ელექტრონულ კომერციაში მონაცემთა დაცვის ლოკალური ტექნოლოგიები

მარინე ქარსელაძე, დოქტორანტი

რეზიუმე

დღეს, საყოფაცხოვრებო პირობებშიც კი შესაძლებელია კომპიუტერული სისტემის მომართვა ისე, რომ ყოველდღიურად სრულდებოდეს ინტერნეტის ინფორმაციული სივრცის სკანირება

ბოლო ათწლეულში გამოჩნდა ტექნიკური საშუალებები, რომელმაც შესაძლებელი გახადა კომერციული საქმიანობის კომპლექსური ავტომატიზაცია ანუ ელექტრონული კომერცია.

საკვანძო სიტყვები: ელ-კომერცია, ბრანდმაუერი, პროქსი-სერვერი, სერვერი

LOCAL SECURITY TECHNOLOGY IN ELECTRONIC COMMERCE

MARINE KARSEDADZE, DOCTORAL

Summary

Today, the living conditions are possible on a computer system for adjusting so that the daily performed the Internet information space scanning.

Until recently, the automation of commercial transactions on the local character. Only in the last decade, a prominent technical means that made it possible to automate complex business electronic commerce.

KEYWORD: electronic commerce, security firewall, server

* * * * * * *

თანამედროვე კომერციას ტრადიციული ვაჭრობისაგან განასხვავებს ის, რომ ეს არაა უბრალოდ საქონელბრუნვა შესრულებული მწარმოებლების ან კლიენტების მიმდინარე მოთხოვნილებების დასაკმაყოფილებლად. ეს არის მთელი რიგი ღონისძიებების უწყვეტი კომპლექსი, რომელიც სრულდება კომერციული პროცესის სხვადასხვა ეტაპებზე.

ტრადიციული სავაჭრო ურთიერთობების გამოკვლევისას მარტივად მოიძებნება იმის მაგალითი თუ როგორ გამოიყენება კომერციული ციკლის თითოეულ ეტაპზე ტექნიკური საშუალებები, მათ შორის ელექტრონული, დანახარჯების შემცირების ავტომატიზაციისათვის. მაგრამ ეს კიდევ არ არის ელექტრონული კომერცია. ელექტრონული კომერციისათვის დამახასიათებელია კომპლექსური ავტომატიზაცია.

ელექტრონული კომერცია - ეს სავაჭრო საქმიანობაა, რომლის ძირითადი მიზანია მოგების მიღება და დამყარებულია კომერციული ციკლის კომპლექსურ ავტომატიზაციაზე გამოთვლითი ტექნიკის გამოყენებით.

"იდეალურ" შემთხვევაში ელექტრონული კომერცია საშუალებას იძლევა სრულად გამოირიცხოს ადამიანი - არამარტო კლიენტი არამედ მყიდველიც კომერციული ციკლიდან.

ურთიერთობის სისტემა გამყიდველი-მყიდველი შეიძლება შეიცვალოს ავტომატურად ფუნქციონირებადი სისტემით სერვერი-კლიენტი წარმოდგენილი მხოლოდ აპარატული და პროგრამული საშუალებებით.

დღეს, საყოფაცხოვრებო პირობებშიც კი შესაძლებელია კომპიუტერული სისტემის მომართვა ისე, რომ ყოველდღიურად სრულდებოდეს ინტერნეტის ინფორმაციული სივრცის სკანირება მაგალითად, რომელიმე (საინტერესო) ავტორის ახალი რომანის მოსაძებნად და სავაჭრო სერვერის მხრიდან კომერციული შეთავაზების აღმოჩენისას ავტომატურად შეასრულოს ურთიერთ ანგარიშსწორება, რის შემდეგაც გადაგზავნის მიღებულ ნაწარმოებს მფლობელის კავშირის მობილური საშუალებებზე.

ბოლო ათწლეულში გამოჩენილმა ტექნიკურმა საშუალებებმა შესაძლებელი გახადა კომერციული საქმიანობის კომპლექსური ავტომატიზაცია ანუ ელექტრონული კომერცია.

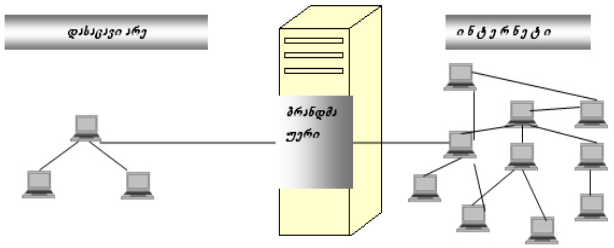
სტატიაში განვიხილავ ინფორმაციის დაცვის და შენახვის ტექნოლოგიას არა ტრანსპორტირების გზაზე, არამედ ინფორმაციის დაცვა შენახვის ადგილზე. კერძოდ, კომპიუტერზე შეუმოწმებელი პროგრამების დაყენებით შეიძლება დაიწყოს სერვერული ტიპის პროგრამის უკონტროლო მოქმედება. ზოგიერთ შემთხვევაში მსგავსი "სერვერები" დაშორებულ კლიენტს გადასცემენ კომპიუტერზე შენახულ ინფორმაციას, ზოგიერთ შემთხვევაში კი შემოიფარგლებიან იმ მონაცემების გადაცემით, რომლებიც კლავიატურიდან შეიყვანებიან კლიენტების სარეგისტრაციო სახელისა და პაროლის ჩათვლით, ხოლო ზოგიერთ შემთხვევაში კომპიუტერის მართვას მთლიანად გადასცემს დაშორებულ ტერმინალს. მსგავს პროგრამებს დაშორებული ადმინისტრირების საშუალებებს უწოდებენ. აიყვანს რა დაშორებული მართვის ქვეშ რომელიმე კომპიუტერს ქსელში, ხულიგანი მისგან იწყებს შეტევას მეორე "მსხვერპლზე" და ასე შემდეგ. შედეგად იქმნება შუალედური კომპიუტერების ჯაჭვი, რომელთა მფლობელები ვერც კი იეჭვიანებენ, რომ მათი სახელითა და მათი კომპიუტერით ვიღაცამ შეიძლება უკანონო მოქმედებები ჩაიდიმოს. განსაკუთრებით საშიში ოპერა-

ციების ჩატარებისას ბოროტმზრახველები წყვეტენ ჯაჭვს და "ასუფთავებენ" გამოყენებულ კომპიუტერებზე პროტოკოლურ ფაილებს, რომლებიც ინახავენ მონაცემებს შემდგარი კავშირის სეანსებზე.

დაშორებული ადმინისტრირების საფრთხე ერთერთი ყველაზე თვალსაჩინო, მაგრამ არა ერთადერთი საფრთხეა ქსელში. არსებობენ მრავალი სხვადასხვა მეთოდები ქსელში უკანონო მოქმედების შესასრულებლად. ზოგიერთის წინააღმდეგ არსებობს დაცვის აქტიური საშუალებები, ზოგიერთის კი - პასიური. არსებობენ "შეტევის" ისეთი სახეები, როგორიცაა "შეკითხვების შტორმი", რომელთა წინააღმდეგაც ძნელად მოიძებნება საბოლოოდ დაცვის ტექნიკური საშუალება, რამეთუ მოთხოვნების მიღება და დამუშავება კომპიუტერული სისტემის ბუნებრივი ფუნქციაა. მოცემულ შემთხვევაში ძირითადი აქცენტი ატა ტექნიკურ საშუალებებზე კეთდება, არამედ დაცვის სამართლებრივ უზრუნველყოფაზე.

ისეთი პროგრამების შექმნა, ან არსებულ პროგრამებში ისეთი ცვლილებების შეტანა შეგნებულად, რომლებიც იწვევენ არასანქცირებულ განადგურებას, ბლოკირებას, მოდიფიცირებას ან ინფორმაციის კოპირებას, კომპიუტერის, კომპიუტერული სისტემების ან ქსელების მუშაობის დარღვევას, ასეთი პროგრამების გამოყენება ან კომპიუტერულ მატარებლებით გავრცელება - ისჯება კანონით გათვალისწინებული თავისუფლების აღკვეთით ან საჯარიმო სანქციებით (საქართველოს კანონი კომპიუტერული დანაშაულებების შესახებ).

საერთაშორისო ქსელის მხრიდან შესაძლო შეტევებისგან კომპიუტერების სრულად დაცვის ყველაზე საიმედო მეთოდი - ინტერნეტიდან ფიზიკური გამორთვაა. გასაგები მიზეზების გამო ამ ტრივიალურ ვარიანტს არ განვიხილავთ, მაგრამ მოცემულ შემთხვევაში პრინციპული განსხვავების გადასაწყვეტად მოქმედებენ ისევე, როგორც სხვა მრავალ ანალოგიურ სიტუაციებში - შემოყავთ შუამავალი. ასეთი შუამავალი შეიძლება იყოს სხვა კომპიუტერი, ან სპეციალური პროგრამული საშუალება, განთავსებული დასაცავ კომპიუტერსა (ლოკალური ქსელსი) და გარემოს (ლოკალური ქსელი, გლობალური ქსელი, ინტენეტი) შორის. ასეთ აპარატულ ან პროგრამულ საშუალებებს ბრანდმაუერებს (Firewall) ბენ. ტექნიკურ ლიტერატურაში იყენებენ ტერმინსაც "დამცავი ეკრანი" ან "ქსელთაშორის ეკრანი". (ნახ.1.)



ნახატი 1.ბრანდმაუერით დაცვის სქემა.

ბრანდმაუერის მოქმედების პრინციპი დამყარებულია იმაზე, რომ ეს საშუალებები აკონტროლებენ შეერთების მდგომარეობას ქვედა გამოყენების დონეზე (შეერთების დონე, ქსელური დონე, სატრანსპორტო დონე) და ამით შეუძლია გამოიჭიროს არასანქცირებული საშუალების მუშაობის ნიშნები, შეუმჩნევლად შემოჭრილი თავისი ვირტუალური შეერთებით კავშირის სისტემაში გამოყენებითი დონის ქვემოთ, რომელიც ექვემდებარება კლიენტის კონტროლს. კერძოდ, ბრანდმაუერს შეუძლია უთვალთვალოს დაშორებული ადმინისტრირების საშუალებებს. იმავდროულად ბრანდმაუერს შეუძლია აკონტროლოს მონაცემთა ნაკადი (ტრაფიკი) და განახორციელოს მისი ფილტრაცია. ბრანდმაუერის შესაბამისი გამართვით შეიძლება მთლიანად ან ნაწილობრივ აუკრძალოს გარეშე კლიენტებს დაცულ არეში მყოფ სამსახურებთან, ან პირიქით, აუკრძალოს შიდა კლიენტებს გარე ქსელის სამსახურებთან მიმართვა.

ბრანდმაუერის მუშაობის არსის უკეთ გასაგებათ განვიხილოთ მარტივი მაგალითი. ვთქვათ ორი საწარმოს ხელმძღვანელები ცვლიან შეტყობინებებს (წერილებს). დაწერილ წერის ხელმძღვანელი გადასცემს მდივანს დასაბეჭდად, ხოლო მდივანი გადასცემს კურიერს მისატანად. ამ სისტემაში კავშირის მხოლოდ სამი დონეა: გამოყენებითი (ხელმძღვანელი), წარდგენის დონე (მდივანი) და ფიზიკური დონე).

ფიზიკური კავშირი არსებობს მხოლოდ კურიერულ სამსახურებს შორის, თუმცა ხელმძღვანელებიც აგრეთვე ვარაუდობენ, რომ მათ შორისაც არის კავშირი.კავშირი ნამდვილად არის, მაგრამ ვირტუალური (შუამავლის გავლით). სხვათაშორის მდივნებსაც შეუძლია ჩათვალონ, რომ მათ შორისაც არის ვირტუალური კავშირი.

დავუშვათ, რომ მდივნებმა მოილაპარაკეს და წერილების ბეჭდვისას ცვლიან ივფორმაციას ერთმანეთში. გამგზავნის მდივანი რაღაცას აწერს ფანქრით წერილის ბოლოში, ხოლო მიმღების მდივანი შლის ფანქრით მიწერილს.

ხელმძღვანელები კავშირის სისტემაში იკავებენ მაღალ დონეს, ამიტომ მათ არ იციან, რომ მათ არხს იყენებენ არასანქცირებულად. თუმცა ამას მარტივად მიხვდებიან კურიერები თუკი მათ მისცემენიმის უფლებას, რომ წაიკითხოს ის რასაც გადასცემენ. სპეციალურად მომზადებულ კურიერს მოცემულ მომენტში შეუძლია მისცეს სიგნალი ხელმძღვანელს, რომ მან აღმოაჩინა დაურეგისტრირებელი კავშირი (შეერთება). სწორედ ამით არიან დაკავებული ბრანდმაუერები.

ბრანდმაუერის გამართვის შედეგად თანამშრომლებზე დაკისრებული შეზღუდვების ერთობლიობა ქსელური უსაფრთხოების რეჟიმის უზრუნველყოფის სფეროში განისაზღვრება საწარმოს პოლიტიკით. ამ პოლიტიკის რეალიზაციაზე პასუხისმგებელია ნდობით აღჭურვილი პირი, როგორც წესი - სისტემის ადმინისტრატორი.

უმარტივესი პროგრამული საშუალების Atჩუარდ (WWW.atguard.com) მუშაობას, რომელიც ასრულებს ბრანდმაუერის ფუნქციას გაეცნობით

მოცემული თავის პრაქტიკულ სამუშაოში. პროგრამა ფონურ რეჟიმში მუშაობს და ასრულებს საკომუნიკაციო პორტების მდგომარეობის შემოწმებას. ამა თუ იმ პორტის გამოყენების მცდელობის აღმოჩენის შემთხვევაში იგი ატყობინებს კლიენტს. თუ კომუნიკაციის განხორციელებია შესახებ მისთვის ცნობილია, მას შეუძლია ნება დართოს თჩ - შეერთების შექმნაზე. წინააღმდეგ შემთხვევაშიკრძალავს და იღებს ზომებს მომთხოვნის იდენტიფიკაციისათვის. შესაძლებელია, რომ მოთხოვნა შემოვიდა გარედან (ხულიგანი ეძებს კონტაქტს საკომუნიკაციო პორტების სკანირების გზით), ან შეიძლება შიგნიდან (დაშორებული ადმინისტრირების საშუალებები უკვე ფარულად მუშაობენ კომპიუტერზე და ცდილობენ ქსელში გასვლას).

პროქსი-სერვერები

პროქსი-სერვერები პროგრამული საშუალებებია, რომლებიც აგრეთვე შუამავლის ფუნქციებს ასრულებენ, მაგრამ ბრანდმაუერებისაგან განსხვავებით არა ინსპექტორები, არამედ დისპეჩერებია. დასაწყისში პროქსი-სერვერები განკუთვნილი იყო არა კომპიუტერების ან ლოკალური ქსელების დასაცავად, არამედ მათი მუშაობის ოპტიმიზაციისათვის ინტერნეტში.

1. კომპიუტერის კლიენტი აგზავნის ინტერნეტში მოთხოვნას გარკვეული ვებ-რესურსის მოწოდებაზე, მაგრამ ეს მოთხოვნა იგზავნება არა ქსელში არამედ პროქსი-სერვერზე.

2. პროქსი-სერვერი თავისი სახელით აგზავნის ინტერნეტში მოთხოვნას ამ ვებ-რესურსის მოწოდებაზე და იღებს გამოძახილს დაშორებული სერვერიდან.

3. მიღებულ რესურს პროქსი-სერვერი გადასცემს კლიენტის მუშა სადგურს.

ამასთან კლიენტს ეძლევა შემდეგი უპირატესობები:

- დაშორებულმა სერვერმა არ იცის ზუსტად ვისგან მიიღო მოთხოვნა, მისი აზრით ის შემოვიდა პროქსი-სერვერიდან (ანონიმურობის ფუნქცია);
- პროქსი-სერვერის გავლით მიღებული ვებ-გვერდები იმახსოვრება მასზე (ქეშირდება), და თუ ლოკალური ქსელის სხვა კლიენტი მიმართავს ვებ-რესურს, რომელიც ახლახან მიიღო მისმა კოლეგამ, მაშინ ის მიიღებს მას არა დაშორებული სერვერიდან, არამედ პროქსი-სერვერიდან, რაც გაცილებით სწრაფად მოხდება (ჩანოტვირთვის დაჩქარების ფუნქცია);
- ვებ-გვერდია ელემენტები პროქსი-სერვერის გავლით ანალიზდება და იფილტრება, ანუ უსარგებლო ინფორმაცია, მაგალითად რეკლამა, შეიძლება დაიცხრილოს (ფილტრაციის ფუნქცია);
- ხანგრძლივი მუშაობის შედეგად პროქსი-სერვერზე გროვდება ინტერნეტის სერვერების დომენური სახელების და მათი lჴ-მისამართების შესაბამისობის შესახებ მონაცემები, რისი წყალობითაც იგივე ვებ-რესურსებთან განმეორებით მიმართვისას უკვე საჭირო აღარ არის მათი lჴ-მისამართების ძებნა DNS - სისტემის შედარებით ნელ იერარქიულ სტრუქტურაში (შეერთების დაჩქარების ფუნქცია).

მიუხედავად იმისა, რომ პროქსი-სერვერის ძირითადი დანიშნულება თითქოს არ არის დაკავშირებული მონაცემების დაცვასთან, მიუხედავად ამისა ის ასეთ დაცვას მაინც უზრუნველყოფს. ჯერ ერთი, საწარმოს ადმინისტრაციის მიერ პროქსი-სერვერის შეიძლება მოიმართოს ისე, რომ შეიზღუდოს თანამშრომლები ვებ-რესურსების იმ ვიწრო წრესთან დასაშვებათ, რომელიც აუცილებელია მათი დავალებების შესასრულებლად. მეორეც, პროქსი-სერვერი, როდორც შუამავალი, შეუძლია აკონტროლოს მასში გამავალი მონაცემების ინფორმაციული შინაარსი. მას შეუძლია დაბლოკოს ვირუსების შემცველი ფაილები და არქივები, აგრეთვე ეთიკური, პოლიტიკური და რელიგიური თვალსაზრისით დაუშვებელი ცნობები. და ბოლოს, პროქსი-სერვერი საშუალებას იძლევა დაიფაროს დასაცავი ქსელის სტრუქტურა და არქიტექტურა გარედან ანალიზისაგან. ეს ძალიან მნიშვნელოვანი მომენტია, რადგანაც ინფორმაციულ სისტემაზე დაშორებულ შეტევას, როგორც წესი წინ უძღვის მისი პროგრამული და აპარატული უზრუნველყოფის შესწავლა გამოკვლევა. პროგრამების ვერსიის ცოდნა, რომლებიც უზრუნველყოფენ ლოკალური ქსელის მუსაობას, საშუალებას აძლევს ხულიგნებს გამოავლინონ მისი სუსტი ადგილები და გამოიყენოს ისინი სპეციალური პროგრამების საშუალებით - ეგრეთწოდებული ექსპლოიტებით. გარე დამკვირვებლებიდან ქსელის არქიტექტურის დამალვა - ეს ერთერთი პირველადი საშუალებაა ინფორმაციული შეტევის საშუალებების გამოყენებისგან თავის დასაცავად.

უმარტივესი პროგრამული საშუალების lnterMute მუშაობას, რომელიც ასრულებს პროქსი-სერვერის ფუნქციას, გაეცნობით მოცემული თავის პრაქტიკულ სამუშაოში. პროგრამა ფონურ რეჟიმში მუშაობს და ასრულებს მოწოდებული ვებ-რესურსების შინაარსის შემოწმებას. კერძოდ, ის კომპიუტერზე cookie მარკერების დაბლოკის საშუალებას იძლევა და აანალიზებს ვებ-გვერდების გაფორმების ელემენტებს.

დასკვნა

სამეურნეო საქმიანობის დროს ხანდახან საწარმოებს შორის აუცილებელი ხდება ნაღდი ანგარიშსწორება. ჩვეულებრივად ეს დაკავშირებულია გადახდის დაჩქარებასთან. ამ შემთხვევაში მხარეები არ თავისუფლდებიან პირველადი დოკუმენტების (საკასო ჩეკები, ანგარიშ ფაქტურები და სხვა) შენახვის ვალდებულებებისაგან შემდგომი აღრიცხვისა და კონტროლისათვის, მაგრამ გამოირიცხულია ბანკის მხრიდან მიმღებისა და გადახდის დანიშნულების აღრიცხვის აუცილებლობა, რაც ამაღლებს ანგარიშსწორების ოპერატულობას. ასეთი ნაღდი ანგარიშსწორების იმიტირება იურიდიულ პირებს შორის შესაძლებელია ელექტრონული ფორმითაც. ამის აუცილებლობა არსებობს ელექტრონული კომერციის B2B მოდელში.

მოდელი, რომლის დროსაც გარიგების ორივე მონაწილე თავისთან ინახავენ გადახდის დოკუმენტებს, ხოლო ბანკი მათ არ ინახავს დაფუძნებულია ბრმა ხელმოწერის მექანიზმზე. ბრმა ხელმოწერის მექანიზმი ტექნიკურად დაფუძნებულია არასიმეტრული კრიპტოგრაფიის (ხელმოწერის) RSA ალგორითმის უნიკალურ მათემატიკურ თვისებაზე. განვიხილოთ ეს თვისებები მაგალითზე.

1. პირველ ეტაპზე გადამხდელი თვითონ ქმნის ნებისმიერი ღირებულების ელექტრონულ კუპიურას, მაგ. 333$. დამატებითი მონაცემების რანგში მასში შეაქვს თავისი მონაცემები, მონაცემები მიმღებზე და გადახდის დანიშნულებაზე.

2. შემდეგ გადამხდელი მიღებულ დოკუმენტს შიფრავს თავისი პირადი (დახურული) გასაღებით. ამის შემდეგ მას შეეძლო ეს კუპიურა გაეგზავნა თავის ბანკში დასამოწმებლად, მაგრამ ბანკს შეუძლია მიიღოს ყველაფერი, რაც ჩაწერილია ელექტრონული კუპიურის ფაილში კლიენტის საერთო (ღია) გასაღებით. ამიტომ გადამხდელს შემოაქვს დამატებითი ეტაპი.

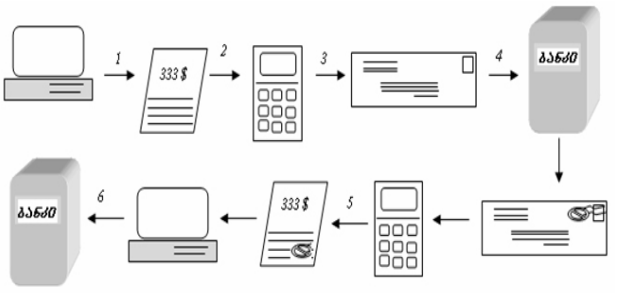
3. დაშიფრული შეტყობინების თითოეული სიმბოლო მრავლდება რაიმე ნებისმიერ რიცხვზე. ეს დაშიფვრის თითქოს დამატებითი ეტაპია. შიფრის დაცვის თვალსაზრისით ეს რათქმა უნდა პრიმიტიულია, მაგრამ საკმარისი, რომ დოკუმენტი თვალში არ მოხვდეს ბანკის თანამშრომელს.

ანალოგიურ მაგალითს ადგილი აქვს ჩვეულებრივი საფოსტო კავშირისას. საფოსტო კონვერტი პრიმიტიული დაცვაა, მაგრამ სრულიად საკმარისი, რომ წერილის შინაარსი თვალში არ მოხვდეს ფოსტის თანამშრომელს.

4. ბანკი გადამხდელისაგან იღებს რაღაც არაწაკითხვად ფაილს თხოვნით დაამოწმოს იგი როგორც 333 $ ღირებულების ელექტრონული კუპიურა. ბანკი ჩამოწერს ამ თანხას გადამხდელის ანგარიშიდან და შიფრავს ფაილს თავისი დახურული გასაღებით, რის შემდეგაც უბრუნებს ფაილს გადამხდელს.

5. გადამხდელი აღადგენს დაშიფრულ შეტყობინებას გაყოფს რა შეტყობინების თითოეულ სიმბოლოს მისთვის ცნობილ რიცხვზე. ამასთან ბანკის ელექტრონული ხელმოწერა არ ირღვევა - სწორედ ამაში მდგომარეობს არასიმეტრული კრიფტოგრაფიის ალგორითმის უნიკალურობა. შედეგად გადამხდელი იღებს გადახდის დოკუმენტს დაშიფრულს საკუთარი დახურული გასაღებით და კიდევ ბანკის დახურული გასაღებით. ამ დოკუმენტს ის გადაუგზავნის თანხის მიმღებს.

6. თანხის მიმღები იყენებს ბანკის და გადამხდელის ღია გასაღებებს ფაილის გასახსნელად. მას შეუძლია თავის ბანკს ეს ფაილი წარუდგინოს შესაბამისი თანხის თავის ანგარიშსწორების ანგარიშზე ჩასარიცხად, ამასთან მას რჩება გადამხდელის მიერ ხელმოწერილი დოკუმენტი, რომელშიც მოტანილია საბუღალტრო აღრიცხვისათვის საჭირო ყველა მონაცემები.



ნახ 2. ურთიერთ ანგარიშსწორების მოდელები ელექტრონული ხელმოწერის მექანიზმის გამოყენებით

გამოყენებული ლიტერატურა:

1. Дика В.В., Банковские информационные системы. М, 2006.

2. Гобарева Я.Л., Кочанова Е.Р., Нестерова Т.Н. М., Банковские информационные системы 2005.

3.თურქია, ე. (2008). ელექტრონული ბიზნესი (მართვის ავტომატიზირებული სისტემების კათედრა).

4. Andam, Z.R. (2003). e-commerce and e-business.

5. Davies, G .,& Wales, P. (2002). A History of Money From Ancient Times to the Present Day. 3rd edition.

6. Mishkin, F.S.(2009). The Economics of money, banking and Financial markets. 9th edition.

7. Singh, S. (2009) Emergency of payment systems in the age of electronic commerce:

8. The state of art - Global Journal of International Business Research Vol. 2. No. 2.

9. Андреев, А. Л .,& Торохов, В.А. (1998) Пластиковые карты.

10. Козье, Д. (1999). Електронная комерция.

11. ინტერნეტ წყარო:

http://library.thinkquest.org/28718/history.html#Barter

http://projects.exeter.ac.uk/RDavies/arian/amser/chrono1.html

http://www.historyworld.net/wrldhis/PlainTextHistories.asp?historyid=ac19

http://www.mfeurasia.com/

http://www.bloomberg.com/