საქართველოს ტექნიკური უნივერსიტეტი

ხელნაწერის უფლებით

კახაბერ ჟამურაშვილი

ელექტრონული გადახდის სისტემებში უსაფრთხოების ნორმების შემუშავება და განვითარება

დოქტორის აკადემიური ხარისხის მოსაპოვებლად

წარდგენილი დისერტაციის

ა ვ ტ ო რ ე ფ ე რ ა ტ ი

სადოქტორო პროგრამა „ინფორმატიკა“ შიფრი 0401

თბილისი

2016 წელი

სამუშაო შესრულებულია საქართველოს ტექნიკურ უნივერსიტეტში
ინფორმატიკისა და მართვის სისტემების ფაკულტეტი
კომპიუტერული ინჟინერიის დეპარტამენტი

ხელმძღვანელები: პროფ. რომან სამხარაძე

რეცენზენტები: ----------

დაცვა შედგება ---------- წლის "------" ----------, --------- საათზე
საქართველოს ტექნიკური უნივერსიტეტის ----------
---------- ფაკულტეტის სადისერტაციო საბჭოს კოლეგიის სხდომაზე,
კორპუსი ----------, აუდიტორია ----------
მისამართი: 0175, თბილისი, კოსტავას 77.

დისერტაციის გაცნობა შეიძლება სტუ-ს ბიბლიოთეკაში,
ხოლო ავტორეფერატისა - ფაკულტეტის ვებგვერდზე

სადისერტაციო საბჭოს მდივანი პროფ. თინათინ კაიშაური

შესავალი

აქტუალობა. ინფორმაციული ტექნოლოგიების განვითარება XX საუკუნის მე-8 საოცრებად არის მიჩნეული, სწორედ ამიტომ აქტუალურია საკითხი თუ რამ განაპირობა ყოველივე ეს: ხალხის ინტერესმა, ეკრანისადმი მიჯაჭვულობამ თუ მიმდინარე საუკუნის რევოლუციურმა გამოგონებებმა, რომლებმაც შეცვალეს კაცობრიობის ცნობიერება, მათი ცხოვრების სტილის გამარტივებითა და სიახლეების მიმართ უწყვეტი სწავლის, ინტერესის სურვილითა და შესრულებით.

გასათვალისწინებელია მსოფლიოს წამყვანი ქვეყნების მაღილი ინტერესი და სხვადასხვა კულტურის წარმომადგენელი ერების ბაზრების ინტერესი, განავითაროწ და გაამრავლოწ საინფორმაციო ტექნოლოგიებში, გამოყენებული სიახლეები, ყურადსაღები და გასათვალისწინებელია, სწორედ ამიტომ გადავწყვიტე, შემეტანა წვლილი აღნიშნულ საკითხში და ჩავატარე კვლევა, თუ რამ გამოიწვია ყოველივე ეს.

კვლევის მიზანი. კვლევის მიზანია ელექტრონული ანგარიშსწორების მეთოდებში, უსაფრთხოების დონის ამაღღლება.

კვლევის ობიექტი. კვლევის ობიექტია საბარათე ანგარიშსწორების საშუალებები.

მეცნიერული სიახლე. მეცნიერული სიახლე მდგგმარეობს შემდეგში, ბარათების დაცვისთვის შემოღებულია ორი მაგნიტურზოლიანი სისტემა, რომლის თანახმად პაროლი იყოფა ორ ნაწილად, თითოეული ნაწილისთვის გამოიყენება დაშიფრვის სხვადასხვა მეთოდი და შემთხვევითი მეთოდით განისაზღვება სიმბოლოების პოზიციები პაროლში. ასეთი მიდგომა მკვეთრად ართულებს საბოლო პაროლის გამოცნობიის პროცესს და შესაბამისად ზრდის სისტემის დაცულობას.

კვლევის მეთოდები. გამოიყენება ავტორიზაციის, ინფორმაციის დაშიფრვისა და გაშიფრვის მეთოდები.

პრაქტიკული ღირებულება. სადისერტაციო ნაშრომის პრაქტიკული

ღირებულება შემდგომში მდგომარეობს. შემუშავებული მიდგომა, ელექტრონული ანგარიშსწორებისას იძლევა ავტორიზაციის მეთოდიკის დახვეწის საშუალებას, რაც შეიძლება წარმატებით გამოყენებულ იქნას, როგორც დაცვის სისტემების პროგრამული უზრუნველყოფის აგებისას, ასევე ანგარიშსწორებისა და საბარათე დაგროვების ნებისმიერ სისტემაში.

დღევანდელი კაცობრიობის ერთ-ერთ პრობლემად დროის სიმწირეა მიჩნეული, სწორედ ამან გახადა აქტუალური, ელექტრონული ინტერნეტ მაღაზიების იდეის ჩამოყალიბება და განხორციელება, ტექნოლოგიურ განვითარებას თუ დავაკვირდებით, აშკარა ცვლილებები თვალშისაცემად გამოჩნდება, თავდაპირველი ელექტრონული მაღაზიის უსაფრთხოების ნიშად სატელეფონო კოდი გახლდათ მიჩნეული, მომხმარებელი გამყიდველს თანხის ჩარიცხვას ტელეფონის საშუალებით (სატელეფონო კოდით) ახდენდა. დღესდღეობით ტექნოლოგია განვითარდა და საბარათე სისტემას ვიყენებთ, უსაფრთხოების ნორმების უზრუნველსაყოფად, თუმცა აქაც არის რიგი საკითხებისა როდესაც მომხმარებელი არ არის დაცული, და მისი ინფორმაცია შესაძლოა ჩავარდეს არაკეთილსინდისიერი პიროვნების ხელში, რაც მფლობელს მატერიალურად დააზარალებს.

ელექტრონული ანგარიშსწორების, რამოდენიმე მეთოდი არსებობს: ა). ვირტუალური დაგროვებადი ანგარიში ბ). ელექტრონული ანგარიში მიბმული საბანკო ანგარიშთან გ). საბანკო საბარათე სისტემა დ). სხვადასხვა დაგროვებითი საბარათე გადახდის სისტემები

მათი რაოდენობიდან და მოთხოვნიდან გამომდინარე აქტუალური გახდა უსაფრთხოების ნორმებისა და სტანდარტების დაწესება, თუმცა აღმოჩენილი ხარვეზები საშუალებას იძლევიან, არაკეთილსინდისიერი მომხმარებლების მხრიდან დაირღვას ინფორმაციული უსაფრთხოების და ე.გ.წ ელექრონული ანგარიშსწორებით მოსარგებლე კლიენტების მატერიალური ფასეულობათა უსაფრთხოება. ამიტომ, აღმოჩენილი ხარვეზები დაუყონებლივ საჭიროებს განხილვასა და გამოსწორებას, რათა შენარჩუნდეს განვითარებისა და სიახლეებისაკენ სწრაფვის ტემპი, რაც

საშუალებას მოგვცემს უფრო ეფექტური გავხადოთ თვითოეული ჩვენთაგანის საქმიანობა, და დავზოგოთ დრო რიგი მატერიალური საკითხების მოსაგვარებლად.

ნაშრომის შინაარსი

შესავალში დასაბუთებულია პრობლემის აქტუალურობა და ნაჩვენებია მეცნიერული კვლევების გააქტიურების აუცილებლობა აღნიშნული პრობლემების გადასაჭრელად.

პირველ თავში ჩატარებულია არსებული საბარათე დაცვის სისტემების მიმოხილვა და კრიტიკული ანალიზი, ნაჩვენებია მათი განვითარების ტენდენციები ნაჩვენებია, რომ არსებული საბარათე დაცვის სისტემები საჭიროებს დახვეწას და გაუმჯობესებას დასაბუთებულია, დაცვის არსებული სისტემების დახვეწისა და ახალი სისტემების შემუშავების აუცილებლობა.

თანამედროვე სამყარო შესულია დინამიკური ცვლილებების პერიოდში, რომლებიც, პირველ რიგში, გამოიხატება გლობალიზაციის პროცესებში და მოიცავს საზოგადოების ცხოვრების ყველა სფეროს, მათ შორის ფინანსებისა და კრედიტის სფეროს. აღნიშნული პროცესების გამო ფინანსური ინსტიტუტები განიცდიან გარკვეულ ზეწოლას და ეწევიან დამატებით რისკებს, რომლებიც აიძულებთ მათ განვითარებისა და მართვის სფეროში გარკვეულ ცვლილებებს. საქმიანობის ახალი პირობები მოითხოვს არამხოლოდ ტრადიციული საბანკო გადაწყვეტილებების აქტიურ გამოყენებას, არამედ მეცნიერებისა და ტექნიკის თანამედროვე მიღწევების დანერგვას, რომლებიც რეალიზებულია დისტანციური საბანკო მომსახურების ისეთ მეთოდებში, როგორიც არის,ინტერნეტბანკი და საბარათე ანგარიშსწორების საშუალებები.

ინტერნეტი (Internet – „ქსელთაშორისი“) – ინფორმაციული ინფრასტრუქტურაა, რომელიც სატელეკომუნიკაციო ქსელების მეშვეობით აკავშირებს კომპიუტერებს. ინტერნეტის პროტოტიპს წარმოადგენს 1960-1970-იანწლებში აშშ-ის თავდაცვის სამინისტროს შეკვეთით შექმნილი პირველი კომპიუტერული ქსელი ARPANET. ინტერნეტის შექმნა დაიწყო 1980-იან წლებში აშშ-ის ეროვნული სამეცნიერო ფონდის ინიციატივით.

ინტერნეტმა გააერთიანა აშშ-ის უნივერსიტეტების ათეულობით ათასი მკვლევარი და სტუდენტი. ქსელის საფუძველს წარმოადგენდა უნივერსიტეტების კომპიუტერული ცენტრები. ინტერნეტი საკმაოდ სწრაფად გახდა პოპულარული, ის გასცდა აშშ-ის საზღვრებს და გადაიქცა გლობალურ ინფორმაციულ ქსელად. 1995 წელს ინტერნეტი აკავშირებდა დაახლოებით 120 ათას კომპიუტერს, ხოლო ინტერნეტის მომხმარებელთა რიცხვმა 40 მლნ ადამიანს გადააჭარბა. 1999 წელს ინტერნეტთან მუდმივად დაკავშირებული კომპიუტერების, ე.წ. „ჰოსტების“ (host) ან „სერვერების“ (server) რაოდენობამ 320 ათასს გადააჭარბა, ხოლო ინტერნეტის აქტიურმა აუდიტორიამ – 113 მლნ ადამიანს. ინტერნეტ მომსახურებისათვის გამოყენებული ტექნოლოგიური პლატფორმა დღეს საქართველოში.

ჯერჯერობით კვლავ მზარდ ტექნოლოგიად მიიჩნევა. ერთის მხრივ, ჩვენი ქვეყანა ერთგვარად წინ მიიწევს ელექტრონული მმართველობის განვითარების კუთხით, თუმცა, მეორეს მხრივ, საქართველოში კვლავ არ არის აღმოფხვრილი ე.წ. “ციფრული დაშორება,” ანუ ინტერნეტის ხელმისაწვდომობის თანაბარი განვითარება ქალაქებსა და რეგიონებს შორის.

ინტერნეტის მომხმარებელთა რიცხვი ძალიან სწრაფი ტემპებით იზრდება. გაეროს ინფორმაციისა და საკომუნიკაციო ტექნოლოგების სპეციალიზებული სააგენტოს, საერთაშორისო სატელეკომუნიკაციო კავშირის (ITU) გამოთვლებით, ინტერნეტი საქართველოს მოსახლეობის 45%-სთვის არის ხელმისაწვდომი.

ინტერნეტის სწრაფი ზრდის ძირითადი მიზეზებია: ფასების შემცირება აპარატურულ და პროგრამულ უზრუნველყოფასა და საკომუნიკაციო მომსახურებაზე, აგრეთვე ინტერნეტის განვითარების სტიმულირება განვითარებული ქვეყნების მთავრობების მხრიდან (ძირითადად, აშშ-ის, ხოლო ბოლო წლებში – ევროპის ქვეყნების მთავრობების მხრიდანაც).

საბანკო ორგანიზაციები წარმოადგენენ ფინანსური მომსახურების სამი ძირითადი სახის მომწოდებლებს: სატრანზაქციო, პორტფელური და საოპერაციო მომსახურების.

პორტფელური მომსახურება დაკავშირებულია ბანკების, როგორც სასესხო-შემნახველი ფინანსური ინსტიტუტების, ტრადიციულ საქმიანობასთან. პორტფელურ მომსახურებას მიეკუთვნება კლიენტებზე სესხების გაცემა (კრედიტები) და ფულადი სახსრების მიღება ანაბრებისთვის (დეპოზიტები). ბანკები ახდენენ დროებით თავისუფალი რესურსების აკუმულირებას დეპოზიტების სახით და ანაწილებენ მათ კრედიტების ფორმით. ამ მომსახურების გაწევით ბანკები გადაანაწილებენ რესურსებს დაზოგვის მსურველი პირებიდან სესხების მსურველი პირებისათვის და ამით უზრუნველყოფენ საწარმოებს დამატებითი ფინანსური რესურსებით. მომსახურების ეს სახე განასხვავებს ბანკებს სხვა ფინანსური შუამავლებისგან. ბანკების შემოსავლების დაახლოებით 70% საკრედიტო-სადეპოზიტო მომსახურების გაწევის შედეგად წარმოიქმნება სატრანზაქციო მომსახურება – ეს არის მომსახურება გარიგებების უფრო ეფექტიანად შესრულებისათვის. ამ ფუნქციის შესრულებისას, ბანკები გვთავაზობენ გარიგებების მომსახურების ორ ძირითად ტიპს:

1. აწარმოებენ ანგარიშსწორების სისტემას, რომელშიც ფასეულობების გადაადგილებას თან ახლავს შესაბამისი ბუღალტრული გატარება. ამ დროს გვერდით პროდუქტად წარმოგვიდგება ინფორმაციის მიწოდება კლიენტების გადახდებზე, შემოსულობებსა და დარიცხულ პროცენტებზე;
2. უზრუნველყოფენ ვალუტის კონვერტაციას (კლიენტების დეპოზიტები, ანაბრები და სხვა აქტივები კონვერტირდება ვალუტაში).

სატრანზაქციო ფუნქციის შესრულებისას, ბანკები გვთავაზობენ გაცვლითი ოპერაციების აღრიცხვის სისტემას (accounting system of exchange), რომელშიც სახსრების მოძრაობა რეგისტრირდება ბუღალტრული გატარებების ფორმით. ვალუტის გაცვლის მომსახურება მეორეხარისხოვანია და საზოგადოების მოძრაობისას უნაღდო

ანგარიშსწორებისა და დაშორებული ტერმინალებით კლიენტების მომსახურების მიმართულებით, იგი სულ უფრო ნაკლებად მნიშვნელოვანი ხდება.ამრიგად, გაცვლის ბუღალტრული მომსახურება – ეს არის გარიგების შესრულების უმნიშვნელოვანესი მომსახურება, რომელსაც გვთავაზობენ საფინანსო შუამავლები. სატრანზაქციო მომსახურება ტექნოლოგიურად ყველაზეტევადია, ამასთანავე, ის დამოკიდებულია მიწოდების ელექტრონულ არხებსა და ტელეკომუნიკაციებზე. ამიტომ ინტერნეტის, როგორც ახალი სატელეკომუნიკაციო არხის, გამოყენებით გამოწვეული ყველაზე რადიკალური ცვლილებები სწორედ მათ ეხება.

საოპერაციო მომსახურებას ბანკები იყენებენ, როგორც დამატებითი შემოსავლების წყაროს (მას „ფასიან მომსახურებასაც“ უწოდებენ). ფართო გაგებით, საოპერაციო მომსახურება წარმოადგენს საბანკო ლიკვიდობის გაყიდვას. მას მიეკუთვნება საინვესტიციო მომსახურება (მათ შორის სატრასტო), სადაზღვევო და სხვა ფასიანი მომსახურება, რომელსაც ბანკები კლიენტებს სთავაზობენ.

აღსანიშნავია, რომ მომსახურების დაყოფა სატრანზაქციო, პორტფელურ და საოპერაციო მომსახურებად, თეორიული ხასიათისაა. საბანკო საქმის განვითარებამ XX საუკუნის უკანასკნელ მეოთხედში, სხვადასხვა სახის მომსახურების შერწყმამდე მიგვიყვანა. დღეს ბანკები გასაყიდად გვთავაზობენ არა ცალკეულ მომსახურებას, არამედ მომსახურების პაკეტს, რომელსაც „საბანკო პროდუქტების“ სახელით მოიხსენიებენ. როგორც წესი, საბანკო პროდუქტი მოიცავს სამივე სახის (სატრანზაქციო, საკრედიტო-სადეპოზიტო და საოპერაციო) მომსახურებას. მაგალითად, პლასტიკური ბარათები გამოიყენება ანგარიშსწორების ოპერაციებისთვის (სატრანზაქციო კომპონენტი), მათზე არსებული ოვერდრაფტების დაფარვისათვის გამოიყენება სხვადასხვა სადეპოზიტო-საკრედიტო სქემები (პორტფელური კომპონენტი), ხოლო პლასტიკური ბარათის გამოყენებისთვის შეიძლება საჭირო გახდეს საკომისიოს გადახდა (როგორც საოპერაციო მომსახურებისათვის).

ერთის მხრივ, ინტერნეტი წარმოადგენს გლობალურ სატელეკომუნიკაციო ქსელს, ხოლო მეორე მხრივ – სპეციფიკურ ინფორმაციულ გარემოს. საბანკო მომსახურების ბაზარზე ინტერნეტის გავლენის გასაგებად საჭიროა ამ ორივე ასპექტის განხილვა. პირველი დაკავშირებულია საბანკო საქმეში ელექტრონული კომუნიკაციების გამოყენებასთან, ხოლო მეორე – ინტერნეტის ფართო ინტერაქტიულ შესაძლებლობებთან.

ელექტრონული საკომუნიკაციო ქსელები ბანკების მიერ გამოიყენება, როგორც საბანკო მომსახურების კავშირის და სადისტრიბუციო არხები (distribution/delivery channel). როგორც კავშირის არხი, ისინი გამოიყენება ბანკების მიერ სხვა ბანკებთან და საკუთარ ფილიალებთან ინფორმაციული

მეორე თავში განხილულია ქსელის ინფრასტრუქტურის დაგეგმარების თანამედროვე მეთოდები, განხილულია არსებული სისუსტეები, ზოგიერთ შემთხვევაში ნაჩვენებია პრობლემის გადაწყვეტის მიმართულებები, განხილულია სასერვერო ინფრასტრუქტურის მოდელები, შემოთავაზებულია, მათი შერჩევის კრიტერიუმები საბარათე სისტემებთან მიმართებაში, განხილულია სასერვერო ინფრასტრუქტურის საექსპლუატაციო პირობები და მათი ეფექტური მონიტორინგის საშუალებები, განხილულია კიბერუსაფრთხოების მიმართულებები, მოყვანილია სხვადასხვა ქვეყნის მაგალითები, შემოთავაზებულია დამცავი საშუალებები და მათი ეფექტური კონფიგურაციის და გამოყენების მიმართულებები.

ნაჩვენებია ექსპერტული სისტემის სტრუქტურა, რომელიც განკუთვნილია ტენიანობის ზუსტი გაზომვებისთვის მასალაში. ფორმირებულია ცოდნისბაზა, რომელიც პროდუქციული წესებისა და ფაქტებისაგან შედგება და ასახავს კვალიფიციური ტექნოლოგის ცოდნას.ექსპერტული სისტემა შედგება: პროცესორისაგან, რომელიც წარმოადგენს ცოდნის ბაზის მაკროქსელის თვლის აპარატს.

მაკროქსელის ცოდნის ბაზისაგან წარმოდგენილია ბლოკი ფაქტების შენახვის, წესებისა და მართვის, რომლებიც სტრუქტურირებულია ერთიან გარსში; ურთიერთქმედების და განმარტებების ბლოკისაგან, რომელიც აერთიანებს ინსტრუმენტების კომპლექტს, რათა ტექნოლოგმა უზრუნველყოს სისტემებს შორის ინტერაქტივობა; საანგარიშო ერთეულისაგან.

ადამიანებს შორის კომუნიკაცია მნიშვნელოვან როლს თამაშობს მათ ცხოვრებაში. მათ სჭირდებათ მიიღონ ინფორმაცია ერთმანეთზე, ახალ ამბებზე, ამინდზე, ფინანსურ მაჩვენებლებზე და ა.შ. ინფორმაციის მიღების და გადაცემის მეთოდები იცვლებოდა და ვითარდებოდა წლების განმავლობაში. ინფორმაციულ საუკუნეში რომელშიც ჩვენ ვცხოვრობთ ინფორმაციის დროული მიღება და ფლობა უაღრესად მნიშვნელოვანია. ამიტომ ინფორმაციის მიღებასა და გადაცემაში კომპიუტერული ქსელი უმნიშვნელოვანეს როლს თამაშობს. კომპიუტერული ქსელი ეხმარება ადამიანებს უსწარაფესად გადასცენ ინფორმაცია მსოფლიოს ნებისმიერ ადგილას. მსოფლიოში მონაცემების გადაცემა გახდა კომპიუტერული სისტემების ფუნდამენტური ნაწილი. კომპიუტერული ტექნოლოგიების სწრაფმა განვითარებამ მოითხოვა კომპიუტერული სისტემების საიმედო, სწრაფი და დაცული კავშირების უზრუნველყოფა. ამიტომ კომპიუტერული ქსელების დაპროექტების, აგების და მართვის სისტემები მნიშვნელოვან როლს თამაშობს თანამედროვე ინფორმაციულ ტექნოლოგიებში. ქსელების ფუნდამენტური პრინციპები და ტიპები რა არის ქსელი? - ქსელი (Network) - ინფორმაციის გაცვლისა და რესურსების ერთობლივად გამოყენებისათვის, ერთმანეთთან ფიქსირებულად ან/და მობილურად დაკავშირებული კომპიუტერების ჯგუფი. საინფორმაციო ქსელები ერთმანეთისაგან განსხვავდებიან სხვადასხვა შესაძლებლობებით, მაგრამ ყველა ქსელს გააჩნია ოთხი ძირითადი საერთო ელემენტი: – წესები (პროტოკოლი), თუ როგორ უნდა მოხდეს ინფორმაციის გაგზავნა და მიღება; ქსელში

გამოყენებული რესურსები - პროგრამები, მონაცემთა ფაილები, აგრეთვე პრინტერები და ქსელში სხვა ერთობლივად მოხმარებადი პერიფერიული მოწყობილობები. ქსელში შეიძლება იყოს გაზიარებული მრავალი ტიპის რესურსი - - სერვისები, როგორიც არის ამობეჭდვა და სკანირება. - მონაცემების შესანახი სივრცე და მოძრავი(removable) მოწყობილობები, როგორებიც არის მყარი და ოპტიკური დისკები - პროგრამები, მონაცემთა ბაზები. კომპიუტერული ქსელი წარმოადგენს ურთიერთდაკავშირებულ და შეთანხმებულად ფუნქციონირებად პროგრამული და აპარატურული კომპონენტების რთულ კომპლექსს. ის არის კომპიუტერების და პერიფერიული მოწყობილობების ერთიანობა, რომლებსაც სპეციალური საკომუნიკაციო საშუალებების და პროგრამული უზრუნველყოფის საშუალებით შეუძლიათ ინფორმაციის გაცვლა. კომპიუტერულ ქსელში კომპიუტერების რაოდენობა ორიდან რამდენიმე ათასამდე შეიძლება იცვლებოდეს. კომპიუტერული მონაცემთა ქსელი არის ჰოსტების(Host კვანძი) ერთობლიობა, დაკავშირებული ერთმანეთთან ქსელური მოწყობილობების საშუალებით. ჰოსტი არის ნებისმიერი მოწყობილობა რომელიც აგზავნის და ღებულობს ინფორმაციას ქსელში. ჰოსტებთან დაკავშირებულ მოწყობილობებს ეწოდებათ პერიფერიული მოწყობილობები. მაგ. პრინტერი დაკავშირებული ქსელში ჩართულ კომპიუტერთან. თუმცა თუ პრინტერი არის დაკავშირებული პირდაპირ ისეთ ქსელურ მოწყობილობასთან როგორიც არის კონცენტრატორი, კომუტატორი ან მარშრუტიზატორი, ამ შემთხვევაში პრინტერიც არის ჰოსტი. შესაძლებელია კომპიუტერული ქსელების კლასიფიკაციის მრავალი სხვადასხვა ხერხი, მათ შორის რაოდენობისა და ქსელის ზომის მიხედვით, მონაცემთა გადაცემის ტიპის მიხედვით, ინფორმაციის გადაცემის სიჩქარის მიხედვით. ქსელები შეიძლება დავყოთ 3 ძირითად კლასად: ლოკალური ქსელი (LAN - Local Area Network) - ერთმანეთთან დაკავშირებული, ერთი ადმინისტრირების ქვეშ მოქცეული კომპიუტერების შედარებით მცირე

ჯგუფი. მნიშვნელოვანია დავიმახსოვროთ, რომ ლოკალური ქსელის ელემენტები იმყოფება ადმინისტრირების ერთი ჯგუფის მართვის ქვეშ, რომელიც განსაზღვრავს ქსელში მომქმედ წვდომის მართვასთან დაკავშირებულ პოლიტიკასა და უსაფრთხოებას ამ კონტექსტში სიტყვა ”ლოკალური” მიანიშნებს ერთობლივ ”ლოკალურ” მართვას და არა კომპონენტებს შორის ფიზიკურ სიახლოვეს რეგიონალური ქსელი (MAN – Metropolitanl Area Network)- ქსელი, რომელიც აერთიანებს ბევრ ლოკალურ ქსელს ერთი რაიონის, ქალაქის ან რეგიონის ფარგლებში. გლობალური ქსელი (WAN – Wide Area Network)- ქსელი, რომელიც აერთიანებს სხვადასხვა ქალაქების, რეგიონების და სახელმწიფოების კომპიუტერებს. გლობალური ქსელის თვალსაჩინო მაგალითს წარმოადგენს ინტერნეტი (Internet). Internet-ი ეს გახლავთ ფართო გლობალური ქსელი, რომელიც თავის თავში მოიცავს მილიონობით ურთიერთდაკავშირებულ ლოკალურ ქსელს. ლოკალურ ქსელებს შორის კავშირის რეალიზაციას ახდენენ ტელეკომუნიკაციური მომსახურების მომწოდებლები. აღნიშნული რესურსების მიზნობრივად ეფექტურად და უსაფრთხოდ გამოყენებისათვის მნიშვნელოვანი მარშუტიზაციის სწორი პროტოკოლების შერჩევა და კონფიგურირება ასევე ფაირვოლისა და ვირტუალური ქსელების ურთიერთდაკავშირება, შესაბამისი მარშუტის გაწერა და მკაცრი ფაირვოლის კონფიგურაციის ამუშავება, რომელიც შეზღუდავს ნებისმიერ არა სასურველ პროტოკოლის, პორტისა და აიპი მისამართის გამოყენებას.

მესამე თავში წარმოდგენილია ორი მაგნიტურზოლიანი სისტემის ინფრასტრუქტურა, მონაცემთა ბაზების ორმაგი ავტორიზაციისათვის საჭირო ინფრასტრუქტურა, განხილულია ორმაგი შიფრაციისა და განშიფრვის მეთოდები, წარმოდგენილია კრიტიკული ანალიზი არსებულ შიფრაციისა და განშიფრვის მეთოდებთან დაკავშირებით, წარმოდგენილია მეცნიერული სიახლე ორიმაგნიტურ ზოლიანი ბარათისა და შიფრაციის მეთოდებში.

არსებობს DES-სტანდარტი აპარატული რეალიზაცია, რომელიც უზრუნველჰყოფს მაღალ მწარმოებლურობას. თავდასხმა მიუხედავად იმისა, რომ ამ ალგორთმზე გაცილებით მეტი კრიპტოანალიზია ჩატარებული, ვიდრე სხვებზე, მისი გატეხვის საუკეთესო გზად უხეში ძალის მეთოდი რჩება. მცირედი კრიპტოგრაფიული სისუსტეები და სამი თეორიული შეტევის შესაძლებლობა, რეალიზაციისათვის მოითხოვს ძალიან დიდი რაოდენობის მასალას ცნობილი და არჩეული ღია ტექსტით შეტევისათვის, რაც პრაქტიკულად შეუძლებლად მიიჩნევა.

ნებისმიერი შიფრისათვის არსებობს შეტევის მეთოდი - ყველა შესაძლო გასაღების გადარჩევა. შესაძლო გასაღებების სიმრავლეს განსაზღვრავს მისი სიგრძე. DES-ისთვის იგი წარმოადგენს 2^{56} სიმბოლოს. ალგორითმის პროექტირების პროცესში წამოიჭრა საკითხი გასაღების სიმოკლის გამო, რაც საფრთხეს წარმოადგენდა მომავალი კრიპტოანალიზის კუთხით. მაგრამ კონსულტაციების შედეგად, რომელშიც მონაწილეობას NSA-ც იღებდა, საბოლოოდ გადაწყდა, რომ გასაღების ზომა თავდაპირველი 128 ბიტიდან 56 ბიტამდე შემცირებულიყო.

DES-ის უხეში ძალით გასატეხად რამდენიმე მანქანა იქნა დაპროექტებული. 1977 წელს უიტფილდ დიფიმ და მარტინ ჰელმანმა დააპროექტეს 20 მილიონ დოლარად ღირებული მანქანა, რომესაც შეეძლო შიფრაციის გასაღების პოვნა ერთ დღეში. 1997 წელს ვინერმა წარმოადგინა მანქანის პროექტი, რომელსაც შეეძლო იგივეს გაკეთება 7 საათში. თუმცა არც ერთი ეს მანქანა არ ყოფილა პრაქტიკულად რეალიზებული. 1997 წელს RSA Security-ის მიერ გამოცხდებულ იქნა კონკურსი ალგორითმის გასატეხად, 100 ათასდოლარიანი პრიზით, რომელიც მოიგო DESCHALL Project-ის ჯგუფმა, რომელთაც ინტერნეტში განაწილებული გამოთვლების ქსელი გამოიყენეს. 1998 წელს გატეხვა მოახდინეს 250 ათას დოლარად ღირებული სპეციალურად აგებული მანქანით (EFF DES cracker), რომელმაც შიფრაციის გასაღების პოვნა 2 დღეში შეძლო.

2006 წელს გერმანიის ორმა საუნივერსიტეტო ჯგუფმა წარმოადგინა მანქანა, სახელად COPACOBANA, რომლის რირებულა 10,000 დოლარს აღწევს და შედგება ფართოდ ხელმისაწვდომი კომპონენტებისგან. COPACOBANA იყენებს XILINX Spartan3-1000-ის ტიპის 120 ცალ პროგრამირებადი ვენტილების მასივს (პვმ), რომლებიც პარალელურ რეჟიმში მუშაობენ. დღესდღეობით DES-ის გატეხვის სისწრაფის რეკორდი ეკუთვნის ფირმა SciEngines-ის აპარატს RIVYERA, რომელიც Spartan-3 5000-ის 128 პბმ-ს იყენებს. გაუმჯობესებული შეტევა არსებობს სამი შეტევის მეთოდი, რომლებიც თეორიულად უმჯობესია გასატეხად, ვიდრე უხეში ძალის მეთოდი: დიფერენციალური კრიპტოანალიზი, წრფივი კრიპტოანალიზი და დეივისის შეტევა. დიფერენციალური კრიპტოანალიზი აღმოჩენილ იქნა 1980 წელს ელი ბიჰემისა და ადი შამირის მიერ. ეს მეთოდი ცნობილი იყო IBM-ისა და NSA-სთვის, თუმცა ფაქტი საიდუმლოდ რჩებოდა. DES-ის 16-ივე ციკლის გასატეხად, დიფერენციალურ კრიპტოანალიზს ესაჭიროება 2^{47} არჩეული ღია ტექსტი. DES თავიდანვე პროექტირებულ იქნა ამ მეთოდის მიმართ მედეგობის გათვალისწინებით. წრფივი კრიპტოანალიზი შეიმუშავა მიცურუ მაცუიმ 1993 წელს და მოითხოვს 2^{43} ცნობილ ღია ტექსტს. თუმცა ამ ტიპის ანალიზის წარმატებული შედეგები ცნობილი არ არის. მრავალჯერადი წრფივი კრიპტოანალიზით შესაძლებელია კრიპტოანალიზის სირთულე კიდევ 4-ჯერ შემცირდეს (2^{41}) წინა ორი მეთოდისგან განსხვავებით, რომლებიც შიფრაციის ალგორითმთა ფართო წრეს ეხება, დეივისის შეტევა კონკრეტულად DES-ის წინააღმდეგაა მიმართული. ყველაზე ძლიერი ვერსია ანალიზისათვის ითხოვს 2^{50} ცნობილ ღია ტექსტს, აქვს 2^{50}გამოთვლითი სირთულე და 51% წარმატების ალბათობა. სხვა სისუსტეები არსებობს DES-ის 4 გასაღები (ე.წ. სუსტი გასაღები), რომელთათვისაც სრულდება პირობა $E_K(E_K(P)) = P$ ანუ $E_K = D_K$

ასევე არსებობს 6 ე.წ. ნახევრად სუსტი გასაღები, რომელთათვისაც

$$E_{K_1}(E_{K_2}(P)) = P \text{ ანუ } E_{K_2} = D_{K_1}.$$

ამ შემთხვევაში ერთი გასაღებით დაშიფრული ინფორმაციის მეორე გასაღებით ხელახლა შიფრაციას მივყავართ საწყის ღია ტექსტზე.

ამ გასაღებების თავიდან აცილება შეიძლება შიფრაციის დროს გასაღების შემთხვევითი არჩევით და წინასწარი შემოწმებით. თავად ამ სუსტი გასაღებების ამორჩევის ალბათობა გასაღებების მთელი სიმრავლიდან მიზერულია, ასევე არ აძლევენ ისინი რაიმე უპირატესობას კრიპტოანალიტიკოსს. დამტკიცებულია, რომ DES-ის მაქსიმალური დაცვა 64 ბიტს შეადგენს, თუნდაც ციკლებში გამოყენებული ქვეგასაღებები ძირითადი გასაღებისგან დამოუკიდებლად იყოს არჩეული (როდესაც საერთო გასაღების სიგრძე 768 ბიტი იქნებოდა). თადაპირველად *IBM (International Business Machines Corporation)*-ის მიერ შემუშავებული ალგორითმი იყენებდა 112-ბიტიან გსაღებს. შემდგომ *NSA*-ს გავლენით გასაღების სიგრძე შემცირდა და დავიდა 56-ბიტამდე. დღემდე, *Triple DES* რჩება ძალზედ გავრცელებული და რაც შეეხება "მარტივ" DES-ალგორითმებს,ის გამოიყენება მხოლოდ მოძველებულ application-ებში. 2001 წელს DES სტნდარტი შეიცვალა *AES(Advanced Encryption Standard)*-ით.

ამერიკულმა *NBS-მ (National Bureau of Standards)*, რომელიც დღეისათვის *NIST-ის (National Institute of Standards and Technology)* სახელით არის ცნობილი, მოითხოვა ისეთი დაშიფვრის შექმნა, რომელიც ვარგისი იქნებოდა დაწესებულებებში გამოსაყენებლად. 1973 წლის 15 მაისს, შეერთებული შტატების *უშიშროების ეროვნულ სააგენტოსთან (NSA, National Security Agency)* კონსულტაციის შემდეგ, NBS-ნა გამოაცხადა კონკურსი დაშიფრვის მეთოდებზე, რომელშიც ვერც ერთმა კონკურსანტმა ვერ დააკმაყოფილა წამოყენებული საკმაოდ მკაცრი მოთხოვნები.1974 წლის 27 აგვისტოს ჩატარდა მეორე კონკურსი. ამჯერად, IBM-ის მიერ წარმოდგენილმა დაშიფრვის მეთოდი, სახელად *Lucifer*, ჩათვლეს მისაღებად. ეს იყო უფრო ადრეულ პერიოდში ჰორსტ ფეისტელის მიერ შემუშავებული დაშიფრვის

მეთოდზე *(ფეისტელის ქსელი, Feistel scheme, Feistel cipher) დაფუძნებული ალგორითმი.* 1975 წლის 17 მარტს შემოთავაზებული იყო ალგორითმი DES, *Lucifer*-ის მოდიფიკაცია, რომელიც მიღებულ იქნა ფედერალურ ბიუროში. მომდევნო წელს გაიმართა 2 ღია სიმპოზიუმი, რომლებზეც განიხილებოდა DES-სტანდარტი. ამ სიმპოზიუმებზე მკაცრად გააკრიტიკეს NSA-ს მიერ ალგორითმში შეტანილი ცვლილებები: გასაღების პირვანდელი სიგრძის შემცირება, *S*-ბლოკების შექმნა. გავრცელდა ჭორები, იმის თაობაზე რომ *NSA*-მ განზრახ გაამარტივა და შეასუსტა ალგორითმი, რათა საშუალება ჰქონოდა მარტივად ეწარმოებინა კონტროლი დაშიფრულ მონაცემებზე. როგორც შემდგომში გაირკვა, DES-ის შემუშავების პროცესში, *NSA*-მ დაარწმუნა *IBM*-ი, რომ გასაღების შემცირებული სიგრძე აუცილებელსა დ საკმარისზე მეტია ნებისმიერი კომერციული *application*-ისთვის, გავლენა იქონია *S*-გადანაცვლებათა შემუშავებაზე და რომ DES-ის საბოლოო დასრულებული ვარიანტი, მათი აზრით, იყო დაშიფრვის საუკეთესო ალგორითმი, რომელშიც აღმოფხვრილი იყო სტატისტიკური ეა მათემატიკური ხარვეზები. აგრეთვე დადგინდა, რომ არასოდეს, *NSA* უშუალოდ არ ჩარეულა ალგორითმის შემუშავებში.

ეჭვების ნაწილი *S*-გადანაცვლებათა ფარული სისუსტის შესახებ გაქარწყლდა 1990-ში, *ელი ბიჰამს (Eli Biham)* და *ადი შამირის (Adi Shmir)* მიერ დიფერენციალურ კრიპტოანალიზზე (ძირითადი მეთოდი სიმეტრიული გასაღების მქონე ბლოკური ალგორითმების გასატეხად) ჩატარებული დამოუკიდებელი გამოკვლევების შედეგების გამოქვეყნების შემდეგ. **DES**-ალგორითმის *S*-ბლოკები აღმოჩნდა გაცილებით უფრო მდგრადი თავდასხმის წინააღმდეგ, ვიდრე ისინი შემთხვევითი წესით რომ აერჩიათ. ეს კი ნიშნავს იმას, რომ კრიპტოანალიზის ეს ტექნიკა *NSA*-სთვის ჯერ კიდევ XXს-ის 70-იან წლებში იყო ცნობილი.

დასკვნები

ნაშრომში მიღებული შედეგების მიმართ შეიძლება გაკეთდეს შემდეგი დასკვნები:

1. ჩატარებულია ელექტრონული გადახდის სისტემებში უსაფრთხოების სფეროების მიმოხილვა და კრიტიკული ანალიზი. მოცემულია მათი განვითარების ტენდეციები.
2. დასაბუთებულია, რომ ელექტრონული გადახდის სისტემებში კრიტიკულ მნიშვნელობას წარმოადგენს ავტორიზაციის დამუშავებისა და შიფრაციის საშუალებები, მნიშვნელოვანია ავტორზაციის მონაცემების დამუშავების, შენახვის და დეშიფრაციის საშუალებების სათანადო ტექნიკური და პროგრამული უზრუნველყოფა.
3. ნაჩვენებია, რომ საბარათე მაგნიტურ ზოლიან გადახდის სისტემებში სისტემებში ნაკლებად, გამოიყენება ინფორმაციის დამუშავების და შენახვის თანამედროვე საშუალებები. დასაბუთებულია ამ მიმართულებით ელექტრონული ანგარიშსწორების უსაფრთხოების შემუშავებისა და აქტიური დანერგვის, აგრეთვე მეცნიერული კვლევების გაძლიერების აუცილებლობა.
4. ელექტრონული ანგარიშსწორების სისტემებისათვის აგებულია ინფრასტრუქტურა ქსელის ინფრასტრუქტურის ეფექტურ დაგეგმარებას და უსაფრთხოების მნიშვნელოვანი საკითხების მოწესრიგებას სხვადასხვა კომპონენტების განსაზღვრისათვის, მათ შორის სერვერული ინფრასტრუქტურის მოწყობას. ნაჩვენებია, რომ სამეცნიერო-ტექნიკური ექსპერიმენტების კვლევების ჩატარების უნიფიცირებული ტექნოლოგია, ინფრასტრუქტურის დაგეგმარებისა და ცენტრალიზირებული მართივის პრინციპების რეჟიმების ერთგვაროვნობა, ერთის მხრივ, და რთული, შრომატევადი

ექსპერიმენტების სერია, მეორეს მხრივ, განსაზღვრავენ ელექტრონული ანგარიშსწორებისათვის შესაბამისი ქსელური და სასერვერო ინფრასტრუქტურის შემუშავების მიზანშეწონილობას, რომელიც თავის თავში აერთიანებს ტექნიკურ, საინფორმაციო-მეთოდიკურ და პროგრამულ საშუალებებს, რომლებიც ორიენტირებულია კიბერუსაფრთხოების ამოცანების გადაწყვეტაზე.

5. აგებულია ორი მაგნიტურ ზოლიანი ანგარიშსწორების სისტემა. შემუშავებულია მონაცემთა ბაზების სტრუქტურა ორდონიანი ავტორიზაციისათვის,

6. უსაფრთხოების უზრუნველსაყოფად და მისი ეფექტიანობის გასაზრდელად. შემუშავებულია ორ მაგნიტურ ზოლიანი ბარათის ფუნქციონირებისათვის საჭირო ინფრასტრუქტურა და ტექნიკური მახასიათებლები. შემუშავებულია დაშიფრვის სისტემის სტრუქტურა, რომელიც მორგებულია ორ მაგნიტურზოლიანი ბარათზე, განმარტებულია მისი მუშაობის ალგორითმი, რომელიც იძლევა უსაფრთხო და სწრაფი ავტორიზაციის საშუალებას.

7. შემუშავებული მიდგომა იძლევა ელექტრონული ანგარიშსწორებისას ავტორიზაციის მეთოდიკის დახვეწის საშუალებას, რაც შეიძლება წარმატებით გამოყენებულ იქნას, როგორც დაცვის სისტემების პროგრამული უზრუნველყოფის აგებისას, ასევე ანგარიშსწორების სხვადასხვა მეთოდებში.

ABSTRACT

An electronic payment systems in safety-critical analysis of the norms and tendences. The tendencies of their development. Reviewed modern payment systems software and hardware products, their development trends. It is proved that the electronic payment systems of critical importance to the process of authentication and encryption techniques, it is important authentication data processing, storage and decryption means of appropriate technical and software provision.

Proven to be quite effective and available means of encryption modern However it should be noted that the broad masses algorithm access assurance, has contributed to the development of so-called decryption methods.
It is shown that the symmetric encryption methods are less secure than modern electronic payment methods, systems development and active implementation of the decisions taken in this regard is well founded, as well as the need to strengthen scientific research. Scientific novelty of the thesis is the following. Proposes a new approach to electronic payment principles, in particular the use of encryption and symmetric asymmetric combined use of the methodology, which allows us to double the use of the card payment authorization to use the new more advanced technology, which will contribute to raising the level of security.
It should be noted that the developed approach can be successfully be used not only for electronic payment, but also in information technology at the direction of where the information needs to be protected mode the storage and safe handling, which will allow us to ensure the information security of the three major components of satisfaction as it is - integrity of information, confidentiality and availability. Conducted as theory analytical research and practical laboratory work.

It is shown that the accuracy of each component depends on the accuracy of the experimental research studies of individual stages, which means a difficult and time-consuming experimental research experiments and a large number of impacts.

Analysis of the results of research performed by the gradual process of structuring, the structure of the settlement systems, developed experimental models to study each stage of the procedure. Each stage is defined in the information-providing methodology scheme. It is shown that the scientific and technical experiments, research unified technology, information collection and processing modes uniformity, on the one hand, and a difficult, time-consuming series of experiments, on the other hand, define the computing system development feasibility, which itself combines technical, information-methodical and software means , which focused on electronic payment methods to raise the level of security. Defined, as well as hardware and software requirements are. Data and knowledge base has been developed, based on a production rule system and to reflect qualified and experienced technology knowledge. The system has been developed by the facts. Developed a database that contains the entrance and exit of data. Developed electronic settlement system structure, which includes a knowledge base, databases and resources necessary auxiliary technical characteristics, developed the graphical user interface technology. Developed a system using the structure, formalize network structure, data synchronization and mirrored the use of alternatives, provides a cost-effective encryption methods in which the user allows his device, be it a card or other electronic authorization for the device, the information is protected in storage and to secure authorization.

დისერტაციის ძირითადი შინაარსი გამოქვეყნებულია შემდეგ სამეცნიერო სტატიებში:

1. კ.ჟამურაშვილი ექსპერტული ელექტრონული გადახდის სისტემებში ინფორმაციული უსაფრთხოების სტრატეგია. გორის სახელმწიფო სასწავლო უნივერსიტეტი, საქართველო, მერვე საერთაშორისო კონფერენცია „განათლება XXI საუკუნეში“. 2015. გვ. 154-158.

2. რ. სამხარაძე, კ. ჟამურაშვილი სტატია საინფორმაციო სისტემების უსაფრთხოების ინფრასტრუქტურის დაგეგმარება. თბილისი, "საქართველოს ტექნიკური უნივერსიტეტი", შრომები. მართვის ავტომატიზებული სისტემები. N1(21). 2016. გვ 66-70

3. რ.სამხარაძე, კ.ჟამურაშვილი. თანამედროვე კრიპტოგრაფიული მეთოდები. თბილისი, "საქართველოს ტექნიკური უნი-ვერსიტეტი", შრომები. მართვის ავტომატიზებული სისტემები. N1(21). 2016.

4. კ.ჟამურაშვილი ინფორმაციული უსაფრთხოება თბილისი, საქართველოს ტექნიკური უნივერსიტეტი, შრომები. ბიზნეს- ინჟინერინგი N 1. 2016 91-93