ელექტრონული საგადახდო სისტემები და მათი განვითარებისტენდენციები

თალიკო ჟვანია, ზვიად საჯაია
საქართველოსტექნიკურიუნივერსიტეტი

რეზიუმე

განხილულიაელექტრონული საგადახდო სისტემების განვითარების ტენდენციები. აღწერილიათანამედროვე ელექტრონული საბანკო გადახდების EFTსისტემა, ამ სისტემისადმი წაყენებული მოთხოვნები, საინფორმაციო უსაფრთხოების უზრუნველყოფის საკითხები.ფორმალიზებულია ის ძირითადი პრობლემები და მათი გადაწყვეტის მექანიზმები, რომლებიც უზრუნველყოფს საგადახდო ინფორმაციის დაცულობას.

საკვანძოსიტყვები:ელექტრონულისაგადახდოსისტემა.ელექტრონულიგადახდებისუსაფრთხოება.

1. შესავალი

XX საუკუნის 60-70-იან წლებშიბანკებმა ელექტრონული გადარიცხვებისათვის სატელეკომუნიკაციო ქსელების წარმატებით გამოყენება დაიწყეს და შესაბამისად გაჩნდა ცნება - ელექტრონული გადახდები. იმ პერიოდში შეიქმნა პირველი ელექტრონული ტერმინალური მოწყობილობები:POS-ტერმინალები და ბანკომატები. ელექტრონული გადახდების ისტორია მჭიდროდ არის დაკავშირებული საბანკო ბარათებთან, რომლებიც გახდა მათი მამოძრავებელი ძალა. ჯერ კიდევ 1980 წლისათვის გამოშვებულ იქნა 73 მილიონი VISA და 55 მილიონი MasterCard პლასტიკური პარათი.

80-90-იანი წლების დასაწყისში პლასტიკური ბარათი, რომელზეც მაგნიტური ზოლი იყო დატანებული, ფაქტობრივად ელექტრონული ანგარიშსწორების ერთადერთი ინსტრუმენტი იყო, ხოლო ელექტრონული საბანკო ოპერაციები ძირითადად შემოიფარგლებოდა ბანკომატებიდან და ბანკის ოფისებიდან ნაღდი ფულის გამოტანით, სავაჭრო და მომსახურების ობიექტებში საქონლისა და მომსახურების საფასურის გადახდით, ბანკთაშორისი ანგარიშსწორების და კლიენტების (იურუდიული პირების) დისტანციური მომსახურებით.ბუნებრივია, ამ პერიოდსათვის მსოფლიოში ჩამოყალიბდა მსხვილი საპროცესინგო ცენტრების ინსტიტუტი, რომელიც უზრუნველყოფს ელექტრონულ გადახდებსა და მათშორის ანგარიშსწორებას. ასეთი მიდგომა ბანკებისგან ნაკლებ დანახარჯებს მოითხოვდა,ვიდრე საკუთარი საპროცესინგო ცენტრების შექმნა.ამასთან, ბანკებს საშუალება არ ჰქონდა, საკუთარ კლიენტთათვის შეეთავაზებინა ექსკლუზიური ელექტრონული მომსახურება.

90-იან წლებში საინფორმაციო ტექნოლოგიების, სატელეკომუნიკაციო სისტემების სწრაფმა ზრდამ და ინტერნეტმა, როგორც საქონლისა და მომსახურების გაყიდვების არხების ერთ-ერთმა უმნიშვნელოვანესმა საშუალებამ, განაპირობეს ელექტრონული გადახდების ბაზარზე სიტუაციის მკვეთრი ცვლა.

1993 წელს ჰოლანდიის კვლევითი ინსტიტუტის CWI (Centrum voor Wiskunde en Informatica) კრიპტოგრაფიის განყოფილების ხელმძღვანელმა - დევიდ ჩაუმ,,ელექტრონული ფულის" იდეოლოგიის რეალიზაციის მიზნით პრინციპულად ახალი ტექნოლოგია შეიმუშავა - სისტემა eCash, რომელიც ამჟამად გამოიყენება ბევრ ელექტრონული ანგარიშსწორების სისტემაში. 1994 წელს ამერიკის შეერთებულ შტატებში eCash ტექნოლოგიის გამოყენებით ინტერნეტით პირველი შეძენა განხორციელდა,ხოლო საუკუნის დასასრულს უკვე ასობით ელექტრონული ანგარიშსწორების სისტემა ფუნქციონირებდა.

ელექტრონული გადახდების ბაზრის ზრდა - ეს არის ობიექტური პროცესი. კვლევების თანახმად, დღეს მსოფლიოში, მაგალითად, ინტერნეტბანკის სისტემას იყენებს დაახლოებით 200 მილიონი ადამიანი. მსოფლიო ბანკის ექსპერტები მიიჩნევენ, რომ განვითარებულ ქვეყნებში ინტერნეტბანკის

სისტემის მომხმარებელთა რაოდენობა 2013 წელს მოსახლეობის 90%-ს გადააჭარბებს.ასეთი პროგნოზების საფუძველს ელექტრონული გადახდების მსოფლიო ბაზრის ზრდის სწრაფი ტემპები იძლევა.

კლიენტთა მომსახურების ელექტრონული არხები და ელექტრონული საგადახდო ინსტრუმენტები მუდმივად ვითარდება. დღეს მომხმარებელს შეუძლია ისარგებლოს ისეთი მომსახურების საშუალებებით, როგორიცაა: ბანკომატები, POS-ტერმინალები, ინტერნეტი, მობილური ტელეფონები, ჯიბის პერსონალური კომპიუტერები, ხოლო საგადახდო ინსტრუმენტებად გამოიყენოს:- პლასტიკური ბარათები, ელექტრონული ჩეკები, ციფრული ფული, სმარტ-ბარათები და ა.შ.

ბანკების ფილიალები სულ უფრო მეტად ემსგავსება ფინანსურ „სუპერმარკეტებს", რადგან ბანკის ფილიალების-„მაღაზიების“ ფართო ქსელის გაშლა გასაგები მიზეზების გამო შეზღუდულია. საბანკო მომსახურების ადვილად წვდომისათვის ბანკები სულ უფრო აქტიურად ქმნის მინი ოფისების ქსელებს, რომლებიც აღჭურვილია ელექტრონული ტერმინალებითა და თვითმომსახურების ელექტრონული საშუალებებით. ისინი ოფისების გარეთ განლაგებულ ოფისების ფართო ქსელს ქმნიან.

2. ძირითადი ნაწილი

ელექტრონული გადახდების ბაზრის თანამედროვე მდგომარეობა და განვითარების პერსპექტივები ხასიათდება შემდეგი ტენდენციებით:

– ელექტრონული ტერმინალური მოწყობილობებისა და ელექტრონული გადახდის არხების სპექტრი ბოლო პერიოდში მნიშვნელოვნად გაფართოვდა და მომავალშიც გაფართოვდება. გარდა ტრადიციული ბანკომატებისა და POS-ტერმინალებისა, ისინი უკვე მოიცავსფულის ბანკნოტების მიმღებ მოწყობილობებს, ვებ-ს(Web), ვაპ-ს(Wap), მობილურ ტელეფონებს, თვითმომსახურების ტერმინალებს და ა.შ. კლიენტისთვის ერთი და იმავე მომსახურება უნდა იქნეს შეთავაზებული სხვადასხვა ტერმინალური მოწყობილობებისა და საგადახდო ინსტრუმენტების გამოყენებით;

– მნიშვნელოვნად გაიზარდა ბანკების მიერ სხვადასხვა ელექტრონული ტერმინალების გამოყენებით შეთავაზებული მომსახურება. ეს არის არა მარტო ნაღდი ფულის მოხსნა და შეძენილი საქონლის ან მომსახურების ღირებულების გადახდა, არამედ ყველა სახის გადასახადის გადახდა, გადარიცხვები, სესხის დაფარვა, დეპოზიტების გახსნა/შევსება და ა.შ. ეს ტენდენცია გაგრძელდება მომავალშიც;

– სწრაფად იზრდება საგადახდო სისტემების რაოდენობა და სახეობები, რომელთა შორისაც საჭიროა ურთიერთშეთანხმებული ქმედება. თუ ცოტა ხნის წინ მხოლოდ „საბარათე" საგადახდო სისტემები არსებობდა, დღეს უკვე არსებობს გადახდების მიმღები სისტემებიც, გადარიცხვების სისტემებიც, ინტერნეტ-მაღაზიებიც და ა.შ.;

– მომხმარებლები ცდილობენ, ელექტრონული ტერმინალების გამოყენებით მიიღონ საბანკო და სხვა მომსახურების ფართო სპექტრი, რადგანაც ეს მათთვის მოსახერხებელი და იაფი საშუალებაა (ხშირად უფასოც). ბანკებისათვის ელექტრონული მომსახურების არხების გამოყენება, როგორც წესი, უფრო იაფი, მასშტაბური და მობილურია, ვიდრე ოპერატორის მიერ მომხმარებლის მომსახურება. ამიტომელექტრონული გადახდების მნიშვნელობა და მოცულობა, რომელიც, როგორც წესი, დროის რეალურ რეჟიმში ხორციელდება, მუდმივად იზრდება;

– იზრდება ბანკების მოთხოვნილება, თავის მომხმარებელს შესთავაზოს უნიკალური ელექტრონული მომსახურება. ბანკებისათვის აღარ არის საკმარისი, კლიენტებს შესთავაზონ ერთნაირი პროდუქტებიდა ჩნდება ექსკლუზიური ელექტრონული მომსახურების შეთავაზების აუცილებლობა. ყველა ეს ტენდენციაუბიძგებს ბანკებს, კლიენტთა მოზიდვა/შენარჩუნებისა და დანახარჯების შემცირების მიზნით, საკუთარი სახსრებით განახორციელონ ელექტრონული საბანკო გადახადების ავტომატიზაცია.

მართალია, ელექტრონული გადახდები საინფორმაციო ტექნოლოგიებისპროგრესისშედეგია, მაგრამ, თავის მხრივ, ელექტრონული გადახდები წარმოადგენს ამ პროგრესის ერთ-ერთ მამოძრავებელ ძალას და საინფორმაციო ტექნოლოგიებს უყენებს ახალ-ახალ მოთხოვნებს.ეს მოთხოვნები მრავალმხრივია: საკომუნიკაციო საშუალებებისა და გამოთვლითი ტექნიკის განვითრების აუცილებლობა, ახალი, უფრო დახვეწილი ალგორითმებისა და კრიპტოგრაფიული დაცვის საშუალებების შემუშავება და სხვა.

განვიხილოთ თანამედროვე ელექტრონული საბანკო გადახდების **EFT** (Electronic Funds Transfer - ფულადი სახსრების ელექტრონული გადარიცხვა) სისტემები და მოთხოვნები, რომლებიც ამ ტიპის სისტემების ავტომატიზაციის პროცესს წაეყენება.

EFTსისტემების ერთი-ერთ მნიშვნელოვან მახასიათებელს წარმოადგენს მათი ინტეგრირების შესაძლებლობები. EFTსისტემები უნდა ურთიერთქმედებდნენ მომსახურების სხვადასხვაგვარ ტერმინალურ მოწყობილობებთან, საპროცესინგო სისტემასთან, საგადახდო სისტემებთან და სხვადასხვა მიზნობრივი დანიშნულების ქსელებთან (საბარათე, გადახდების მიმღები, გადარიცხვების მიღება/გაცემის, ინტერნეტ-ექვაირინგის და ა.შ.) და, რაც მთავარია, საკრედიტო ორგანიზაციების ბექ-ოფისისა და ფრონტ-ოფისის სისტემებთან (ავტომატიზირებული საბანკო სისტემები, ABS).

ბუნებრივია, ელექტრონული გადახდების საინფორმაციო უსაფრთხოების უზრუნველყოფა EFTსისტემის განუყოფელი ფუნქციაა. ამასთან მნიშვნელოვანია ინფორმაციული უსაფრთხოების მოთხოვნათა შესრულების უზრუნველყოფა (როგორც საკრედიტო ინსტიტუტის, ასევე სხვადასხვა საგადახდო სისტემების) ელექტრონული გადახდის მთელ გზაზე - ტერმინალიდან მისი ავტორიზაციის ცენტრამდე და პირიქით.

EFTსისტემის ფუნქციონალურ შესაძლებლობების მიმართ მოთხოვნები შეიძლება დაიყოს საერთო და სპეციალურ მოთხოვნებად. საერთო მოთხოვნებს უნდა აკმაყოფილებდეს ნებისმიერი EFTსისტემა. მათ მიეკუთვნება, უპირველეს ყოვლისა, ელექტრონული ტრანზაქციების მარშრუტიზაცია და ავტორიზაცია (პროდუქტის შემოწმება, ლიმიტების კონტროლი და ა.შ.), საკომისიოსა და მოსაკრებლების გათვლა, მონაცემთა მომზადება გადახდების გაანგარიშებისათვის და ა.შ. EFTსისტემების სპეციალური მოთხოვნები მათი კონკრეტული დანიშნულებით განისაზღვრება: საბარათე EFT-სისტემებისათვის იქნება ერთი ტიპის მოთხოვნები, გადახდების მიმღები სისტემებისათვის - მეორე, გადარიცხვების მიღება/გაცემის სისტემებისათვის - მესამე. თუმცა, ბანკების უმეტესობა საჭიროებს უნივერსალურ EFTსისტემას, რათა უზრუნველყოს თავისი კლიენტების ელექტრონული და ექსკლუზიური მომსახურების ფართო სპექტრი: საბანკო ბარათებთან მუშაობა, ონლაინ გადახდების მიღება, სესხების დაფარვა თვით მომსახურების ტერმინალებით და ა.შ.

უნივერსალური EFTსისტემის ბიზნეს-არქიტექტურა უნდა იყოს მოქნილი და გაფართოვებადი.სასურველია, ბანკს შეეძლოს, იძენს რა EFT-სისტემას, მაგალითად, თვითმომსახურების ტერმინალებში გადახდების მისაღებად, შემდგომში ტექნოლოგიური პლატფორმის შეცვლის გარეშე გამოიყენოს იგი ონლაინ გადარიცხვების მიღება/გაცემისათვის.

EFTსისტემების მიმართ ზემოთ ჩამოთვლილი ბევრი მოთხოვნა შესაძლებელია გადაწყდესპროგრამული უზრუნველყოფის შემუშავების მიმართ თანამედროვე არქიტექტურული მიდგომებით. თანამედროვე ბანკებისათვის პროგრამული უზრუნველყოფის მსოფლიოში წამყვანი მიმწოდებლები თანდათან გადადიან სერვისზე ორიენტირებული არქიტექტურის (SOA) გამოყენებაზე, როგორც IT გადაწყვეტილებების ბაზისზე. კერძოდ, გამოკითხვის შედეგები აჩვენებს, რომ 80% ევროპული ბანკებისა ან უკვე გამოიყენებენ საკუთარ IT-არქიტექტურაში SOA-ს პრინციპებს, ან გეგმავენ მათ დანერგვას უახლოეს მომავალში.

ელექტრონული გადახდების უსაფრთხოება. სტატისტიკური მონაცემებით, ყველაზე ხშირად თავდასხმა ხორციელდება შემდეგ სისტემებზე: ტერმინალებზე (32%), მონაცემთა ბაზების სერვერებზე (30%), აპლიკაციების სერვერებზე (12%), ვებ-სერვერებზე (10%); სამუშაო სადგურებზე, აუტენტიფიკაციის სერვერებზე,სარეზერვო კოპირების სერვერებზე, ფაილ-სერვერებზე და სხვა (ერთად მხოლოდ 10%). აღნიშნული სტატისტიკიდან გარკვევით ჩანს საიტებისა და აპლიკაციების უსაფრთხოების აქტუალურობა, რადგანაც მათი დაუცველობის გამო ხშირად ხდება შესაძლებელი მონაცემების წვდომა.

რა უზრუნველყოფს საგადახდო სისტემების უსაფრთხოებას? ვებ-გვერდზე SSL (*Transport Layer Security*) სერტიფიკატის არსებობა არ არის საკმარისი პირობა უსაფრთხო ინტერნეტ-გადასახადების საწარმოებლად. მხოლოდ კომპლექსური მიდგომა იძლევა საშუალებას, ითქვას, რომ სერტიფიცირებული თანამედროვე საერთაშორისო სტანდარტებითინტერნეტ-გადახდების დამუშავება მაღალ დონეზეა უზრუნველყოფილი.მომხმარებელთა დაცვას უზრუნველყოფს:

– სისტემაში შესასვლელი სახელი/პაროლი, რომელიც გადის ტესტირებას სირთულეზე;

– საბანკო ბარათის ნომრის, მოქმედების ვადის, მფლობელის სახელის, CVV/CVC კოდების კომბინაცია;

– ინტერნეტ-გადასახადების განხორციელებისათვის ვირტუალური ბარათის შექმნის უნარი, რომელიც დუბლირებას უკეთებს ძირითად ბარათს.

ქვემოთ ჩამოთვლილია ის ძირითადი წესები,რომლებსაც მყიდველი უნდა იცავდეს:

– არასოდეს არავის შეატყობინოთპაროლი, მათ შორის საგადახდო სისტემების თანამშრომლებს;

– დარწმუნდით, რომ კავშირი მართლაც ხორციელდება SSL დაცულ რეჟიმში - თქვენი ბრაუზერის ქვედა მარჯვენა კუთხეში უნდა ჩანდეს დახურული ბოქლომის ნიშანი;

– დარწმუნდით, რომ კავშირი განხორციელდა საგადახდო სისტემის მისამართთან ან ინტერნეტ-ბანკთან;

– არასოდეს შეინახოთ ინფორმაცია პაროლის შესახებ ნებისმიერ ინფორმაციის მატარებელზე, მათ შორის კომპიუტერში. თუ თქვენ გაგიჩნდათ ეჭვი, რომ ვინმემ მოიპოვა თქვენი პირად ანგარიშის წვდომა, შეცვალეთ პაროლი ან დაბლოკეთ თქვენი ანგარიში;

– მუშაობის დასრულების შემდეგ აუცილებლად დააჭირეთ გასვლის ღილაკს;

– დარწმუნდით, რომ თქვენი კომპიუტერი არ არის დავირუსებული. დააყენეთ და გააქტიურეთ ანტივირუსული პროგრამა. ეცადეთ მათ მუდმივად განახლებას, რადგან ვირუსის მოქმედება შეიძლება მიმართულ იყოს თქვენი პაროლის შესახებ ინფორმაციის მოსაპოვებლად;

– გამოიყენეთ პროგრამული უზრუნველყოფის სანდო და საიმედო წყაროები და რეგულარულად განახორციელეთ მათი განახლება.

თავის მხრივ ელექტრონული საგადახდო სისტემის ტექნიკური დაცვა მოიცავს:

– საგადახდო სერვისის კლიენტის ფიქსირებულ IP-მისამართთან და ტელეფონის ნომერთან მიბმას;

– სისტემაში კლიენტის წვდომის განხორციელებასHTTPS/SSL დაშიფრული ოქმის მეშვეობით;

– ვირტუალური კლავიატურის გამოყენების შესაძლებლობას საიდენტიფიკაციო მონაცემების შესაყვანად;

– ტრანზაქციის ფორმირებისა და ავტორიზაციის არხების გაყოფას;

– ტრანზაქციის ავტორიზებას სპეციალური კოდის მეშვეობით, რომელიც მოკლე ტექსტური შეტყობინების (SMS) სახით კლიენტს მიეწოდება გადახდის განხორციელების შემდეგ მობილურ

ტელეფონზე (ასოებისა და ციფრებისა შემთხვევითი კომბინაცია, რომელიც მოქმედებს მხოლოდ რამდენიმე წუთის განმავლობაში).

ბოროტმოქმედები ყველაზე ხშირად ცდილობენ, მიიღონ წვდომა ბარათის მონაცემებზე. საგადახდო უსაფრთხოების სფეროში უსაფრთხოების სპეციალისტების ანგარიშებში მითითებული სტატისტიკით,100-დან საშუალოდ 91 შემთხვევაში შეტევების მიზანი იყო საბარათე მონაცემები.

საინფორმაციო უსაფრთხოების თვალსაზრისით ელექტრონული გადახდების სისტემებში არსებობს შემდეგი დაუცველი ადგილები:

– საგადახდო დავალებების გადაცემა ბანკსა და კლიენტს შორის,ბანკსა და ბანკს შორის;

– ინფორმაციის დამუშავება გამგზავნი და მიმღები ორგანიზაციის შიგნით;

– კლიენტების წვდომა ანგარიშებზე აკუმულირებულ სახსრებთან;

– ერთ-ერთ ყველაზე დაუცველ ადგილს ელექტრონული გადახდების სისტემაში წარმოადგენს საგადახდო და სხვა ინფორმაციის გადაგზავნა ბანკებს შორის, ბანკსა და ბანკომატს შორის, ბანკსა და კლიენტს შორის.

საგადახდო ინფორმაციის გადაცემისას უცილ;ებელია დაცულ იქნეს უსაფრთხოების შემდეგი ძირითადი მოთხოვნები:

– გამგზავნ და მიმღებ ორგანიზაციათა შიდა სისტემები უნდა იყოს ადაპტირებული ელექტრონული დოკუმენტების გაგზავნისა და მიღებისათვის. ამასთან, უნდა უზრუნველყოფდეს საჭირო დაცვას მათი დამუშავებისას ორგანიზაციის შიგნით;

– ელექტრონული დოკუმენტის გამგზავნისა და მიმღების ურთიერთქმედება უშუალოდ ხორციელდება კავშირის არხების საშუალებით.

გადახდების დაცვის ორგანიზებისას ხდება შემდეგი პრობლემების გადაწყვეტა:

– აბონენტთა ურთიერთამოცნობა (კავშირის დამყარებისას ურთიერთიდენტიფიკაციის პრობლემა);

– საკომუნიკაციო არხებით გადაცემული ელექტრონული დოკუმენტების დაცვა (დოკუმენტის კონფიდენციალურობისა და მთლიანობის უზრუნველყოფის პრობლემა);

– ელექტრონული დოკუმენტების გაცვლის პროცესის უსაფრთხოების დაცვა (დოკუმენტის გაგზავნისა და მიღების დადასტურებების პრობლემა);

– დოკუმენტის შესრულების უზრუნველყოფა (გამგზავნსა და მიმღებს შორის ურთიერთუნდობლობის პრობლემა, მათი სხვადასხვა ორგანიზაციასთან კუთვნილებისა და ურთიერთ დამოუკიდებლობის გამო).

ელექტრონული გადახდების ცალკეულ კვანძებზე ინფორმაციის დაცვის ფუნქციის უზრნველსაყოფად უნდა განხორციელდეს უსაფრთხოების შემდეგი მექანიზმები:სისტემების წვდომის მართვა;შეტყობინებათა მთლიანობის კონტროლი;შეტყობინების კონფიდენციალურობის უზრუნველყოფა;აბონენტთა ურთიერთაუტენტიფიკაცია;შეტყობინების ავტორობაზე უარის თქმის შეუძლებლობა;შეტყობინების მიწოდების გარანტია;შეტყობინებასთან დაკავშირებით ზომების მიღებაზე უარის თქმის შეუძლებლობა;შეტყობინებათა მიმდევრობის რეგისტრაცია;შეტყობინებათა მიმდევრობის მთლიანობის კონტროლი.

ზემოთ აღნიშნული პრობლემების გადაწყვეტის ხარისხი დიდ წილად განისაზღვრება კრიპტოგრაფიული საშუალებების რაციონალური არჩევანით დაცვის მექანიზმების რეალიზაციისას.

3. დასკვნა

ელექტრონული საგადახდო სისტემების მომსახურების მაღალი დონისა და მუშაობის საიმედოობის უზრუნველსაყოფად ძირითად ამოცანას წარმოადგენს ელექტრონული საგადახდო სისტემების უსაფრთხოების მართვის განაწილებული სისტემების სინთეზი, რომლებიც აერთიანებენ როგორც

ელექტრონულ საგადახდო სისტემაში ინფორმაციის მთლიანობის, წვდომის ადმინისტრირებისა და კონფედენციალურობის დაცვის შესაძლებლობებს, ასევე დინამიკური მონიტორინგისა და ქსელური ტრაფიკის ანალიზის ავტომატიზებულ საშუალებებს.

ლიტერატურა:

1. Abrazhevich D. Electronic payment systems: a user-centered perspective and interaction design. Technical Universiy Eindhoven. 2004.

2. Morten L. Bech, Rod Garratt. Illiquidity in the Interbank Payment System following Wide-Scale Disruptions. Thesis. Federal Reserve Bank of New York Staff Reports, no. 239. March 2006. JEL classification: C72, E58

3. Strategic Review of Innovation in the Payments System. Reserve Bank of Australia 2012.

ELECTRONIC PAYMENT SYSTEMS AND THEIR DEVELOPMENT TRENDS

Zhvania Taliko, Sajaia Zviad
Georgian Technical University

Summary

There are described the main tendencies of development of electronic payment systems in this article. Particularly, the modern electronic banking EFT payments system. There are also described requirements for this system, main questions of information security and are formalized basic problems and their solution mechanismswhich provides protection of payment information.

ЭЛЕКТРОННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ И ИХ ТЕНДЕНЦИИ РАЗВИТИЯ

Жвания Т., Саджаиа З.
Грузинский Технический Университет

Резюме

Рассмстриваются тенденции развития электронных платежных систем.Описаны современная электронная банковская платежная система EFT, требования к системе, вопросы информационной безопасности.Формализованы те основные проблемы и механизмы решения, которые обеспечивают защищенность платежной информации.