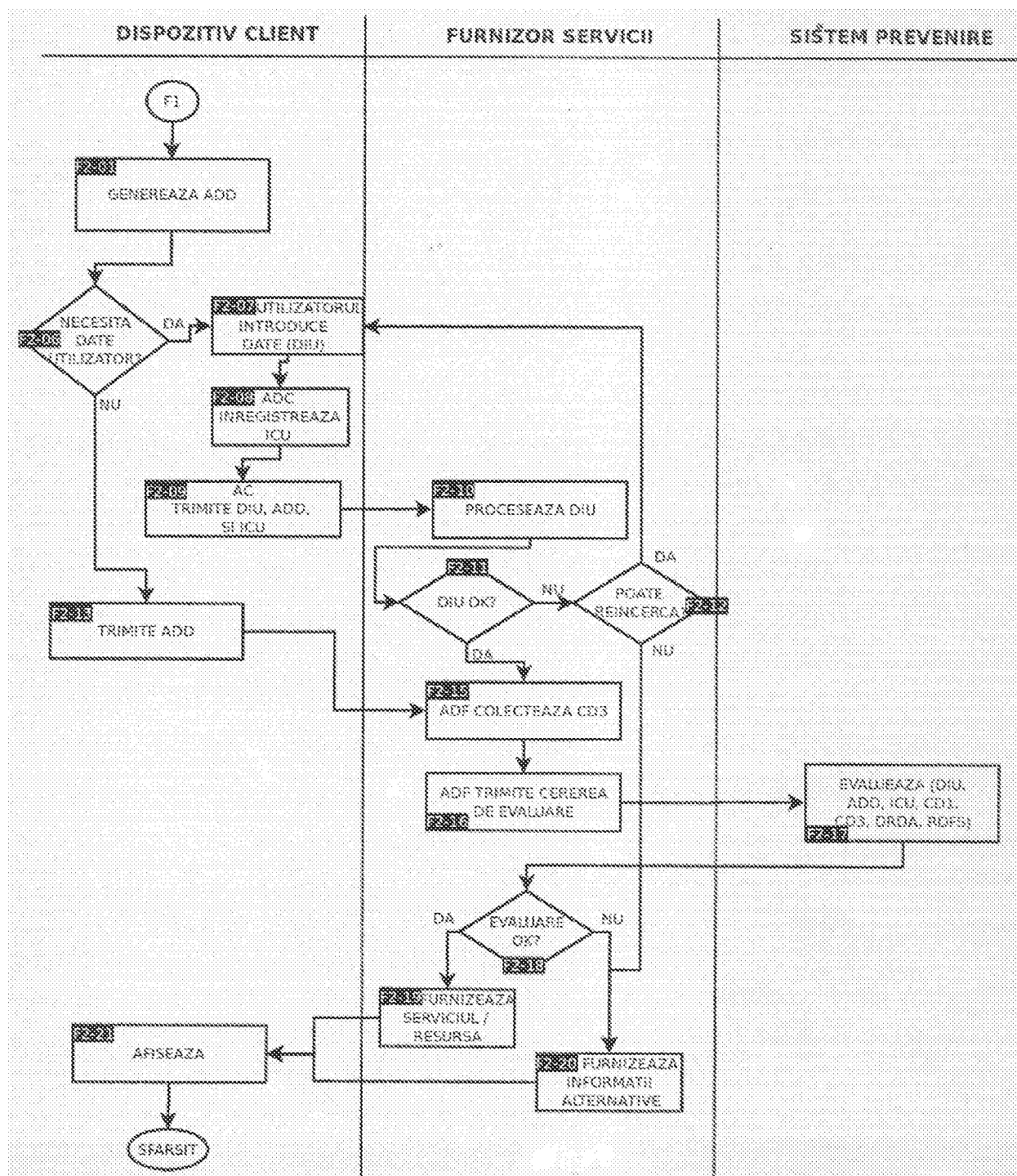


Fig. 3

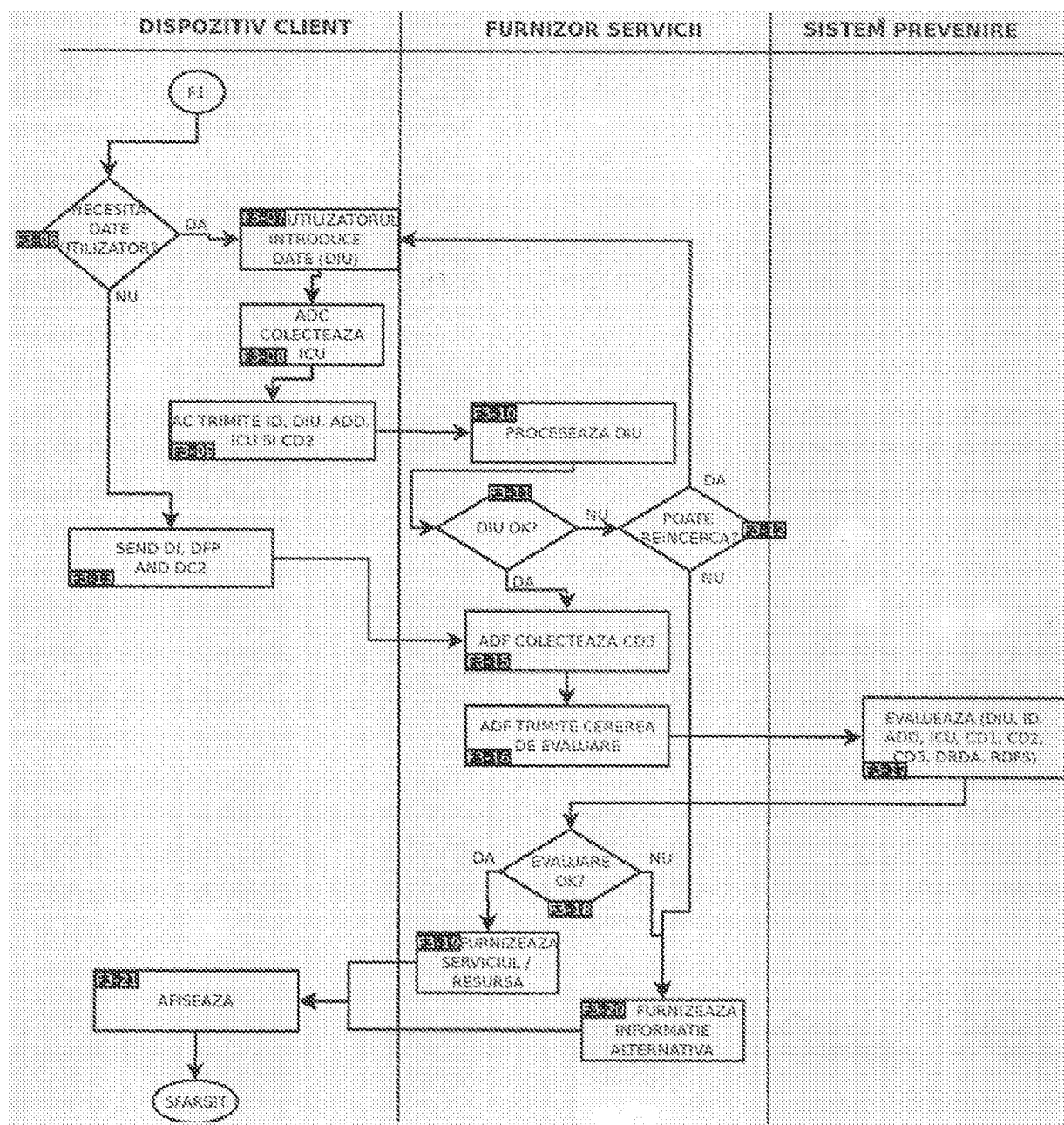


Fig. 4

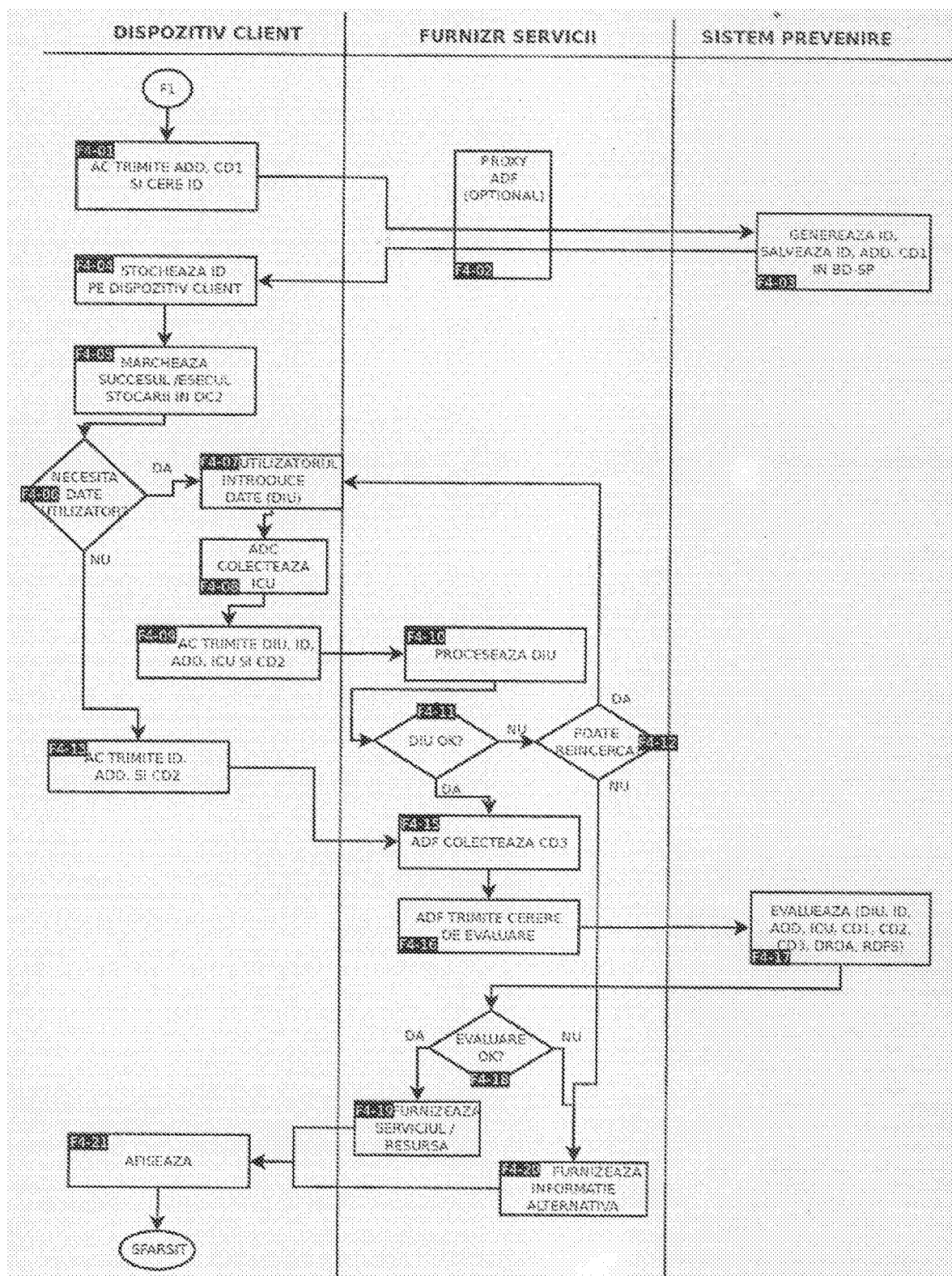


Fig. 5

RAPORT DE DOCUMENTARE

I. Datele de identificare a cererii		
(21) Nr. depozit: s 2015 0017 (22) Data depozit: 2015.02.17 (71) Solicitant: SOCIETATEA CU RĂSPUNDERE LIMITATĂ "SIGURANȚĂ TRANZACȚII", MD (54) Titlul: Metodă de prevenire a infracțiunii la solicitarea prestării de servicii prin intermediul rețelei Internet		
II. Clasificarea obiectului invenției:		
(51) Int.Cl: <i>H04L 9/00</i> (2006.01) <i>H04L 29/06</i> (2006.01) <i>H04K 1/00</i> (2006.01)		
III. Colecții și Baze de date de brevete cercetate (denumirea, termeni caracteristici, ecuații de căutare reprezentative)		
MD - Intern « Documentare Invenții » (inclusiv cereri nepublicate; trunchiere automată stanga/dreapta): H04L, H04K, infracțiune, servicii, internet, autentificare, account, server, cookie, fișier SU, EA, CIS (Eapatis): H04L*, H04K*, политика конфиденциальности, подозрительная активность, услуги, аутентификация, аккаунт, сервер, идентификация, провайдер		
IV. Baze de date și colecții de literatură nonbrevet cercetate		
ru.wikipedia.org www.google.ru		
V. Documente considerate a fi relevante		
Categorია*	Date de identificare ale documentelor citate si, unde este cazul, indicarea pasajelor pertinente	Numărul revendicării vizate
A, D, C	US7330871 B2 2008.02.12	1
* categoriile speciale ale documentelor citate:		
A – document care definește stadiul anterior general	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 pe care se bazează invenția	
X – document de relevanță deosebită: invenția revendicată nu poate fi considerată nouă sau implicând activitate inventivă când documentul este luat în considerație de unul singur	E – document anterior dar publicat la data depozit național reglementar sau după aceasta dată	
Y – document de relevanță deosebită: invenția revendicată nu poate fi considerată ca implicând activitate inventivă când documentul este asociat cu unul sau mai multe documente de aceeași categorie	D – document menționat în descrierea cererii de brevet	

O - document referitor la o divulgare orală, un act de folosire, la o expoziție sau la orice alte mijloace de divulgare	C – document considerat ca cea mai apropiată soluție & – document, care face parte din aceeași familie de brevete
P - document publicat înainte de data de depozit, dar după data priorității invocate	L – document citat cu alte scopuri
Data finalizării documentării 2015.07.10	
Examinator GHIȚU Irina jr.	