საქართველოს ტექნიკური უნივერსიტეტი

კახაბერ ჟამურაშვილი

ელექტრონული გადახდის სისტემებში უსაფრთხოების ნორმების შემუშავება და განვითარება

წარმოდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა „ინფორმატიკა“ შიფრი 0401

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0175, საქართველო

ივლისი, 2016 წელი

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

საქართველოს ტექნიკური უნივერსიტეტი

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

ჩვენ, ქვემორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით კახაბერ ჟამურაშვილის მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: „ელექტრონული გადახდის სისტემებში უსაფრთხოების ნორმების შემუშავება და განვითარება" და ვაძლევთ რეკომენდაციას საქარველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

თარიღი

ხელმძღვანელები: პროფ. რომან სამხარაძე

რეცენზენტი: ————————————————

————————————————

————————————————

————————————————

საქართველოს ტექნიკური უნივერსიტეტი

2016

ავტორი: კახაბერ ჟამურაშვილი

დასახელება: "ელექტრონული გადახდის სისტემებში უსაფრთხოების ნორმების შემუშავება და განვითარება“

ფაკულტეტი: "ინფორმატიკისა და მართვის სისტემების ფაკულტეტი"

აკადემიური ხარისხი: დოქტორი

სხდომა ჩატარდა:

ინდივიდუალური პიროვნების ან ინსტიტუტების მიერ შემოყვანილი დასახელების დისერტაციის გაცნობის მიზნით მოთხოვნის შემთხვევაში მისი არაკომერციული მიზნების კოპირებისა და გავრცელების უფლება მინიჭებული აქვს საქართველოს ტექნიკურ უნივერსიტეტს ავტორთან შეთანხმებით.

კ. ჟამურაშვილი

ავტორის ხელმოწერა

ავტორი ინარჩუნებს დანარჩენ საგამომცემლო უფლებებს და არც მთლიანი ნაშრომის და არც მისი ცალკეული კომპონენტების გადაბეჭდვა ან სხვა რაიმე მეთოდით რეპროდუქცია დაუშვებელია ავტორის წერილობითი ნებართვის გარეშე.

ავტორი ირწმუნება, რომ ნაშრომში გამოყენებული საავტორო უფლებებით დაცულ მასალებზე მიღებულია შესაბამისი ნებართვა (გარდა იმ მცირე ზომის ციტატებისა, რომლებიც მოითხოვენ მხოლოდ სპეციფიურ მიმართებას ლიტერატურის ციტირებაში, როგორც ეს მიღებულია სამეცნიერო ნაშრომების შესრულებისას) და ყველა მათგანზე იღებს პასუხისმგებლობას.

მიძღვნა

ამ ნაშრომს ვუძღვნი ჩემს ოჯახს უდიდესი მხარდაჭერისა და გვერდში დგომისათვის.

რეზიუმე

ჩატარებულია ელექტრონული გადახდის სისტემებში უსაფრთხოების ნორმების მიმოხილავა და კრიტიკული ანალიზი. მოცემულია მათი განვითარების ტენდენციები. მიმოხილულია თანამედროვე გადახდის სისტემების პროგრამული და აპარატურული საშუალებები, მათი განვითარების მიმართულებები.

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.

დამტკიცებულია, რომ შიფრაციის თანამედროვე საშუალებები საკმაოდ ეფექტური და ხელმისაწვდომია თუმცა აღსანიშნავია ის ფაქტიც, რომ მისი ალგორთმის ფართო მასისათვის ხელმისაწვდომობის უზრუნველყოფამ, ხელი შეუწყო ეგრეთ წოდებული დეშიფრაციის მეთოდების განვითარებას.

ნაჩვენებია, რომ შიფრაციის სიმეტრიული მეთოდები ნაკლებად უსაფრთხოა თანამედროვე ელექტრონლი ანგარიშწორების მეთოდებში, დასაბუთებულია ამ მიმართულებით მიღებული გადაწყვეტილებები სისტემების შემუშავებისა და აქტიური დანერგვის, აგრეთვე მეცნიერული კვლევების გაძლიერების აუცილებლობა.

სადისერტაციო ნაშრომის მეცნიერული სიახლე შემდეგში მდგომარეობს. შემოთავაზებულია ახალი მიდგომა ელექტრონული ანგარიშწსორების პრინციპებში, კერძოდ გამოყენებულია შიფრაციის სიმეტრული და ასიმტრული მეთოდოლოგიის კომბინირებული გამოყენება, რაც საბარათე ანგარიშსწორების გამოყენებისას საშუალებას გვაძლევს ორმაგი ავტორიზაციის ახალი უფრო გაუმჯობესებული ტექნოლოგია გამოვიყენოთ, რაც ხელს შეუწყობს უსაფრთხოების დონის ამაღლებას.

უნდა აღინიშნოს, რომ შემუშავებული მიდგომა წარმატებით შეიძლება იყოს გამოყენებული არა მხოლოდ ელექტრონული ანგარიშსწორებისას, არამედ ზოგადად ინფორმაციული ტექნოლოგიების ნებისმიერ მიმართულებაში სადაც საჭიროა ინფორმაციის დაცულ რეჟიმში შენახვა და უსაფრთხო დამუშავება, რაც საშუალებას მოგვცემს უზრუნველყოფილ იქნა ინფორმაციული უსაფრთხოების სამი ძირითადი კომპონენტის დაკმაყოფილება როგორიც არის - ინფორმაციის მთლიანობა, კონფიდენციალურბა და ხელმისაწვდომობა.

ჩატარებულია, როგორც თეოროიული ანალიტიკური კვლევა ასევე პრაქტიკული ლაბორატორიული სამუშაოები.

ნაჩვენებია, რომ ამა თუ იმ კომპონენტის განსაზღვრის სიზუსტე დამოკიდებულია ექსპერიმენტალური კვლევების ჩატარების სიზუსტეზე კვლევების ცალკეულ ეტაპებზე, რაც გულისხმობს რთული და შრომატევადი ექსპერიმენტალური კვლევების ჩატარებას ექსპერიმენტებისა და ზემოქმედებების დიდი რაოდენობის გამო.

ანალიზის შედეგების მიხედვით შესრულებულია კვლევების პროცესის ეტაპობრივი სტრუქტურიზაცია, არსებული ანგარიშსწორების სისტემის სტრუქტურის გათვალისწინებით, შემუშავებულია ექსპერიმენტის პროცედურული მოდელები კვლევის თითოეულ ეტაპზე. კვლევის თითოეული ეტაპისთვის განსაზღვრულია ინფორმაციულ-მეთოდოლოგიური უზრუნველყოფის უნიფიცირებული სქემა.

ნაჩვენებია, რომ სამეცნიერო-ტექნიკური ექსპერიმენტების კვლევების ჩატარების უნიფიცირებული ტექნოლოგია, ინფორმაციის შეგროვებისა და დამუშავების რეჟიმების ერთგვაროვნობა, ერთის მხრივ, და რთული, შრომატევადი ექსპერიმენტების სერია, მეორეს მხრივ, განსაზღვრავენ გამოთვლითი სისტემის შემუშავების მიზანშეწონილობას, რომელიც თავის თავში აერთიანებს ტექნიკურ, საინფორმაციო-მეთოდიკურ და პროგრამულ საშუალებებს, რომლებიც ორიენტირებულია ელექტრონული ანგარიშსწორების მეთოდებში უსაფრთხოების დონის ამაღლებაზე. განსაზღვრულია, აგრეთვე მოთხოვნები აპარატურული და პროგრამული უზრუნველყოფის მიმართ.

შემუშავებულია მონაცემთა და ცოდნის ბაზა, რომელიც ეფუძნება პროდუქციული წესების სისტემას და ასახავს კვალიფიციური და გამოცდილი ტექნოლოგის ცოდნას. შემუშავებულია ფაქტების სისტემა. შემუშავებულია მონაცემთა ბაზა, რომელიც შეიცავს შესასვლელ და გამოსასვლელ მონაცემებს.

შემუშავებულია ელექტრონილი ანგარიშსწორების სისტემის სტრუქტურა, რომელიც მოიცავს ცოდნის ბაზას, მონაცემთა ბაზასა საჭირო რესურსებსა და დამხმარე საშუალებათა ტექნიკურ მახასიათებლებს, შემუშავებულია ტექნოლოგიის გრაფიკული ინტერფეისი.

შემუშავებული სისტემური სტრუქტურის გამოყენებით, ფორმალიზირებულია ქსელის სტრუქტურა, მონაცემთა ბაზების სინქრონიზაციისა და სარკისებული მეთოდების გამოყენების ალტერნატივები, უზრუნველყოფს ეფექტური შიფრაციის მეთოდების გამოყენებას რაც მომხმარებლს საშუალებას აძლევს მისსავე მოწყობილობაში, იქნება ეს ბარათი თუ სხვა ელექტრონული ავტორიზაციისათვის განკუთვნილი მოწყობილობა, მოახდინოს ინფორმაციის დაცულ რეჟიმში შენახვა და განახორციელოს დაცული ავტორიზაცია.

ABSTRACT

An electronic payment systems in safety-critical analysis of the norms and 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 autorization 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 algortmis 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 simetric and asimtric 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 in 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, developed experimental models to study each stage of the procedure. Each stage is defined in the information-providing methodologi calunified 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, formalaized 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.

შინაარსი

ცხრილების ნუსხა

ნახაზების ნუსხა

გამოყენებული აბრევიატურების ნუსხა

IT - ინფორმაციული ტექნოლოგიები

იუმს - ინფორმაციული უსაფრთხოების მართვის სისტემა

პომ - პრობლემური ორიენტაციის მოდული

https – hyper text transfer protocol

ssl – secure socet layer

dns – domain name system

მადლიერება

მადლობას ვუხდი ჩემს ხელმძღვანელებს პროფესორ რომან სამხარაძეს ნაშრომზე მუშაობის პერიოდში უამრავი გაწეული კონსულტაციებისა და ფასდაუდებელი დახმარებისათვის.

შესავალი

ინფორმაციული ტექნოლოგიების განვითარება XX საუკუნის მე-8 საოცრებად არის მიჩნეული, სწორედ ამიტომ აქტუალულრია 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, განავითაროონ და გაამრავლონ საინფორმაციო ტექნოლოგიებში, გამოყენებული სიახლეები, ყურადსაღები და გასათვალისწინებელია, სწორედ ამიტომ გადავწყვიტე, შემეტანა წვლილი აღნიშნულ საკითხში და ჩავატარე კვლევა, თუ რამ გამოიწვია ყოველივე ეს.

ერთ-ერთი მთავარი მიზეზი ყოველივე ამისა გახლდათ, ინტერნეტ მაღაზიები, ვებ საიტები, გამარტივებული ელექტრული საინფორმაციო ბაზები, რომლებიც საშუალებას იძლევია დროის მცირედ მონაკვეთში მოვიძიოთ სასურველი ინფორმაცია, სტატისტიკური მონაცმების საფუძველზე გავუკეთოთ შესაბამისი ანალიზი, და გამოვიყენოთ საჭიროებისამებრ.

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. მიმაჩნია რომ 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, სწორედ ამ საკითხების დაყენებასა და გადაწყვეტას მსურს დავუკავშირო ჩემი სამეცნიერო ნაშრომი.

ლიტერატურის მიმოხილვა

თავი I. ელექტრონული გადახდის სისტემების მიმოხილვა

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 სფეროშიგარკვეულ 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.

1.1თანამედროვე ანგარიშსწორების სისტემები

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 გაცვლისთვის, აგრეთვე, ანგარიშსწორების განხორციელებისათვის. როგორც სადისტრიბუციო არხები, საკომუნიკაციო ქსელები უზრუნველყოფს ფიზიკურ კონტაქტს კლიენტთან და გამოიყენება კლიენტების ინფორმირების, კონსულტაციისა და მათთვის პროდუქციის ან მომსახურების მიწოდებისათვის. მიწოდების არხების მეშვეობით ხორციელდება ინფორმაციის მიწოდება, ფინანსური ტრანზაქციების შესრულება და უკუკავშირი კლიენტებთან (feedback, კლიენტებთან ურთიერთობის მხარდაჭერა). როგორც ზემოთ ავღნიშნეთ, საბანკო სატრანზაქციო მომსახურება მოითხოვს მატერიალურ რესურსებს და უშუალოდაა დაკავშირებული კავშირის ელექტრონული არხების განვითარებასთან. სწორედ სატრანზაქციო მომსახურების გაწევის ხარჯების შემცირებისკენ სწრაფვამ განაპირობა მიწოდების ელექტრონული არხებისა და მასთან დაკავშირებული ელექტრონული გადახდის სისტემების (EFTS – Electronic Funds Transfer System) განვითარება 1970-იან წლებში. ნებისმიერი ფინანსური ტრანზაქციის მომსახურებისთვის ტრადიციულად გამოიყენებოდა ნაღდი ფული და ჩეკები. EFT სისტემების წარმოშობამ და განვითარებამ მიგვიყვანა ახალი გადახდის ინსტრუმენტის, ელექტრონული ფონდების, წარმოქმნამდე. ბანკებმა დაიწყეს გადახდის ელექტრონული საშუალებების განვითარება საოპერაციო ხარჯების შემცირების, ბაზრის წილის შენარჩუნება-გაფართოებისა და შემოსავლების ახალი წყაროების მოპოვების მიზნით. სწორედ სატრანზაქციო მომსახურების სფერო წარმოადგენს ტექნოლოგიური ინოვაციების ძირითად წყაროს საბანკო საქმეში ელექტრონული გადახდების განხორციელებისათვის შემუშავდა სპეციალური სისტემები: სახლისა და კორპორაციული ბანკინგი (home banking, PCbanking), რომლებიც გულისხმობდა ბანკის საოპერაციო სისტემებთან მიერთებას სატელეფონო კავშირის ხაზებით და ისეთ ცნობილ

სისტემებს, როგორებიცაა „კლიენტი-ბანკი“, სპეციალიზებული გამომთვლელი ქსელები დამატებითი ფუნქციებითა და მომსახურებით (სინონიმია „კერძო ქსელები“ ან „ფასიანი ქსელები“, Value Added Networks – VAN), სავაჭრო ტერმინალები (POS-ტერმინალები – Point-Of-Sale terminals), ბანკომატები (ATM – Automated Teller Machines) და სხვა. ელექტრონული არხების გამოყენება საკმაოდ სწრაფად განვითარდა არამხოლოდ საგადასახადო ოპერაციების ჩატარებისთვის, არამედ ბანკის სხვა მომსახურების მიწოდებისათვის (სადისტრიბუციო არხების სახით). ამრიგად, ბანკომატებმა, რომლებიც თავდაპირველად როგორც საკასო აპარატები გამოიყენებოდა, დაიწყო ანგარიშების დაშორებული მართვის მომსახურების გაწევა, მათი მეშვეობით შესაძლებელი გახდა ამონაწერების მიღება და შენატანების გაკეთება.

არსებობს ორი ძირითადი ეკონომიკური მიზეზი, რომლის გამოც ბანკებმა ყურადღება მიაქციეს ინტერნეტს. პირველ რიგში, ნებისმიერი საკომუნიკაციო ქსელის ღირებულება, ფაქტობრივად, ფიქსირებულია. უფრო სწორად რომ ვთქვათ, საკომუნიკაციო ქსელებისთვის დამახასიათებელია მუდმივი ხარჯების მაღალი დონე. ეს ნიშნავს, რომ ქსელური მომსახურების მომგებიანობა დამოკიდებულია მასშტაბის ეფექტზე. მაგალითად, თავის დროზე იყო დაანგარიშებული, რომ, ბანკომატების ქსელის გამოყენების დროს წაუგებლობის წერტილი არის 1 000 ურთიერთდაკავშირებული ბანკომატი და როგორც მინიმუმ, 2 000-2 500 ოპერაცია თვეში თითოეულ მათგანში მასშტაბის ეფექტი ამცირებს საშუალო დანახარჯებს. შესაბამისად, რაც უფრო ფართოა ქსელი და რაც უფრო დიდია კლიენტების რიცხვი, მით ნაკლები იქნება საშუალო (ზღვრული) დანახარჯები. ამრიგად, ელექტრონული საკომუნიკაციო ქსელების ინტეგრაცია ეკონომიკურად მომგებიანია.

დღეს, ბანკების კერძო ქსელებს ხშირად ისე აპროექტებენ, რომ მათ შეეძლოთ ურთიერთქმედება სხვა კომპანიებისა და ბანკების ქსელებთან – ეს კეთდება ელექტრონული ფორმით ცირკულირებად მონაცემთა რიცხვის მაქსიმიზაციისათვის. 70-იანი წლებიდან დაწყებული მრავალჯერ სცადეს,

შეექმნათ საფინანსო დაწესებულებებსა და საწარმოებს შორის ინფორმაციის ელექტრონული გაცვლის ერთიანი სტანდარტი (EDI – Electronic Data Interchange). მაშინ როდესაც მოლაპარაკებებმა EDI-ის ერთიანი სტანდარტის შექმნის შესახებ შედეგი არ გამოიღეს, ინტერნეტი დღეს წარმოადგენს სხვადასხვა კომპანიების ქსელების ურთიერთქმედების წერტილს. ინტერნეტი გულისხმობს საერთო TCP/IP პროტოკოლის გამოყენებას, რომელიც საშუალებას იძლევა, დავაკავშიროთ ორი ნებისმიერი კომპიუტერი. აქედან გამომდინარე, ინტერნეტი, ფაქტობრივად, წარმოადგენს საკომუნიკაციო სტანდარტს და მას გააჩნია პოტენციალი, გახდეს უნივერსალური ქსელი, რომელშიც წარმოდგენილია ინფორმაციული გაცვლის ყველა სახეობა. ასეთი ქსელის გამოყენება გამორიცხავს ფუნქციათა დუბლირებას და ეკონომიკურად უფრო ეფექტიანი იქნება. გამოყენების მეორე მიზეზი ისაა, რომ ინტერნეტი ბანკებს აძლევს შესაძლებლობას, იპოვონ ბალანსი კონკურენციასა და თანამშრომლობას შორის. ინტერნეტის გამოყენება ნებისმიერ ადამიანს აძლევს საშუალებას, საკომუნიკაციო ქსელების შექმნასა და მხარდაჭერაში დიდი კაპიტალური დაბანდების გარეშე შექმნას საკუთარი (პროგრამულ უზრუნველყოფაზე დაფუძნებული) საგადასახადო სისტემა. ინტერნეტის საგადახდო სისტემები წარმოადგენს მხოლოდ პროგრამულ გადაწყვეტილებებს, რომლებიც მუშაობს არსებული აპარატურული და ქსელური ინფრასტრუქტურის პირობებში. ეს ნიშნავს, რომ ნებისმიერ მცირე კომპანიას შეუძლია, შეიმუშაოს და გამოიყენოს საკუთარი საგადახდო სისტემები. კომპანიათა უმეტესობა, რომლებიც დღეს ქმნიან საგადახდო სისტემებს, მართლაც მცირე ზომისაა. ამასთანავე, ინტერნეტის ყველა საგადახდო სისტემა იყენებს ერთსა და იმავე პროტოკოლს (TCP/IP) და ამიტომ მათ ადვილად შეუძლია ურთიერთქმედება. აქედან გამომდინარე, კონკურენცია ფართოვდება მომგებიანობის შემცირებისა და ურთიერთქმედების უნარის შეფერხების გარეშე.

გასულ წლებში საკომუნიკაციო ინფრასტრუქტურის შექმნასა და განვითარებაში დიდი კაპიტალდაბანდებების აუცილებლობა

წარმოადგენდა საბანკო სექტორში კონცენტრაციის ერთ-ერთ მიზეზს და უპირატესობას აძლევდა მსხვილ საფინანსო ინსტიტუტებს მცირე ინსტიტუტებთან მიმართებაში. ეს უზრუნველყოფდა საბანკო მომსახურების ბაზარზე შესვლის საკმაოდ საიმედო ბარიერს. ინტერნეტის გამოყენება ბანკებისა და სხვა ფინანსური შუამავლებისგან არ მოითხოვს ხარჯების გაწევას საკომუნიკაციო ინფრასტრუქტურის შექმნისა და მხარდაჭერისათვის. ინტერნეტი ღია საკომუნიკაციო ქსელია, ანუ ნებისმიერ მსურველს შეუძლია გამოიყენოს ამ ქსელის ინფრასტრუქტურა. სხვა სიტყვებით რომ ვთქვათ, ინტერნეტი ამცირებს ბაზარზე შესვლის ბარიერებს და მისი გამოყენების კიდევ ერთ თავისებურებას წარმოადგენს საბანკო ელექტრონული მომსახურების ბაზარზე კონკურენციის გამწვავება. მოთხოვნის თვალსაზრისით, სატრანზაქციო მომსახურებასთან დაკავშირებულ ყველაზე მნიშვნელოვან ტენდენციას წარმოადგენს ბაზრების გლობალიზაცია. წარსულში ეს ტენდენცია მხოლოდ დიდ ტრანსნაციონალურ კორპორაციებს ეხებოდა. ევროპული ბაზრების გაერთიანება და სავაჭრო შეზღუდვების შემცირება გულისხმობს, რომ ნებისმიერი საშუალო და მცირე ზომის კომპანია კონკურირებადი უნდა იყოს საერთაშორისო არენაზე. თავის მხრივ, ეს მოითხოვს სწრაფ და ერთგვაროვან (სტანდარტიზებულ) გადახდის პროცედურებს საერთაშორისო გარიგებებისათვის. დღევანდელი საბანკო სისტემა არ არის მორგებული დიდი რაოდენობის მცირე და საშუალო კლიენტების საგადახდო საჭიროებების დაკმაყოფილებაზე. თუ მსხვილ კორპორაციებსა და ინსტიტუტებს შეუძლიათ კაპიტალის გადაადგილება ერთი ქვეყნიდან მეორეში და მისი კონვერტაცია ერთი ვალუტიდან მეორეში, მაშინ ტიპური საცალო საერთაშორისო გადახდა მოითხოვს დროის პერიოდს გაზრდას რამდენიმე დღიდან ერთ კვირამდე და, შესაძლოა, საკმაოდ ძვირიც იყოს. არსებითად, ბანკებს არ გააჩნიათ სიტუაციის გაუმჯობესების სტიმული, ვინაიდან გადახდების ხანგრძლივობა გულისხმობს, რომ ბანკს შეუძლია, კლიენტის მიერ გადახდის თარიღსა და ბანკის მიერ ჩატარებული გადახდის თარიღს შორის დროის მონაკვეთში, გამოიმუშავოს პროცენტი

კლიენტის ფულიდან (დასავლურ ლიტერატურაში ბანკების საპროცენტო შემოსავლების ამ ნაირსახეობას უწოდებენ შემოსავლებს „ფლოუტიდან“გლობალიზაციის სხვა ასპექტი დაკავშირებულია იმასთან, რომ სხვადასხვა ქვეყნის ინტერნეტის მომხმარებლები საბანკო მომსახურების პოტენციური ბაზარია. ბაზრის ტევადობა შეიძლება შეფასდეს ინტერნეტის აქტიური აუდიტორიის მოცულობით ერთადერთი ელემენტი, რომელიც არ არის წარმოდგენილი, არის უსაფრთხო საგადახდო სისტემები. თუ ბანკები ხელიდან გაუშვებენ ბაზარზე შესვლის შანსს, მაშინ მათ შეიძლება დაკაგრონ მონოპოლია საგადახდო მომსახურებაზე. სწორედ კონკურენციის ფაქტორი არის ბანკების მიერ ინტერნეტის „ათვისების“ მეორე ფაქტორი.

საბანკო საქმეში ინტერნეტის გამოყენების სამი პრინციპული ხერხი არსებობს: ინფორმაციის მიწოდება, ოპერაციების განხორციელება და კლიენტებთან ურთიერთობების მხარდაჭერა. ინტერნეტის ისეთი სპეციფიკური თავისებურებები, როგორებიცაა ინტერაქტიულობა და ოპერატიულობა, იძლევა საშუალებას, შევათავსოთ სხვადასხვა ფუნქციები. მაგალითად, ერთდროულად მივაწოდოთ ინფორმაცია და განვახორციელოთ კლიენტებთან ურთიერთობა. ინტერნეტი შეიძლება გამოყენებულ იქნას, როგორც კომუნიკაციის კიდევ ერთი არხი.

ინტერნეტის საკომუნიკაციო შესაძლებლობებმა უკვე შეცვალა საბანკო მომსახურების მიწოდების მეთოდი: მომსახურება მიეწოდება ინტერაქტიულად, რეალური დროის რეჟიმში, ინტერნეტთან დაკავშირებული კლიენტის დაშორებული პერსონალური კომპიუტერიდან ან მობილური ტელეფონიდან. ინტერნეტით კლიენტების დისტანციურ საბანკო მომსახურებას (remote banking) უწოდებენ „ინტერნეტბანკინგს (internet banking). ინტერნეტის, როგორც მიწოდების ახალი არხის, გამოყენების ეფექტიანობა განხილულია ქვემოთ.

ინტერნეტ ბანკი – ეს არის საბანკო მომსახურება, რომელიც გულისხმობს ინტერნეტით ანგარიშის დისტანციურ მართვას. ინტერნეტ ბანკი წარმოადგენს დისტანციური ბანკინგის ისეთი ნაირსახეობების ლოგიკურ

გაგრძელებას, როგორებიცაა PCbanking (ანგარიშთან წვდომა პერსონალური კომპიუტერის საშუალებით, რაც ხორციელდება პირდაპირი მოდემური კავშირით საბანკო ქსელთან), telephone banking (ანგარიშების მომსახურება ტელეფონით) და video banking (კლიენტისა და ბანკის პერსონალის ინტერაქტიული ურთიერთობის სისტემა) .

ინტერნეტ ბანკი – კლიენტების დისტანციური საბანკო მომსახურების ერთ-ერთი სახეა, რომელიც იყენებს ინტერნეტის გარემოს ტრანსპორტის სახით და, ამასთანავე, იყენებს ისეთ სტანდარტულ (მოცემული მომენტისათვის ინტერნეტის მომხმარებელთა უმეტესობისათვის ხელმისაწვდომი) Web-ბრაუზერებს, როგორებიცაა Internet Explorer და Netscape Navigator, რომლებიც არ ითხოვს დამატებითი პროგრამული უზრუნველყოფის დაყენებას კლიენტის მხრიდან.

ინტერნეტ ბანკი – ინტერნეტით ყველა იმ სტანდარტული ოპერაციის შესრულების შესაძლებლობა, რომლებიც კლიენტის მიერ შეიძლება განხორციელდეს ბანკის ოფისში (ნაღდ ფულთან დაკავშირებული ოპერაციების გარდა)

როგორც წესი, ინტერნეტ ბანკის ქვეშ იგულისხმება ფიზიკური პირების ანგარიშების მომსახურება ინტერნეტის საშუალებით.

FinCEN-ის მოხსენების «A Survey of Electronic Cash, Electronic Banking and Internet Gaming» თანახმად, ინტერნეტ ბანკი ინფორმაციის მიწოდების დამხმარე არხია, რომლის მეშვეობითაც კლიენტებს შეუძლიათ, განახორციელონ ელექტრონული ტრანზაქციები ბანკის ოფისში ფიზიკურად შესვლის გარეშე დისტანციური საბანკო მომსახურება არის საკრედიტო ორგანიზაციების კლიენტების საბანკო ოპერაციებისა და გარიგებების შესრულება სატელეკომუნიკაციო სისტემების გამოყენებით.

ინფორმაციული ტექნოლოგიები არის ტექნოლოგიები, რომლებიც იყენებს გამომთვლელი ტექნიკისა და ტელეკომუნიკაციის საშუალებებს სხვადასხვა სახის ინფორმაციის (სიმბოლური, გრაფიკული და ა.შ.) შექმნის, შეგროვების, შენახვის, დამუშავებისა და გადაცემისათვის.

ინტერნეტტექნოლოგიები არის ინფორმაციული ტექნოლოგიები, რომლებსაც საკრედიტო ორგანიზაციები იყენებენ ინტერნეტით კლიენტების დისტანციური საბანკო მომსახურებისა და ამ ორგანიზაციების საქმიანობასთან დაკავშირებული ინფორმაციის მიღებისა და გავრცელებისათვის.

Web-საიტი არის ინტერნეტში წარმოდგენილი იერარქიულად ორგანიზებული, უშუალოდ ადრესირებადივიზუალურად აღქმადი საინფორმაციო გვერდებისა და WEB-სერვერის პროგრამულ-ინფორმაციულ საშუალებებზე წვდომის მართვის ელემენტების ერთობლიობა. ფუნქციონალური დანიშნულებით WEB-საიტები იყოფა: საინფორმაციო – გამოიყენება საკრედიტო ორგანიზაციისა და მისი საქმიანობის შესახებ მონაცემების მუდმივად გავრცელებისათვის. მოცემული სახის WEB-საიტები შეიძლება გამოყენებული იყოს, როგორც მომხმარებელთან ინტერაქტიული ურთიერთქმედების საშუალება, მათგან ამა თუ იმ ინფორმაციის მიღების ან მათთვის ინფორმაციის გადაცემის მიზნით, დისტანციური საბანკო მომსახურების ფარგლებში ოპერაციების ჩატარების გარეშე; საოპერაციო – გამოიყენება სო-ს კლიენტების მიერ, დისტანციური საბანკო მომსახურების (დსმ) ფარგლებში, საბანკო ოპერაციებისა და გარიგებების ჩატარებისათვის. ინტერნეტ ბანკი – ეს არის ინტერნეტ ტექნოლოგიის გამოყენებით განხორციელებული დისტანციური საბანკო მომსახურება საკრედიტო ორგანიზაციის საოპერაციო WEB-საიტის მეშვეობით. თუმცა ეს ცნება სრულად არ ასახავს ინტერნეტ ბანკის ეკონომიკურ და ტექნოლოგიურ ასპექტებს. ინტერნეტ ბანკის ცნების ფორმულირებისათვის აუცილებელია: ა) დისტანციური წვდომის მომსახურების ევოლუციის ანალიზი; ბ) საბანკო ანგარიშების მართვაზე დისტანციური წვდომის მომსახურების კლასიფიკაცია.

წინა საუკუნის 80-იან წლებში საფუძველი ჩაეყარა კლიენტების საბანკო მომსახურების პრინციპულად ახალ მიმართულებას – home banking (სახლის ბანკი). ზოგადად, home banking – ეს არის საბანკო მომსახურების მიწოდება არა ოფისში კლიენტისა და ბანკის თანამშრომლის უშუალო

კონტაქტით, არამედ სახლში ან კომპანიის ოფისში – ყველგან, სადაც ეს კლიენტისათვის იქნება კომფორტული. დღეს, კავშირის გამოყენებული მეთოდების მიხედვით, გამოყოფენ დისტანციური საბანკო მომსახურებისხუთ ძირითად ნაირსახეობას: სატელეფონო ბანკი (telephone banking);კომპიუტერული ბანკინგი (PCbanking); ვიდეობანკინგი (video banking); ინტერნეტბანკინგი (internet banking); მობილური ბანკინგი (mobile banking). როგორც ეს სახელწოდებიდან ჩანს, სახლის ბანკის თითოეული ნაირსახეობა იყენებს კავშირის კონკრეტულ არხს. აქედან გამომდინარე, შეგვიძლია დავასკვნათ, რომ სატელეკომუნიკაციო ტექნოლოგიების განვითარება ხელს უწყობს დისტანციური საბანკო მომსახურების სრულყოფას. ინტერნეტ ბანკის ადგილი ელექტრონული კომერციისსტრუქტურაში წარმოდგენილია ზემოხსენებულიდან გამომდინარე, ინტერნეტ ბანკი – ეს არის ელექტრონული კომერციის სახე, რომელსაც საკრედიტო ორგანიზაციები იყენებენ ფიზიკური ან/და იურიდიული პირებისათვის სტანდარტული და სპეციალური საბანკო მომსახურების დროის ნებისმიერ მომენტში დისტანციური მიწოდებისათვის გლობალური კომპიუტერული ქსელის,ინტერნეტის, მეშვეობით, დამატებითი პროგრამული ზრუნველყოფის გარეშე. ინტერნეტ ბანკის ადგილი ელექტრონული კომერციის სტრუქტურაში.

ინტერნეტი იძლევა საშუალებას, არა მხოლოდ ერთდროულად მივაწოდოთ სხვადასხვა ტრადიციული საბანკო მომსახურების უფრო მეტი რაოდენობა, არამედ იგი აფართოებს მომსახურებათა სპექტრს ახალი სახეობებით. საბანკო მომსახურების ახალი სახეობები, ძირითადად, დაკავშირებული არის ახალი ბაზრის, ელექტრონული კომერციის ბაზრის, ათვისებასთან. კერძოდ, ინტერნეტის გამოყენებამ უკვე მიგვიყვანა ფინანსური ტრანზაქციების მომსახურების ახალი ინსტრუმენტების აღმოჩენამდე – „ელექტრონულ ფულამდე“ (e-money).

ზემოთ ხსენებულიდან გამომდინარე, შეიძლება ითქვას, რომ ინტერნეტის, როგორც საბანკო მომსახურების დისტრიბუციის ახალი არხის გამოყენებას

მივყავართ ბანკების საოპერაციო დანახარჯების შემცირებამდე მომსახურების მოცულობისა და საბანკო მომსახურების სპექტრის გაფართოების ხარჯზე. მეორე მხრივ, ინტერნეტი წარმოადგენს ღია ინფორმაციულ გარემოს და მას პოტენციურად შეუძლია გაანადგუროს ელექტრონული საბანკო მომსახურების ბაზარზე შესვლის ბარიერები (ძირითადად ეს ეხება საცალო მომსახურებას). ინტერნეტის გამოყენება არის კონკურენციის გამწვავების მიზეზი საბანკო საქმეში. კონკურენციის გამწვავება დაკავშირებულია ფინანსური და საბანკო მომსახურების ბაზრებზე ახალი მოთამაშეების გამოჩენასთან.

1.2 უსაფრთხოების მდგომარეობა მიმოხილვა არსებული ანგარიშსწორების მეთოდების მიხედვით

ელექტრონული გაცვლა და სისტემატიზაცია, როდესაც ვირჩევთ სისტემის წესს, არსებობს ხელმძღვანელობს, ორი წესი: პოპულაროობა (გავრცელების) და საიმედოობის (დაცვა), და ეს ფაქტორი მნიშვნელოვნად ავიწროვებს სპექტრი განიხილება ელექტრონული ფული.მოდით ცდილობენ ანალიზი ზოგიერთი ყველაზე პოპულარული და მოსახერხებელი სისტემა ჩვენს ქვეყანაში. დღემდე, ელექტრონული ფული გავრცელებულია მთელ მსოფლიოში.მათ შეუძლიათ გადაიხადონ მობილური ტელეფონი, ინტერნეტი, ითამაშოს მათ კაზინო, მათ გაყიდოს ნებისმიერი პროდუქტის ... ზოგადად: მიღების და ხარჯვის. მაგრამ პრობლემა ის არის, რომ სხვადასხვა ოპერაციების უნდა მიიღოს სხვადასხვა გადახდის სისტემები.მაგალითად, ავტორები SHZH მიიღოს მისი საფასური მხოლოდ WMZ - სავალუტო სისტემა WebMoney.ეს არის ყველაზე პოპულარული , ყველაზე დაცული რუსული სისტემა.მაგალითად, აშშ-ის გაცილებით ნაკლებია, Vogue, მაგრამ რუსეთსა და უკრაინაში, უმრავლესობა

გამოიყენება. დაცვის მაღალი ხარისხი ამ სისტემაში იქცევა დიდი პრობლემები: WebMoney კრძალავს მონაწილეობას პროექტები, პირამიდები, ინვესტირებას HYIP - ზოგადად, გაუმკლავდეთ ნებისმიერი საეჭვო საქმიანობაში;ამ მხრივ იკრძალება გაცვლა WebMoney სავალუტო სისტემა, რომელიც ადამიანს არ ისურვა. მაგალითად, გაცვლა WM to Liberty Reserve და E-ოქროს, თქვენ უნდა მიიღოს პირადი მოწმობა WebMoney - წარმოადგინოს ნოტარიულად დამოწმებული ასლი თქვენი პასპორტი და ეწვევა სიმბოლური თანხა (და hassle რაღაც ამ much!). WebMoney საშუალებას ერთ ანგარიშზე აქვს მრავალი ჩანთები.ეს შეიძლება იყოს ჩანთები სხვადასხვა ვალუტაში: WMZ (USD), WMR (რუსული რუბლი), WMU (უკრაინის გრივნა), WME (ევრო), WMB (Belarusian რუბლი), WMY (Uzbek თანხები), WMG (ოქრო). რუსი სისტემა - Yandex.ქალი ხელმისაწვდომია მხოლოდ საქართველოს მოქალაქეებს რუსეთის ფედერაციის (კერძოდ, მოითხოვოს დაბრუნების სისტემა შესაძლებელია მხოლოდ რუსეთსა და ამ აუცილებელია წარმოადგინოს რუსეთის პასპორტი).ამ სისტემაში, მხოლოდ ერთი ვალუტა - რუსული რუბლი.აღსანიშნავია, რომ Yandex ოდნავ იაფია, ვიდრე იმ WMR , იგი ასოცირდება ქვედა გავრცელების პირველი. და ახლა უცხო სისტემა.ცოტა ხნის წინ სარგებლობდა დიდი პოპულარობით სისტემა E-Gold: ფულის გამო აკავშირებს ძვირფასი ლითონები შეიძლება არ შეგეშინდეთ, რომ ამ ვალუტაში მოულოდნელად გაუფასურდა.სამწუხაროდ, არც ისე დიდი ხნის წინ, E-gold უკვე სერიოზული პრობლემები მათი მთავრობა (აშშ), ასე რომ, ვერავინ გარანტიას, რომ სისტემა იმუშავებს კიდევ ერთხელ, როგორც ადრე.

ყველაზე სავალი ვალუტაში მსოფლიოში "მუქი" მოგება - Liberty Reserve.სისტემა დაფუძნებულია კოსტა რიკაში, კანონების რესპუბლიკის საშუალებას Liberty იყოს თავისუფალი სისტემა: თქვენ არ არის საჭირო იმისათვის, რომ უზრუნველყოს რეალური მონაცემები (სახელი), Liberty საშუალებას გაძლევთ ინვესტირებას ნებისმიერი პროექტის (თუმცა, აცხადებს, რომ იმ შემთხვევაში, თუ დაკარგვის ფულიისინი უკან არ

უბრუნდება - არა, რეალურად, ეჭვგარეშეა!).აქამდე უკვე შესაძლებელია გაცვლა WM for LR, ადამიანები, რომლებიც მიღებული WM არ არის საკმაოდ პატიოსანი გზით, ფულის გათეთრება: WM თარგმნა LR, მაშინ LR უკან WM.მერე ვნახოთ, როგორ და იგივე იყო რეალურად მიღებული ფული - შეუძლებელია.Liberty Reserve ფართოდ გამოიყენება HYIP-პროექტი (საინვესტიციო ფონდების ძალიან მაღალი პროცენტი).ვალუტა LR - აშშ დოლარი, ევრო. სისტემა ძალიან მაღალი ხარისხის დაცვა .რეგისტრაციას, თქვენ უნდა შევიდეს ანგარიშის ნომერი, პაროლი, კოდი იმიჯი.გადარიცხვები ასევე ვრცელდება სამი ციფრი უშიშროების PIN, როდესაც თანხის ასევე უნდა 4-5 ციფრი შესვლა PIN.მცირე თანხის საფასურად, როდესაც გადაცემის ფული, შეგიძლიათ დაალაგეთ თქვენი ანგარიში მიმღები. Liberty ეძებს ახალ მომხმარებელს, რომ მათ აქვთ რეფერალური სისტემა მუშაობს .რეგისტრაციისას რეფერალური ლინკი, თქვენ (ისევე, როგორც ერთი, რომლის ლინკი გვხვდება, რა თქმა უნდა) მოხვდნენ თქვენს ანგარიშზე პატარა სიმბოლური თანხა .იმისათვის, რომ მიიღოთ ფული დაწკაპვით ბმულს, თქვენ უნდა შეასრულოს ორი პირობა: უნდა გადავიდეს, რომ გახსნათ ბმული, ვიდრე გადაწერა ბრაუზერი;და რეგისტრაციის, როდესაც თქვენ გადაეგზავნება დადასტურებას ელ, თქვენ ვერ დახურვა წინა ფანჯარა.გარდა ამისა, თქვენ არ შეგიძლიათ სხვადასხვა ანგარიშები, რათა მოგების მათთვის - სისტემა წაშლი. როგორც წესი, ერთხელ პირი შევიდა მსოფლიოს ელექტრონული ფული, მას აქვს რამდენიმე ჩანთები სხვადასხვა სისტემები მათი მოთხოვნების შესაბამისად.მე ჩამოთვლილი მხოლოდ ფრაქცია არსებული სისტემები, ცდილობს იდენტიფიცირება ყველაზე პოპულარული მიმოხილვა.

საქართველოს საბანკო სისტემის განვითარების ისტორიული რეტროსპექტივა, სადაც მიმოხილულია შემდეგი საკითხები: საბანკო საქმის განვითარების ეტაპები საქართველოში; საქართველოს საბანკო-საკრედიტო სისტემა თანამედროვე ეტაპზე; საბანკო ოპერაციები და მათი ადგილი ფულადი ურთიერთობების სრტუქტურაში. დაზუსტებულია, რომ საბანკო სისტემა საბაზრო ეკომონიკის ერთ- ერთ ურთულეს და აუცილებელ

სფეროს წარმოადგენს, რომელიც განვითა- რების თავისებურებებით ხასიათდება და მთლიანად ეკონომიკური სისტემის ქმედუნარიანობის ხარისხს განსაზღვრავს. საბაზრო ურთიერთო- ბები წარმოუდგენელია ფულად-საკრედიტო სისტემის აქტიური ფუნქციო- ნირების გარეშე, იგი ზემოქმედებას ახდენს ეკომონიკის პრაქტიკურად ყველა სფეროზე, განსაზღვრავს მის მიმართულებებს და ტრაექტორიებს. ამავე დროს საბანკო სისტემა, გარკვეული აზრით, ავტომონიური „სამყაროა“, რომელსაც განვითარების საკუთარი და სპეციფიკური 13 კანონზომიერებები ახასიათებს. სამედიცინო ანალოგიის შესაბამისად თუ ვიმსჯელებთ, „ფული“ - ეკომონიკის სისხლია, „საბანკო სისტემა“ - მისი სისხლგამტარი არტერიები, ხოლო ბანკები კი - „გულები“ გამოდიან, რომლებიც ეკონომიკის სიცოცხლის უნარიანობაზე და განვითარებაზე მოქმედებენ. უკვე დიდი ხანია, როგორც ქართველ, ისე უცხოელ ექსპერტთა აღიარებით, საქართველოში რეფორმებისა და ინსტიტუციონალური ჩამოყალიბების თვალსაზრისით, ყველაზე წინ სწორედ კომერციული ბანკები წავიდნენ. საქართველოში ფულად-საკრედიტო სისტემის ინსტიტუციონალური ჩამოყალიბების, მაკროეკონომიკური გარემოს სტაბილიზაციის პროცესის, კომერციული ბანკების წარმოშობისა და განვითარების, საბანკო რეფორმის ჩატარების სხვადასხვა ეტაპის შედეგად ბოლო ორი ათწლეულის განმავლობაში ფინანსურ სისტემაში ჩამოყალიბდა დადებითი ტენდენციები, რომელთაგან აღსანიშნავია რამდენიმე მნიშვნელოვანი მომენტი: სახელმწიფომ შეძლო ეკონომიკის სტაბილიზაციისა და ფულად-საკრედიტო საბიუჯეტო-საგადახდო სისტემების თანმიმდევრული ერთიანი პოლიტიკის განხორციელება; ფულის რაციონალური მიწოდების საფუძველზე, შესაძლებელი გახდა ინფლაციური პროცესების მართვა და შენარჩუნდა სხვა ვალუტების მიმართ ლარის გაცვლითი კურსის სტაბილურობა; მნიშვნელოვანი წარმატებები იქნა მიღწეული ბანკების კონსოლიდაციისა და გამსხვილების საქმეში, რაც ბანკებს შორის კონკურენციის გაზრდასთან ერთად მნიშვნელოვნად განაპირობა მინიმალური საწესდებო კაპიტალის ეტაპობრივმა ზრდამ; სტაბილურმა

გაცვლითმა კურსმა, საბანკო სისტემისადმი მოსახლეობის ნდობის ამაღლებამ დადებითი ზეგავლენა მოახდინა დეპოზიტებისა და საკრედიტო დაბანდებების ზრდაზე.

საქართველოს ეროვნული ბანიკის მიერ დამტკიცებული ანგარიშსწორების მეთოდები და საშუალებები: ა) ბანკში საგადახდო დავალების ელექტრონული შეტყობინებების სახით წარდგენა (ან მისი გამოსახულების გადაცემა) ხდება საგადახდო საბუთების ელექტრონულად გაცვლის შესახებ ელექტრონული სისტემების, პროგრამულ–კრიპტოგრაფიული დაცვების და ელექტრონულ-ციფრული ხელმოწერების გამოყენების თაობაზე ბანკსა და კლიენტს შორის გაფორმებული ხელშეკრულების საფუძველზე. საგადახდო დავალების ელექტრონული შეტყობინებების სახით წარდგენისას, ბანკს ქაღალდის საგადახდო დავალება არ წარედგინება; ბ) ელექტრონული საგადახდო საბუთი ელექტრონული შეტყობინებების სახით გასაცვლელად უნდა შეესაბამებოდეს: ბ.ა) საქართველოს ეროვნული ბანკის მიერ დადგენილ მოთხოვნებს – ბანკთაშორისი ანგარიშსწორების შემთხვევაში; ბ.ბ) კომერციული ბანკის მიერ დადგენილ მოთხოვნებს – სათავო ბანკსა და მის ფილიალებს შორის, აგრეთვე ბანკსა კლიენტებს შორის (კლიენტ-ბანკით, ინტერნეტით, მობილური ტელეფონებით ან სხვ.) ანგარიშსწორების შემთხვევაში; გ) ბანკთაშორის ანგარიშსწორების სისტემაში წარსადგენი ელექტრონული საგადახდო საბუთი უნდა შეიცავდეს მე-3 მუხლის მე-2 პუნქტით განსაზღვრულ ყველა რეკვიზიტს, გარდა იმ რეკვიზიტებისა, რომელთა გადატანაც ელექტრონულ ფორმატში შეუძლებელია (ბეჭედი, შტამპი, ხელმოწერები), ამასთან, იგი უნდა შეიცავდეს დამატებით რეკვიზიტებს – საბუთის უნიკალურ კოდს (რეფერენსს), ბანკში გატარების თარიღს, ელექტრონულ-ციფრულ ხელმოწერას. ბანკის საოპერაციო დღის სისტემაში ელექტრონულ საგადახდო საბუთს შესაძლოა ჰქონდეს სხვა დამატებითი რეკვიტებიც (მაგ., შიდა ოპერაციების განმკარგულებლების და შემსრულებლებლების კოდები, სპეციალური სისტემური ნიშნები,

მიმდინარე სტატუსი და სხვ.). ინფორმაციის კომპიუტერულ ტექნიკაში შეტანის დროს ელექტრონულ საგადახდო დავალებაში ძირითადი ველების შეტანა ხდება უშუალოდ ქაღალდის საგადახდო დავალებიდან, ხოლო დამატებითი ველების წარმოშობა (ან გამოძახება) ხდება სისტემური საშუალებებით (პროგრამულ- ტექნიკური საშუალებები); დ) საგადახდო დავალების ელექტრონული სახით წარდგენისას, სავალდებულოა დაცულ იქნეს მხარეთა შორის შეთანხმებული, არასანქცირებული გადახდებისაგან დაცვის მოქმედებები. არასანქცირებული გადახდებისაგან დაცვის მოქმედებები ითვლება შეთანხმებულად: დ.ა) როდესაც კლიენტმა ხელშეკრულებით აღიარა ბანკის მიერ შეთავაზებული არასანქცირებული გადახდებისაგან დაცვის მოქმედებები; დ.ბ) თუ კლიენტმა არ მიიღო ბანკის წინადადებები და ბანკს შესთავაზა დაცვის სხვა წინადადებები, რომლებიც ბანკისათვის აღმოჩნდა მისაღები. ასეთ შემთხვევაში არასანქცირებული გადახდების დაცვის მოქმედებებისათვის პასუხისმგებლობა ეკისრება კლიენტს; ე) კლიენტის მომსახურე ბანკის მიერ კორესპონდენტ ბანკში გადაცემული სანქცირებული ელექტრონული საგადახდო დავალება ჩაითვლება შეცდომით გადაცემულად: ე.ა) როდესაც საგადახდო დავალების რეკვიზიტები არ შეესაბამება გადამხდელის საგადახდო დავალების რეკვიზიტებს; ე.ბ) როდესაც საგადახდო დავალება გადაცემულია განმეორებით; ვ) იმ შემთხვევაში, თუ კლიენტის მიერ მის მომსახურე ბანკში გადაცემული საგადახდო დავალება შეცდომითაა გადაცემული, კლიენტი ვალდებულია ხელშეკრულებით გათვალისწინებულ ვადაში შეატყობინოს ბანკს აღმოჩენილი შეცდომის შესახებ. კლიენტმა შეტყობინებაში უნდა ასახოს საგადახდო დავალების რეკვიზიტები და მის მიერ გამოვლენილი არასწორი რეკვიზიტები; ზ) თუ ბანკს არ წარედგინა ასეთი შეტყობინება, არასწორი რეკვიზიტებით გადაცემული საგადახდო დავალება ჩაითვლება შესასრულებლად მიღებულად და ბანკი პასუხს არ აგებს მისი შესრულების შედეგად დამდგარ ფაქტზე. იმ შემთხვევაში, თუ კლიენტის მიერ შეცდომით გადაცემული საგადახდო დავალების გამო მომსახურე ბანკმა განიცადა

ზარალი, კლიენტი პასუხისმგებელია ბანკისათვის მიყენებული ფაქტობრივი ზარალისათვის. 2. საგადახდო დავალების ქაღალდით წარდგენა: ა) საგადახდო დავალება (მათ შორის საინკასო დავალება) ბანკში წარსადგენად ძალაშია მათი გამოწერიდან ათი კალენდარული დღის განმავლობაში (გამოწერის დღის ჩაუთვლელად); ბ) საგადახდო დავალებები შესასრულებლად მიიღება კლიენტის ანგარიშზე საკმარისი სახსრების არსებობის შემთხვევაში (გარდა ბიუჯეტის და მასთან გათანაბრებულ გადასახდელებზე წარდგენილი საგადახდო დავალებებისა, რომლებიც მიიღება კლიენტის ანგარიშზე თანხების არსებობის მიუხედავად და აღირიცხება ვადაზე გაუნაღდებელი საბუთების კარტოთეკაში). საგადახდო დავალების კარტოთეკაში მოთავსების შემთხვევაში, საგადახდო დავალების ყველა ეგზემპლარის ზედა მარჯვენა კუთხეში კეთდება შენიშვნა კარტოთეკაში მოთავსების შესახებ, თარიღის ჩვენებით. ვადაზე გაუნაღდებელი საბუთების კარტოთეკიდან საგადახდო დავალებების განაღდების წესები მოცემულია N3 დანართში; გ) ქაღალდის საგადახდო დავალების გაფორმება (დოკუმენტალური ოპერაციების გარდა) ხდება ამ წესების 8 და 9 დანართებში მოცემული ფორმით, რომელთა შევსების წესებიც მოცემულია N4 დანართში. ველები, რომელთა რეკვიზიტებსაც მნიშვნელობები არ გააჩნია, რჩება შეუვსებელი (არასაბიუჯეტო ანგარიშებზე გადარიცხვის ამსახველი საგადახდო დავალებების ველები); დ) კლიენტის მიერ ამ წესების დაცვით შედგენილი ქაღალდის საგადახდო დავალება ბანკს წარედგინება ერთ ეგზემპლარად, რომელიც წარმოადგენს დედანს. საგადახდო დავალების კლიენტისადმი დასაბრუნებელი მეორე ეგზემპლარი (ან ნებისმიერი სხვა რაოდენობა, რომელსაც ბანკი განსაზღვრავს დამოუკიდებლად და აისახება ოპერაციების წარმოების შესახებ ბანკის მიერ გაცხადებულ პირობებში – შიდასაბანკო წესებში) არის მისი ასლი (გადაღებული ასლგადამღები ტექნიკით, სკანერით და ა. შ. – თუ ასლის გადაღება შესრულებულია ხარვეზების გარეშე). საგადახდო დავალების დედანი რჩება ბანკში და წარმოადგენს ოპერაციის შესრულების საფუძველს, ხოლო ბანკის პასუხისმგებელი

მუშაკის ხელმოწერით და შტამპით დამოწმებული ასლი, სავალდებულო წესით, უბრუნდება კლიენტს; ე) კლიენტის მიერ ბანკში წარდგენილ საგადახდო დავალების ნაწილობრივი შესრულების პირობის მითითება დაუშვებელია. თანმიმდევრული ოპერაციების ჯგუფი,რომლებიც თავისთავად წარმოადგენენ მონაცემებთან მუშაობისლოგიკურ ერთეულს.

1.3 ელექტრონული ფოლის პოპულარიზაცია როგორც თანამედროვე ცხოვრების ნაწილი

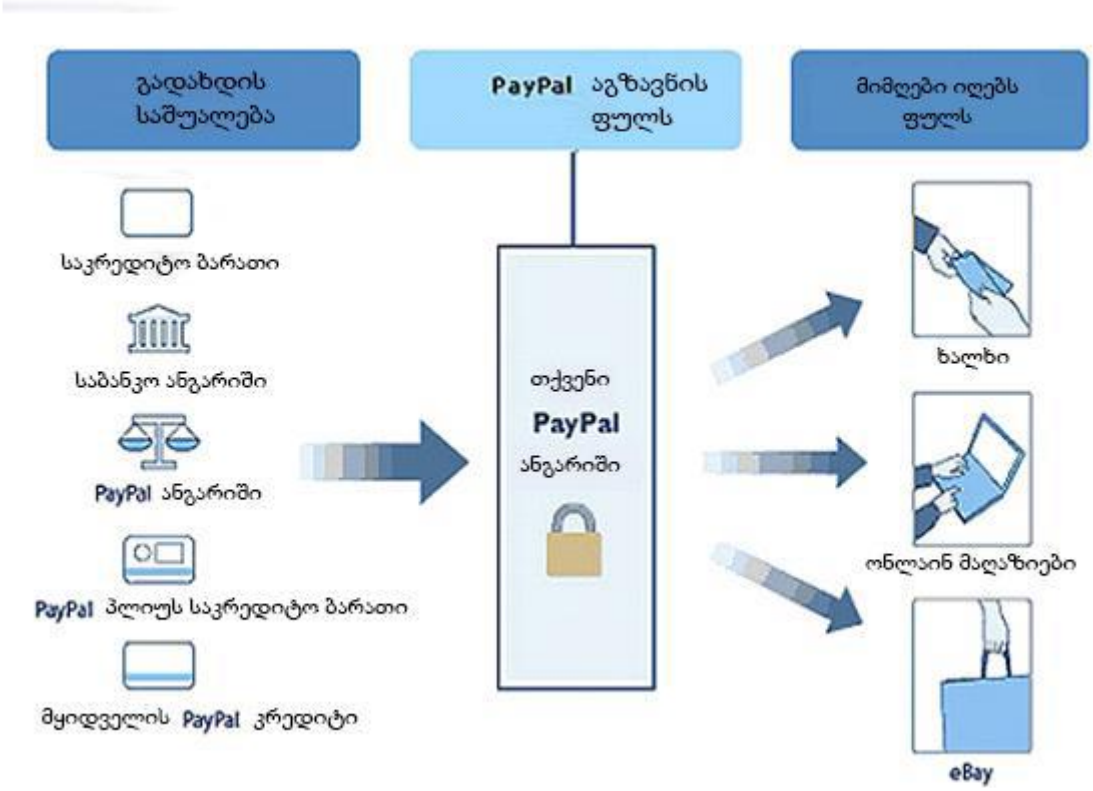
საგადამხდელო სისტემები უზრუნველყოფენ სხვადასხვასახის ტრანზაქციებს: ბანკის განყოფილებებში ნაღდი ფულისყიდვა და გამოტანა, ბანკომატიდან ნაღდი ფულის გამოტანა,კლიენტის ანგარიშზე არსებული ნაშთის შესახებ ინფორმაციისმიღება და სხვა. ტრანზაქციები განსხვავდებიან აგრეთვე საგადამხდელოსისტემაში ბარათის შესახებ ინფორმაციის წარდგენის მეთოდით.არსებობენ ელექტრონული ტრანზაქციები (ბარათის შესახებინფორმაცია იკითხება მაგნიტური ზოლიდან/ჩიპიდან) და ხმოვანიავტორიზაციის ტრანზაქციები (paper based). CNP - ტრანზაქცია (Cardholder Not Present) წარმოადგენსპლასტიკური ბარათის მეშვეობით ყიდვის ოპერაციას, რომლისგანხორციელების მომენტში კლიენტი პირადად არ იმყოფებასავაჭრო წერტილში, ხოლო ავტორიზაციისათვის საჭირო თავისიბარათის რეკვიზიტებს (ბარათის ნომერი, მოქმედების ვადა)დაუსწრებლად ატყობინებს სავაჭრო წერტილს (წერილი, ფაქსი,მონაცემთა გადაცემის ქსელები და სხვა). ელექტრონული საგადამხდელო სისტემის ტექნოლოგიურიბირთვია საპროცესინგო ცენტრი. ის წარმოადგენს სპეციალიზირებულგამოთვლით ცენტრს, რომელიც ფუნქციონირებს განსაკუთრებულპირობებში და გარანტირებულად დროის რეალურრეჟიმში ამუშავებს ტრანზაქციების ინტენსიურ ნაკადს. მართლაც სადებეტო ბარათის გამოყენება განაპირობებს ყოველი ბარათის“ონლაინ” ავტორიზაციის აუცილებლობობას საგადამხდელო სისტემის

მომსახურეობის ნებისმიერ წერტილში. საკრედიტობარათებთან ოპერაციების დროს კი ავტორიზაცია ყოველთვისარ არის აუცილებელი, მაგრამ მაგალითად ბანკომატებში ფულისმიღების დროს ავტორიზაცია ყოველთვის ტარდება. საპროცესინგოცენტრის გამოთვლით შესაძლებლობებს არანაკლებმოთხოვნებს უყენებს დღის შედეგების შეჯამების დროს ანგარიშსწორებისჩატარებისათვის მონაცემების მომზადება. ამ დროსდამუშავებას ექვემდებარება ტრანზაქციების პროტოკოლებისუმეტესი ნაწილი, ხოლო შესრულების დრო შეზღუდულია რამოდენიმესაათით. ამგვარად ელექტრონული საგადამხდელო სისტემის საიმედო ფუნქციონირებისათვის საჭიროა; საპროცესინგო ცენტრში არსებითი გამოთვლითი სიმძლავრეების არსებობა; განვითარებული კომუნიკაციური ინფრასტრუქტურის არსებობა, რადგან საპროცესინგო ცენტრს უნდა ჰქონდეს დიდი რაოდენობის გეოგრაფიულად დაშორებული წერტილების ერთდროული მომსახურეობის შესაძლებლობა ზემოთთქმულის გათვალისწინებით შეიძლება გავაკეთოთ შემდეგი დასკვნა: წარმატებული ელექტრონული საგადამხდელოსისტემა უნდა აკმაყოფილებდეს შემდეგ ძირითად მოთხოვნებს: ოპერირებდეს ელექტრონული ფულით, მაგრამ იმავდროულად უნდა გააჩნდეს ანგარიშის შევსების სხვა ფართო ესაძლებლობა (მათ შორის საკრედიტო ბარათების მეშვეობით), უნდა გააჩნდეს ერთიანი საემისიო ცენტრი და რამოდენიმე ძლიერი ბანკის მხარდაჭერა, გამოიყენოს ინფორმაციის დაცვის სანდო მექანიზმი, რომელიც დამყარებული იქნება შემოწმებულ კრიპტოგრაფიკულ სტანდარტებზე, იყოს იაფი ინტერნეტ-მომხმარებლებისათვის . ანგარიშსწორებისჩატარებისათვის მონაცემების მომზადება. ამ დროსდამუშავებას ექვემდებარება ტრანზაქციების პროტოკოლებისუმეტესი ნაწილი, ხოლო შესრულების დრო შეზღუდულია რამოდენიმესაათით. ამგვარად ელექტრონული საგადამხდელო სისტემის საიმედოფუნქციონირებისათვის საჭიროა; საპროცესინგო ცენტრში არსებითი გამოთვლითი სიმძლავრეების არსებობა; განვითარებული კომუნიკაციური ინფრასტრუქტურის არსებობა, რადგან საპროცესინგო

ცენტრს უნდა ჰქონდეს დიდი რაოდენობის გეოგრაფიულად დაშორებული წერტილების ერთდროული მომსახურეობის შესაძლებლობა ზემოთთქმულის გათვალისწინებით შეიძლება გავაკეთოთშემდეგი დასკვნა: წარმატებული ელექტრონული საგადამხდელოსისტემა უნდა აკმაყოფილებდეს შემდეგ ძირითად მოთხოვნებს: ოპერირებდეს ელექტრონული ფულით, მაგრამ იმავდროულად უნდა გააჩნდეს ანგარიშის შევსების სხვა ფართო ესაძლებლობა (მათ შორის საკრედიტო ბარათების მეშვეობით) უნდა გააჩნდეს ერთიანი საემისიო ცენტრი და რამოდენიმე ძლიერი ბანკის მხარდაჭერა გამოიყენოს ინფორმაციის დაცვის სანდო მექანიზმი, რომელიც დამყარებული იქნება შემოწმებულ კრიპტოგრაფიკულ სტანდარტებზე იყოს იაფი ინტერნეტ-მომხმარებლებისათვის.

განვიხილოთ მსოფლიოში დღეს ფართოდ გავრცელებული და ცნობილი ელექტრონული საგადასახადო სისტემები: **PayPal** (www.paypal.com)- მსოფლიოში ერთ-ერთი უმსხვილესი დებეტური ელექტრონული საგადამხდელო სისტემა. მოქმედებს 1998 წლიდან. 2002 წელს ის შეისყიდა აუქციონმა ebay(www.paypal.com). **PayPal** უზრუნველყოფსაუქციონზე საქმიანი გარიგებების 85%. დღესდღეობითსისტემა მუშაობს მსოფლიოს 190 ქვეყანაში დაგააჩნია 164 მილიონი დარეგისტრირებული მომხმარებელი.გადახდები სისტემაში წარმოებს დაცული შეერთების მეშვეობითანგარიშის ვერიფიკაციის დროს მომხმარებლისელექტრონული ფოსტის მისამართის და პაროლის შეყვანისშემდეგ. სისტემის მთავარი უპირატესობებია: გადახდებისმყისიერი ჩარიცხვა, უსაფრთხოების მაღალი ხარისხი დათანხის მთლიანი და ნაწილობრივი დაბრუნება თუ ნაყიდისაქონელი არ არის მიღებული ან არ შეესაბამება მის აღწერილობას. **PayPal** - ის საშუალებით შესაძლებელია:
10 000-მდე სხვადასხვა ონლაინ მაღაზიებში შევიძინოთ პროდუქტი; უსაფრთხოდ შევიძინოთ საქონელი ebay-ზე; ჩვენ ახლობლებთან გავაგზავნოთ ფული მსოფლიოს 190 ქვეყანაში; პროდუქტის საფასური გადავიხადოთ ჩვენთვის სასურველ ვალუტაში; 45 დღის განმავლობაში

თუკი ვერ მივიღებთ შეძენილ პროდუქტს ან მიღებული საქონელი განსხვავებული აღმოჩნდება ჩვენი სასურველი ნივთისგან, მოქმედებს ,,PayPal Buyer Protection Policy“ რომლის საშუალებითაც შეგვეძლება გადახდილი თანხის დაბრუნება; ინტერნეტით გავყიდოთ ჩვენი პროდუქტი; გადახდა/ყიდვა ვაწარმვოოთ ელ.ფოსტის საშუალებით; პირდაპირ ჩვენი საბანკო ანგარიშიდან მივიღოთ ან გადავიხადოთ მეორე პირისგან მოვითხოვოთ თანხა ელ.ფოსტის საშუალებით; ვაგზავნოთ ბიზნეს ინვოისები უფასოდ (invoice). **E-gold (www.Egold.com)** - მსოფლიოში ყველაზე მსხვილი და პოპულარული ელექტრონული საგადამხდელო სისტემა. E-gold-ის ყოველდღიური ბრუნვა შეადგენს 500 000 $ -ზე მეტს. სისტემა შეიქმნა და ამუშავდა 1996 წელს. E-gold არის ინტერნაციონალური საგადამხდელო სისტემა, რომლის ფულადი საშუალებები გაიგივებულია ძვირფას ლითონებთან. ეს თავისებურება მას განსაკუთრებით ეფექტურს ხდის საერთაშორისო გადახდების წარმოების დროს, რადგანაც მომხმარებლების ანგარიშები არ არის მიბმული არც ერთ ნაციონალურ ვალუტასთან.



E-gold- ის მომხმარებელი შეიძლება უფასოდ გახდესნებისმიერი ადამიანი მსოფლიოს ნებისმიერი ქვეყნიდან.ანგარიშზე ფული ინახება არჩეული ძვირფასი ლითონისშესაბამის ექვივალენტურ მასასთან. დაფარულად ეს არისოქრო. მაგრამ მომხმარებლებს შეუძლიათ მისი გაყიდვა დაპლატინის, ვერცხლის ან პალადიუმის ყიდვა.სხვა საგადამხდელო სისტემებში მომხმარებლის ფულისექვივალენტი შეიძლება გახდეს რომელიმე მსოფლიოვალუტა (დოლარი, ევრო და სხვა). თუ 74 მსოფლიო ბაზარზედოლარის კურსი ეცემა, მაშინ უფასურდება მომხმარებლისფული საგადამხდელო სისტემის საფულეში. E-gold-ისსისტემაში კი ამ უსიამოვნების აცილება შესაძლებელია,რადგან ის 100%-ით უზრუნველყოფილია ძვირფასი ლითონებით. მთელ თავის ოქროს მარაგსE-gold ინახავსბანკში Nova Scotia (აშშ, ტორონტო). სხვა საგადამხდელო სისტემებისაგან განსხვავებით E-gold-ში არ არის პროგრამული უზრუნველყოფა. ანგარიშების და ფულის მართვა ხორციელდება ფირმის ვებ-საიტიდან. ერთი მხრივ ეს კარგია, რადგან არ არის საჭირო პროგრამული უზრუნველყოფის გადმოწერა და დაყენება. მეორეს მხრივ კი მომხმარებელმა რომ მიაღწიოს თავის ანგარიშამდე, საჭიროა რამოდენიმეჯერ ჩამოტვირთოს ვებ-გვერდები ფირმის ვებ-საიტიდან. ეს კი ნაკლებად მოსახერხებელია. E-gold-ში ყველა მონაცემები გადაიცემა დაცული პროტოკოლით https://,რაც განაპირობებს მაღალიუსაფრთხოების ხარისხს. თავისი არსებობის მანძილზევერავინ ვერ გაარღვია E-gold-ის უსაფრთხოების სისტემა **Mondex (www.mondexusa.com)** - ელექტრონული საგადამხდელოსისტემა, რომელიც აერთიანებს ტრადიციული ნაღდი ფულის თვისებებსელექტრონული გადახდებისმოხერხებულობასთან. სისტემაშეიმუშავა კომპანიამ "mondex International". მისიაქციების 51% ეკუთვნისკომპანია Mastercards-ს, ხოლოდანარჩენი 49% მსოფლიოწამყვანბანკებსდასაფინანსოინსტიტუტებს. სისტემა Mondex ამუშავდა 1994 წელსდიდიბრიტანეთის ქალაქსუინდონში. ელექტრონულინაღდიფულიშეიძლება მარტ ბარათზე იყოს ჩატვირთული ქსელთან მიერთებული კომპიუტერისმეშვეობით. ბარათის მფლობელებს

შორის ანგარიშსწორებისათვისშემუშავებულიასპეციალური მოწყობილობა - ‘‘საფულე’’, ხოლოანგარიშზენაშთის გასარკვევად - ჯიბისდამთვლელი.

CyberCash (www.cybercash.com) - ამერიკული კომპანია, რომელმაც შეიმაშავა ელექტრონული საგადამხდელო სისტემა ინტერნეტში ანგარიშსწორებისას საკრედიტო ბარათების მეშვეობით. არც ელექტრონულ მაღაზიას და არც რომელიმე სხვა გამყიდველს არ შეუძლია გაიგოს ინფორმაცია კლიენტის საკრედიტო ბარათზე. პრაქტიკულად ნულამდე არის დაყვანილი ინტერნეტში მონაცემთა ხელში ჩაგდების მცდელობა. CyberCash არ იტოვებს არავითარ მონაცემებს ყიდვის შესახებ და მხოლოდ ბანკ–ემიტენტს გააჩნია ყიდვის ყველა დეტალზე ინფორმაცია.პროგრამული უზრუნველყოფა (CyberCashwallet) და მომსახურება უფასოა. კომპანია უმატებს 2% ოპერაციის მოცულობიდან. სისტემა იდეალურია კატალოგებით გაყიდვის დროს. აღსანიშნავია, რომ კომპანიამ აამუშავა სპეციალური მიკროგადახდების სისტემა CyberCoin.

 CheckFree (www.checkfree.com) - მსოფლიოში დღესდღეისობით ყველაზე გამოყენებული ელექტრონული საგადამხდელო სისტემაა, რადგან ის ჩართულია ყველაზე მსხვილ ინტერნეტ პროვაიდერების CompuServe და AOL– ის სტანდარტულ პაკეტში. სისტემამ 1995 წელს კლიენტებს შესთავაზა ინტერნეტში ელექტრონული ჩეკური სამსახური CheckFree Payment Services. კლიენტის მოთხოვნის მიხედვით ეს სამსახური გამოწერს ჩეკს და ასრულებს მყიდველსა და გამყიდველს შორის ელექტრონულ ანგარიშსწორებას. ინტერნეტში მიკროგადახდებს სისტემა აწარმოებს. First Virtual (www.firstvirtual.com) – ეს არის ინტერნეტში პრაქტიკულად პირველი საგადამხდელო სისტემა. კომპანიამ თავისი სისტემა Internet Payment System აამუშავა 1994 წელს. სისტემაში დაშვებისათვის მომხმარებლებმა საჭიროა დაარეგისტრირონ საკრედიტო ბარათის ნომერი საიდენტიფიკაციო ნომერის მისანიჭებლად First Virtual–ში ტელეფონით ან ფაქსით. შემდგომში ეს ნომერი გამოიყენება საკრედიტო ბარათის ნომერის ნაცვლად ინტერნეტში ოპერაციების ჩატარების დროს. სისტემის თავისებურებაა, რომ ის არ იყენებს უსაფრთხოების დაცვის რთულ

სისტემებს და კლიენტებიდან ტრანზაქციის დადასტურებას აწარმოებს ელექტრონული ფოსტის საშუალებით **ACH** (**Automated Clearing House**) - არის ელექტრონული ქსელი ფინანსური გადარიცხვებისთვის ამერიკის შეერთებულ შტატებში. ACH ამუშავებს დიდი მოცულობის საკრედიტო და სადებეტო ტრანზაქციებს (გადარიცხვებს). ACH საკრედიტო გადარიცხვები მოიცავს პირდაპირ სადეპოზიტო გადასახდელებს და გამყიდველის გადასახდელებს. ACH პირდაპირი სადებეტო გადარიცხვები შეიცავს სამომხმარებლო გადახდის შესახებ სადაზღვევო პრემიას, იპოთეკური სესხებს და სხვა სახის გადასახადებს. სადებეტო გადარიცხვები ტრანზაქციები) მოიცავს ასევე POP (point-of-purchase) კონვერტაციის პილოტურ პროგრამას, რომელიც სპონსორდება Electronic Payment Association მიერ. ორივე ახელმწიფოც და კომერციული უწყებები იყენებენ (ACH) გადახდებს. Paycash-ის ციფრული ფულის პირველმა სამამულო სისტემის აპრობაციამ წარმოდგენილი ბანკით ,,ტავრიული" (სანკტ-პეტერბურგი) სტარტი აიღო 1998წ. დასაწყისში. 1999წ თებერვლიდან სისტემა Paycash-ში გაჩნდა შესაძლებლობა გაკეთდეს ესყიდვები ინტერნეტის მეშვეობით რეალური ფულის მეშვეობით. მსყიდველობითი სისტემის მონაწილეებია ბანკი და კლიენტი. კლიენტის სახით შეიძლება მოგვევლინონ ფიზიკური და იურიდიული პირები. ბანკის აზრით ყველა კლიენტი თანასწორია. რათა კლიენტმა მიიღოს გადასახადები, არ არის საჭირო ,,მაღაზიის" განსაკუთრებული სტატუსი. ყველა ოპერაციას კლიენტი ასრულებს საფულის უზრუნველყოფის სპეციალური პროგრამის მეშვეობით. სისტემის მუშაობის სქემა ასე გამოიყურება. მომავალი კლიენტი ,,საფულის" მეშვეობით ხსნის ანგარიშს ბანკში და გადაჰყავს ამ

ანგარიშზე ფული. ამის შემდეგ იგი ხდება კლიენტი. კლიენტი ქმნის თავის კომპიუტერში საფულის მეშვეობით ერთ ან რამოდენიმე საგადასახადო წიგნაკს. შემდეგ ისევ ,,საფულის" მეშვეობით გადაჰყავს რაღაც თანხა თავისი ანგარიშიდან ერთ-ერთ წიგნაკში ანუ თავის კომპიუტერში. ამავე დროს ბანკი ვერ საზღვრავს რომელ წიგნაკში ჩაირიცხება თანხა, ვის ეკუთვნის კონკრეტული საგადასახადო წიგნაკები. ახლა უკვე კლიენტი

მზადაა ანგარიში გაასწოროს ინტერნეტში, ანონიმურად, იმ ფულით, რომელიც მის საგადასახადო წიგნაკში დევს. თითოეული გადასახადი ავტორიზირდება ბანკის მეშვეობით, ჯაჭვი ასეთია: გამყიდველი →მყიდველი →გამყიდველი →ბანკი →გამყიდველი →მყიდველი. თავდაპირველად გამყიდველი სთხოვს ფულს მყიდველს, მოთხოვნაში ირთვება ხელშეკრულების ხელმოწერილი კონტრაქტი. შემდეგ მყიდველი უგზავნის გამყიდველს გადასახადის მონაცემებს. გამყიდველი აგზავნის მათ ბანკში, ბანკი აწარმოებს აუცილებელ გადამოწმებას და უგზავნის გამყიდველს ქვითარს, ქვითარსაც მყიდველისათვის. გამყიდველი აცნობებს მყიდველს თავის გადაწყვეტილებებს და უგზავნის მას ბანკის დაშიფრულ მონაცემებს მყიდველის სახელზე.

პლასტიკური ბარათები- საბანკო ბარათი ანუ პლასტიკური ბარათი წარმოადგენს ანგარიშების და მსგავსი დოკუმენტების საშუალებას, რომელიც ხორციელდება ბარათის მფლობელის ანგარიშზე. პლასტიკური ბარათის ერთ-ერთი ძირითადი ფუქციაა – მისი მომხმარებლისსაგადასახადო სისტემის იდენტიფიკაციის უზრუნველყოფა. ამ ბარათზე შეიტანება ემიტენტის და საგადასახადო სისტემის ლოგოტიპები. ბარათის მფლობელის სახელი, ანგარიშის ნომერი, მოხმარების ვადა და შეიძლება მფლობელის სურათიც და ხელმოწერაც. საგადასახადო სისტემები, რომლებიც გამოიყენებს საკრედიტო ბარათებს, უზრუნველყოფენ უსაფრთხოებასა და აუტენტაფიკაციას. საკრედიტო ბარათის გამოყენებით ინტერნეტიდან საქონელის ყიდვა მიმდინარეობს იგივე სცენარით, მხოლოდ დამატებით ტრანზაქციისა და აუტენტიფიკაციის უსაფრთხოების უზრუნველყოფით, როგორც მყიდველსა ისე გამყიდველსა. უკვე წარმოიშვა ინტერნეტში საკრედიტო ბარათების გამოყენების სხვადასხვა ფორმები. მათი განმასხვავებელი ნიშნებია: ტრანზაქციისა და საპროგრამო უზრუნველყოფის უშიშროების დონე, რაც აუცილებელია მყიდველისა და გამყიდველისათვის მისი განხორციელებისათვის. ამჟამად საკრედიტო ბარათების ტრანზაქცია აღწევს 90%ტრან- ზაქციის საერთო მოცულობიდან რომელიც

შესრულებულია ინტერ- ნეტში. საბანკო სისტემების განვითარებასთან ერთად, წარმოიქმნა ლასტიკური ბარათების სხვადასხვა სახეობა, რომლებიც ერთმანეთისგან განსხვავდება დანიშნულებით, ფუნქციური და ტექნიკური მახასიათებლებით, ანგარიშსწორების მექანიზმის თვალსაზრისით გამოყოფენ ორმხრივ და მრავალმხრივ სისტემებს. ორმხრივი ბარათების წარმოქმნა მოხდა ანგარიშსწორების მონაწილეთა შორის ორმხრივი შეთანხმების საფუძველზე. ამ დროს ბარათის მფლობელს საშუალება აქვს ჩაკეტილ ქსელში საქონლის შესყიდვისა, რომელსაც თავის მხრივ ბარათის ემიტენტი აკონტროლებს (უნივერმაღები, ბენზინის გასამართი სადგურები და სხვა). ამ ბარათებისგან განსხვავებით მრავალმხრივ სისტემებს ხელმძღვანელობენ საბანკო ბარათების ეროვნული ასოციაციები ან კიდევ კომპანიები, რომლებიც ტურიზმისა და გართობის ბარათებს უშვებენ (მაგ. American express). ბარათების სხვაგვარი დაყოფა მათი ფუნქციური დახასიათებით განისაზღვრება. განსხვავდება საკრედიტო და დებიტური ბარათები. პირველი უკავშირდება ბანკში საკრედიტო ხაზის გახსნას, რაც მფლობელს საშუალებას აძლევს, საქონლის ყიდვისას ან საკრედიტო სესხის აღებისას კრედიტით ისარგებლოს ,მეორე განკუთვნილია საბანკო ავტომატებიდან ნაღდი ფულის მისაღებად ან კიდევ ელექტრონული ტერმინალების საშუალებით საქონლის შესყიდვას.

ტურიზმისა და გართობის ბარათები (travel and entertainment cards, შემოკლებით T & E-cards). ზემოთხსენებული ტერმინოლოგიის თანახმად ეს “საგადასახადო ბარათებია”, რომლებიც მომსახურეობის სფეროზე სპეციალიზირდებიან. მაგ.“American express” და “Diners club” ბარათებს მთელ მსოფლიოში ათობით ათასი სავაჭრო დასერვისის სფეროში მომსახურე ორგანიზაცია იღებს.

ვაჭრობისა და მომსახურების სფეროში გავრცელებულია კერძო საგადასახადო ბარათები (private cards, retail cards,affinity cards). ამ ბარათების მოხმარება იზღუდება სავაჭრო დაწესებულებების დახურული ქსელით. ბარათები საბანკო ავტომატებისათვის(ATM cards) დებიტორული ბარათების სახესხვაობაა, რომლებიც მფლობელს საშუალებას აძლევს

მიიღოს ნაღდი ფული ბანკში დარჩენილი ანგარიშის ფარგლებში. ბარათის გამოყენება 24 საათის განმავლობაშია შესაძლებელი.

საქართველოში პირველად პლასტიკური ბარათი გამოშვებული იქნა 1996 წელს, ეს პლასტიკური ბარათები გამოშვებული იყო გაერთიანება UFC – ის მიერ, ამ პლასტიკური ბარათის ემიტენტი ბანკი იყო აბსოლუტ ბანკი, შემდგომში ამ გაერთიანების წევრები გახდნენ თიბისი ბანკი, თბილკომბანკი, თბილკრედიტბანკი და ინტელექტბანკი. UFC – ის პლასტიკური ბარათები წარმოადგენდნენ სადებეტო ბარათების ნაირსახეობას 1997 წლის 17 იანვარს საქართველოში ჩამოყალიბდა სააქციო საზოგადოება "ჯორჯიან ქარდი". მისი ერთ-ერთი აქციონერი არის ფრანგული ფირმა "იმედი", იგი ფლობს აქციათა საკონტროლო პაკეტს, მისი წილი შეადგენს 51 %-ს. "ჯორჯიან ქარდი" - ის აქციონერები არიან ასევე ქართული ბანკებიც.

"ჯორჯიან ქარდი" - ის პლასტიკური ბარათები იყოფა შემდეგ ჯგუფებად:Classic, Gold და Business. Classic-ისა და Gold-ისპლასტიკური ბარათები განკუთვნილია ფიზიკური პირებისათვის , ამასთან Gold-ის ბარათები Classic-ის ბარათებთან შედარებით მეტი პრიორიტეტით გამოირჩევა, ეს ბარათები გაიცემიან მაღალი კრედიტუნარიანობის მქონე კლიენტებზე. Businessპლასტიკური ბა- რათები კიგანკუთვნილიაიურიდიულიპირებისათვის.

Webmoney Transfer (http://www.webmoney.ru/) - სისტემა გახსნილია თავისუფალი ხმარებისათვის, ყველა მსურველისთვის მსოფლიოს ყველა კუთხეში. სგადახდო სისტემა Webmoney Transfer უნივერსალური სტრუქტურაა. იგი აძლევს საშუალებას ინტერნეტ ქსელის ნებისმიერ მომხმარებელს განახორციელოს უსაფრთხო ფულადი ანგარიშსწორება რეალურ დროში. სისტემის კლიენტები არიან მოვაჭრეები და მყიდველები პროდუქტებისა და მომსახურეობის. საგადახდო სისტემა Webmoney Transfer - ის დახმარებით შეიძლება მომენტალური შეუქცევადი ოპერაციების განხორციელება დაკავშირებული ქონების გადაცემის უფლებასთან ნებისმიერ საქონელზე და მომსახურეობაზე, საკუთარი ვებ-

სერვერების შექმნა ან საწარმოთა ქსელის შექმნა, ოპერაციების განხორციელება სხვა მონაწილეებთან. საგადახდო სისტემაში ტრანზაქციულ საშუალებად გამოიყენება სიმბოლო MW (Webmoney), რომელიც არსებობს რამოდენიმე ტიპისა და ინახება მფლობელის ელექტრონულ საფულეში: WMR - ეკვივალენტიRUR(რუბლი) – R-საფულეზე WME - ეკვივალენტიEUR(ევრო) – E-საფულეზე WMZ ეკვივალენტიUSD (დოლარი) – Z-საფულეზე სისტემაში რეგისტრაცია და სახსრების მართვა ხორციელდება საკლიენტო პროგრამა WM KEEPER საშუალებით. მისი საშუალებით შესაძლებელია განხოციელდეს მომენტალური ანგარიშსწორება WM - ში საგადახდო სისტემების სხვა კლიენტებთან, გადაიხადოთ თანხა საქონელზე და მომსახურეობაზე ქსელში.

აპარატურულ პროგრამული კომპლექსური საშუალებები უზრუნველყოფს განახორციელოთ უსაფრთხო ტრანზაქციები. კომპიუტერული უსაფრთხოების სპეციალური კომპლექსი სრულიად გამორიცხავს თქვენი საშუალებებისა და ინფორმაციის არასანქცირებულ უფლებას. კონფიდენციალურ შეტყობინებათა სამსახურის საშუალებით თქვენ შეგიძლიათ აწარმოოთ დაცული მიმოწერა სხვა მომხმარებლებთან.

საქართველოში ელექტრონული კომერცია ნელა მაგრამ მაინც ვითარდება. სახელმწიფო ახალ ნაბიჯებს დგამს, - საკანონმდებლო-ნორმატიული ბაზა, კიბერუსაფრთხოება, ლოჯისტიკა და შეკვეთილი ნაწარმის ადგილზე მიტანა, მომხმარებლების უფლებების დაცვა, ელექტრონული ვაჭრობის პოპულარიზაცია, - ეს ის თემებია, რომლებიც საჭიროებს დახვეწას, რათა კიდევ უფრო განვითარდეს საქართველოში ელექტრონული კომერცია.

ელ. კომერციის განვითარების ნათელი მაგალითია საქართველოს ელექტრონულად საგადამხდელო სისტემის, კომპანია PayPal-ის ინტერნეტ სისტემასთან მიერთება და დღეიდან მისი საშუალებით ჩვენს ყველა 82

მოქალაქეს შეუძლია მსოფლიოს მასშტაბით არსებულ ათასობით ელექტრონულ მაღაზიაში სასურველი პროდუქტი შეიძინოს.

აქამდე ბევრი ცნობილი ვებ-გვერდი ქართული ბარათით სარგებლობის საშუალებას არ იძლეოდა, ახლა კი „ფეიფალის“ საგადამხდელო სერვისის გამოყენებით რამდენიმე წუთში, მარტივად ხდება ანგარიშის გახსნა და მყიდველებს აღარ სჭირდებათ გამყიდველის ანგარიშის დეტალების, საქონლის მიმღების მისამართის ან ტრანზაქციი ხელახლა გამეორება. PayPal-ის სერვისი განსხვავდება ქვეყნებს შორის. საქრთველო ჯერ მხოლოდ PayPalმინიმალური მომსახურების პაკეტის კატეგორიის ქვეყნებში შევიდა მაგრამ დასაწყისისთვის ესეც კარგია.
„საქართველოს ბანკის“ (http://bankofgeorgia.ge/) შვილობილი კომპანია ipay-გვთავაზობს პროექტ iDeals.ge, რომელიც არისინდივიდუალური და ჯგუფური შესყიდვების ვებგვერდი, სადაც თქვენ მიიღებთ შემოთავაზებებს თქვენთვის სასურველ საქონელსა და მომსახურებაზე წარმოუდგენლად დაბალ ფასად. საქონლისმომსახურების შესაძენად ანგარიშსწორება ხდება პირდაპირვებგვერდზე, პლასტიკური ბარათების საშუალებით. შენაძენის დასამოწმებლად, თქვენ მიიღებთ სპეციალურ კოდს, თქვენს „პირად კაბინეტში“ და ელფოსტაზე. მიღებულ სპეციალურ კოდს, პირადობის დამადასტურებელ საბუთთან ერთად (პირადობის მოწმობა ან საქართველოს მოქალაქის პასპორტი), წარადგენთ შესაბამის სავაჭრო თუ მომსახურების ობიექტში და მიიღებთ შენაძენს.მისი საშუალებით შესაძლებელია, თითქმის ყველა სახის გადახდის განხორციელება: დაწყებული კომუნალური გადახდებით დამთავრებული სხვა სახელმწიფო სერვისებით. პოსტერმინალებით მომსახურება საგადამხდელო სისტემის ფარგლებში - არის ასევე საქართველოს ბანკის სერვისი , რომელიც დაგეხმარებათ: -დაზოგოთ ხარჯები; - გაზარდოთ გაყიდვები და მოიზიდოთ ახალი მომხმარებლები; - თქვენს შესახებ ინფორმაცია მიაწოდოთ მომხმარებელს; -გაიმარტივოთ ანგარიშსწორებასთან დაკავშირებული პროცედურები მისი ძირითადი უპირატესობებია: 1.მხოლოდსაქართველოსბანკისტერმინალებშიარისშესაძლებელიყველატიპ

ისბარათითგადახდა: VISA, MasterCard, American Express (ექსკლუზიურად 2009 წლიდან) დაDinersclub/Discovery (ექსკლუზიურად2011 წლიდან);

2. საქართველოში არსებული ბარათების დაახლოებით 60-65% საქართველოსსაპროცესინგოცენტრისმიერარისემიტირებული (1,5 მლნ-ზემეტი VISA/ MasterCard და 107 ათასზემეტიAmerican Express ბარათი), რაც საშუალებას მოგცემთდა ზოგიერთი ხარჯები; 3. საჭროების შემთხვევაში ტექნიკურ მხარდაჭერას მიიღებთ 24 საათისგანმავლობაში; . ქსელში გაერთიანებულია 3000-ზემეტი საშუალო თუ მსხვილი ორგანიზაცია, რაც პოს ტერმინალებით მოსარგებლე კომპანიების 80%-ზემეტსშეადგენს; 5. ბანკითავისპარტნიორსავაჭრორგანიზაციებთანერთადახორციელებსსხვად ასხვაწამახალისებელაქციებს. შედეგად, ინფორმაცია სხვადასხვა სასაკომუნიკაციო არხების დახმარებით იგზავნება მომხმარებელთან – საქართველოს ბანკის ბარათების მფლობელებთან. აქციების შედეგად სავაჭრო ობიექტებს ეზრდებათ ტრანზაქციების მოცულობა და ეძლევათ შესაძლებლობა მოიზიდონ ახალი მომხმარებლები. ასევე სრულიად ახალი ინტერნეტ ბანკი (ExpressOnline)- იურიდიული პირებისთვის, რომლის მეშვეობით რათქმაუნდა, სხვა

სტანდარტულ საბანკო ოპერაციებთან ერთად შეგიძლიათ განახორციელოდ გადახდები ყველა სახის და გადარიცხვები TBC ბანკის (http://www.tbcbank.ge/) Viza და Mastercard პლასტიკური ბარათები - სწრაფი, მოქნილი და უსაფრთხო სისტემაა ინტერნეტ გადახდების მისაღებად და ასევე თითოეულ ინტერნეტ ობიექტის მოთხოვნებზე მორგებული ფართო ფუნქციონალური შესაძლებლობებით: -გადახდების დაყოვნება-დამუშავება თქვენი ბიზნესის, მოთხოვნებიდან გამომდინარე; - თანხების დაბრუნების ოპერაციები; შესრულებული ოპერაციების სტატუსის შემოწმება; ბიზნეს დღის დახურვის მართვა; -თითეული გადახდის დეტალური იდენტიფიკაცია ობიექტის საბანკო ანგარიშის ამონაწერში. Visa და MasterCard მიერ დანერგილი მაქსიმალურად უსაფრთხო ტექნოლოგია3D-Secure (Verified by Visa, MasterCard SecureCode), რომელიც უზურნველყოფს TBC ბანკიდან ყოველი ტრანზაქციის

დამატებით აუტენტიფიცირებას, ამცირებს თაღლითური გადახდების განხორციელების რისკს და მასთან დაკავშირებულ ფინანსურ დანაკარგებს . TBC ბანკის (http://www.tbcbank.ge/) ინტერნეტ ბანკზე - რეგისტრაციით საშუალება გეძლევათ ისარგებლოთ დისტანციური მოსმახურების მთელი პაკეთით: ინტერნეტბანკი, მობაილ ბანკი და Ipad ბანკი. აღსანიშნავია, რომ ტრანზაქციების ინფორმაცია ერთიპროდუქტიდან მეორეში გადაიცემა მომენტალურად. TBC ბანკის ინტერნეტ ბანკით შესაძლებელია: ანგარიშებზე არსებული ბალანსების ნახვა, ამონაწერის გაკეთება - გადარიცხვა კომპანიის ანგარიშებზე, სხვა პირის ან კომპანიის ანგარიშზე და ბიუჯეტში, კომუნალური გადასახადების გადახდა, დეპოზიტების და სესხების მართვა, ვალუტის კურსების ნახვა და კონვერტაცია - ინტერნეტბანკის მომხმარებლების დამატება და მათთვის უფლებების მინიჭებაკომპანიის მოთხოვნებს მორგებული სერტიფიკაციის მეთოდის დაყენება. E-money (https://www.emoney.ge) - ქართული საგადასახადო სისტემის emoney.ge (www.emoney.ge)მაგალითზე, რომელიც შემოღებულია ბანკი ”ქართუ”-ს მიერ ნაჩვენებია, რომ კორპორაციულ გამყიდველებს, კორპორაციულ მყიდველებს და ინდივიდუალურ მყიდველებს სთავაზობენ რეგისტრაციის სხვადასხვა ვარიანტს და შესაბსამისად ელექტრონული კომერციის სხვადასხვა პროგრამულ საშუალებებს. Emoney არის მულტისავალუტო ელექტრონული საფულე, რომელსაც იყენებს 750,000 ფიზიკური და იურიდიული პირი საქართველოში და მის ფარგლებს გარეთ. EMoney -ს საფულე თავის მომხმარებლებს აძლევს საშუალებას მარტივად, კომფორტულად და რაც მთავარია ზედმეტი დანახარჯების გარეშე იშოპინგონ ინტერნეტში და გადაიხადონ სხვადასხვა პროვაიდერების გადასახადები EMoney -ს ვებ გვერდის მეშვეობით. ლიბერთი ბანკის ანგარიშებსა და ბარათების არსებულ ინფრასტრუქტურაზე დაყრდნობით, EMoney უახლოეს მომავალში ონლაინ გადახდებისა და ინტერნეტ შოპინგის ყველაზე პოპულარული საშუალება გახდება მთელს კავკასიის რეგიონში, რითაც მცირე ბიზნესის წარმომადგენლებისათვის შექმნის გადახდების მიღების ყველაზე ხელსაყრელ და იაფ საშუალებას.

EMoney ელექტრონული საფულის დახმარებით თქვენ შეგიძლიათ შეავსოთ მობილური ტელეფონის ბალანსი, გადაიხადოთ კომუნალური და ასობით სხვა პროვაიდერის გადასახადი დამატებითი საკომისიოს გარეშე.

Emoneyჩაერთო ამიერკავკასიაში პოპულარული, საერთაშორისო პროვაიდერები, რაც ნიშნავს რომ თქვენ უკვე შეგიძლიათ შეავსოთ თქვენი Skype, World of Tanks, Odnoklassniki, WebMoneyდა სხვა ანგარიშები. EmoneyGeorgia-ს ერთერთი აქციონერი არის ლიბერთი ბანკი, რომელიც ემსახურება 1.4 მილიონ კლიენტს 550 მომსახურების წერტილიდან. ეს საშუალებას გვაძლევს კლიენტებს შევთავაზოთ მრავალი სერვისი, რომელიც არის ბანკთან ინტეგრირებული. კლიენტებს შეუძლიათ მარტივად და სწრაფად გაიარონ ვერიფიკაცია ბანკის ქსელში მთელი საქართველოს მასშტაბით. სრულიად უფასოდ შეუკვეთონ PAY მულტისავალუტო ანგარიში და გადააბან იგი თავისEmoney საფულეს.

Emoney სისტემა საშუალებას აძლევს თავის კლიენტებს მარტივად და სწრაფად შეიტანონ და გაანაღდონ თანხა თავისი საფულიდან მრავალი არხის მეშვეობით. Emoney საფულიდან თანხის გატანა შესაძლებელია ლიბერთი ბანკის ქსელიდან: 550 მომსახურე წერტილიდან საქართველოს მასშტაბით, 3113 ბანკომატიდან ელექტრონული პირადობის მეშვეობით. ნებისმიერ ქართულ საბანკო ანგარიშზე, გადარიცხვის გზით. -Emoney საფულეს ბალანსის შევსება შესაძლებელია მარტივად და სწრაფად მრავალი არხიდან. ლიბერთი ბანკის მომსახურების წერტილების ფართო ქსელიდან -ლიბერთი ბანკის ბანკომატებიდან ნებისმიერი ტიპის თვითმომსახურების ტერმინალიდან (NOVA, OSMP, TBC Pay, ExpressPay) -საფულეზე გადაბმული PAY ბარათიდან ნებისმიერი VIZA ან Mastercard ბარათიდან.

Emoney ვერიფიცირებულ კლიენტებს შეუძლიათ უფასოდ შექმნან EMoneyVISA ვირტუალური ბარათი, რაც მათ საშუალებას მისცემს მოხერხებულად იშოპინგონ მსოფლიოს ონლაინ მაღაზიებში, რომლებზეც შესაძლებელია გადახდების მიღება VIZA ბარათების მეშვეობით. ვირტუალური ბარათის შექმნა შესაძლებელია 1 დღიდან 1 წლამდე ვადით

ნებისმიერი რაოდენობით და თქვენთვის სასურველი ლიმიტებით, რაც კიდევ უფრო უსაფრთხოს ხდის ვირტუალური ბარათით სარგებლობას.

Emoney საფულის გამოყენებით, თქვენ შეგიძლიათ:

-ის მომხმარებლები, რომლებიც გაივლიან სწრაფ და კომფორტულ ავტორიზაციის/ვერიფიკაციის პროცესს ლიბერთი ბანკის ფილიალებში, უფასოდ მიიღებენ მულტისავალუტო PAY ბარათებს, რომლის გადაბმაც შესაძლებელია Emoney საფულესთან. ეს არის დამატებითი კომფორტი, რათა კლიენტებმა მარტივად შეავსონ თავიანთი Emoney საფულესაბანკო ანგარიშებიდან; იმ მომხმარებლებს, რომლებსაც Emoney საფულეზე გადაბმული აქვთ PAY ბარათი, შეუძლიათ უფასოდ შექმნან Emoney ვირტუალურიVIZA ბარათი, რომელიც მისცემთ საშუალებას გამოიყენონ ბარათიმსოფლიოს 1000-ზე მეტ ონლაინ მაღაზიაში; - მომხმარებლებს შეუძლიათ სწრაფად და მარტივად შეავსონ საფულის ანგარიში. საქართველოს მოქალაქეებს შეუძლიათ შეავსონ ბალანსი ლიბერთი ბანკისა და კორ სტანდარტ ბანკის ფილიალებში და სერვისცენტრებში, ასევე შესაძლებელია NOVA, OSMP, TBC Pay, ExpressPayთვითმომსახურების აპარატებში; -საფულის მომხმარებლებს შეუძლიათ გადააბან თავიანთი VIZA ან Mastercard ბარათები Emoney-ის საფულეს და სატესტო გადარიცხვით ავტორიზირებულ მომხმარებლებს საშუალება ექნებათ მომავალში ბარათის მონაცემების შეყვანის გარეშე მარტივად და სწრაფად შეავსოთ თავიანთი Emoney საფულის ბალანსი; -Emoney მომხმარებლებს საშუალება აქვთ გამოიყენონ აფულისბალანსი Swoop.ge, Freeshop.ge, MyPhone.ge, eAuction.ge, PAYstore, Mobi.ge, MyVideo.ge,MyMarket.ge, MyAuto.ge, MyHome.ge, MyParts.ge, MyDeal.ge-სა და სხვაელექტრონული კომერციის ლიდერ ვებ გვერდებზე უნიფეი (Unipay) (https://www.unipay.com) ქართულ ონლაინ ბაზარზე ელექტრონული გადარიცხვები სახალიკომპანია „უნიფეი“ შემოვიდა, რომელიც ავითარებს და ნერგავს ელექტრონული გადარიცხვების ა და ელექტრონული კომერციისგადაწყვეტილებებს. ონლაინ სამყარო სულუფრო და უფრო მეტ ადგილს იკავებს თითოეული ადამიანის ყოველდღიურ ცხოვრებაში.

მსოფლიო მასშტაბით ვითარდება ონლაინ მაღაზიები და ელექტრონული კომერცია. კომპანიის მიზანი კი, მომხმარებლის უზრუნველყოფაა მსოფლიო ბაზარზე არსებული ინოვაციური პროდუქტებითა და განვითარებადი ტექნოლოგიური სერვისებით. მთელს მსოფლიოში ისეთი პროდუქტები, როგორიც არის უნიფეი - ელექტრონული საფულე - ძალიან პოპულარულია და მომხმარებლების დიდი რაოდენობით გამოირჩევა. ასეთი სახის მომსახურებებს სთავაზობენ ისეთი გიგანტი კომპანიები, როგორიცაა: “PayPal”, “Alertpay”, “Moneybookers”, “eWay” დასხვა. საინტერესოაისფაქტი, რომ ქართველ მომხმარებელში არის მზარდი მოთხოვნა ანგარიშსწორების წარმოების სრულ ონლაინ რეჟიმზე. ბაზარზე გამოსვლამდე კომპანია უნიფეიმ შეისწავლა მომხმარებლის მოთხოვნები და მზაობა ელექტრონულ საფულესთან მიმართებაში. ამ კვლევების შედეგად გამოიკვეთა ძალიან საინტერესო ტენდენციები და პოტენციური მომხმარებლის მხრიდან იმაზე გაცილებით დიდი დაინტერესება ,ვიდრე ამას კომპანია ელოდა. ამ ყველაფრის გათვალისწინებით, კომპანია უნიფეიმ მიიღო გადაწყვეტილება შეექმნა ერთიანი ონლაინ ანგარიშსწორების სისტემა, რომელიც მომხმარებელს უზრუნველყოფს ზუსტად იმ სერვისით, რომელიც მას სჭირდება. უნიფეის მომხმარებელი იყენებს უსაფრთხო სის ტემას. მკაცრად არის დაცული მომხმარებლის პირადი ინფორმაცია. ასევე მომხმარებლებს სთავაზობს თანამედროვე ტექნოლოგიებ ს მარტივი და იაფი გადარიცხვებისთვის. უნიფეი იცავს მომხმარებლის მონაცემებ სარასანქცირებული წვდომისგან, გამოყენებისგან ან გამჟღავნებისგან. ანგარიშის სისტემა და ყველა ინტერნეტ კომუნიკაცია დაცულია SSL (დაცულისოკეტებისფენა) პროტოკოლის გამოყენებით, რომელსაც გააჩნია უსაფრთხოების მაღალიდონის 256–ბიტიანი სიძლიერის შიფრირების უნარი და სერტიფიცირებულია GeoTrust–ისმიერ. უნიფეი ხელს უწყობს ბიზნესის განვითარებას ინტერნეტში, ონლაინ გაყიდვებისა და ცნობადობის ზრდას კომპანიებისთვის. მხოლოდ ერთი მარტივი ინტეგრაციის საშუალებით ორგანიზაცია უკავშირდება ათიათას ობით შემსყიდველს მსოფლიო მაშტაბით, სადაც ანგარიშსწორება ხდება უსაფრთხო და

მარტივად. კომპანია უნიფეი სთავაზობს კომპანიებს მზა ელექტრონული კომერციის გადაწყვეტილებებს, რაც იმის საშულებას იძლევა, რომ მარტივად და ეფექტურად დაიწყონ ბიზნესის წარმოება ინტერნეტში ახლად დაარსებულმა მცირე კომპანიებმაც კი. უნიფეის თანთანამშრომლობა უპირველესად ნიშნავს სწრაფ გადახდებს, მაქსიმალურუსაფრთხოებას, ფართო დაფარვის ზონასა და მის ქსელში ჩართული კომპანიების შემოსავლების ზრდას. შპს „უნიფეი“ ონლაინ ანგარიშსწორების სისტემაა, რომელიც საშუალებას გაძლევთ გააგზავნოთ, გადაიხადოთ და მიიღოთ თანხა ინტერნეტში, ყველაზესწრაფად, მარტივადდაუსაფრთხოდ. პირადი ელექტორნული საფულე ანგარიშსწორების ყველაზე თანამედროვე, უსაფრთხო და მოსახერხებელი მეთოდია, რომელიც არა მხოლოდ ამარტივებს მყიდველსა და გამყიდველს შორის ფინანსურ ურთიერთობას, არამედ ორივე მხარეს სთავაზობს ფულადი ოპერაციების განხორციელებისათვის უამრავ დამატებით ფუნქციას.ელექტრონული ფული და ელექტრონული საგადამხდელოსისტემები - ეს ორი ერთმანეთთან მჭიდროდ დაკავშირებულიცნებებია.მეორე მხრივ საგადამხდელო სისტემებს ოპერირება შეუძლიათარა მარტო ელექტრონული ფულით, არამედ შეუძლიათ განახორციელონჩვეულებრივი უნაღდო გადახდები და ოპერირება ნაღდსაშუალებებთან. დღესდღეობით არ არსებობს ელექტრონული ფული, რომელიცმოქმედებს ერთზე მეტ საგადამხდელო სისტემაში, მაგრამთეორიულად ასეთი მოვლენა სავსებით შესაძლებელია. ყველაურთიერთანგარიშსწორება საგადამხდელო სისტემებს შორის, იმშემთხვევაშიც კი როცა ერთი ელექტრონული ფული იცვლებასხვა ელექტრონულ ფულზე ხორციელდება ჩვეულებრივი უნაღდოგადახდების სახით. უნაღდო ანგარიშსწორების ოპერაციებს საგადამხდელოსისტემებში უწოდებენ ტრანზაქციებს. ტრანზაქცია (ინგლისურისიტყვა - transaction წარმოქმნილია ლათინური სიტყვიდან -transactio `შესრულება~) - თანმიმდევრული ოპერაციების ჯგუფი,რომლებიც თავისთავად წარმოადგენენ მონაცემებთან მუშაობისლოგიკურ ერთეულს.

საგადამხდელო სისტემები უზრუნველყოფენ სხვადასხვასახის ტრანზაქციებს: ბანკის განყოფილებებში ნაღდი ფულისყიდვა და გამოტანა, ბანკომატიდან ნაღდი ფულის გამოტანა,კლიენტის ანგარიშზე არსებული ნაშთის შესახებ ინფორმაციისმიღება და სხვა. ტრანზაქციები განსხვავდებიან აგრეთვე საგადამხდელოსისტემაში ბარათის შესახებ ინფორმაციის წარდგენის მეთოდით.არსებობენ ელექტრონული ტრანზაქციები (ბარათის შესახებინფორმაცია იკითხება მაგნიტური ზოლიდან/ჩიპიდან) და ხმოვანიავტორიზაციის ტრანზაქციები (paper based). CNP - ტრანზაქცია (Cardholder Not Present) წარმოადგენსპლასტიკური ბარათის მეშვეობით ყიდვის ოპერაციას, რომლისგანხორციელების მომენტში კლიენტი პირადად არ იმყოფებასავაჭრო წერტილში, ხოლო ავტორიზაციისათვის საჭირო თავისიბარათის რეკვიზიტებს (ბარათის ნომერი, მოქმედების ვადა)დაუსწრებლად ატყობინებს სავაჭრო წერტილს (წერილი, ფაქსი,მონაცემთა გადაცემის ქსელები და სხვა).

ელექტრონული საგადამხდელო სისტემის ტექნოლოგიურიბირთვია საპროცესინგო ცენტრი. ის წარმოადგენს სპეციალიზირებულგამოთვლით ცენტრს, რომელიც ფუნქციონირებს განსაკუთრებულპირობებში და გარანტირებულად დროის რეალურრეჟიმში ამუშავებს ტრანზაქციების ინტენსიურ ნაკადს. მართლაც სადებეტო ბარათის გამოყენება განაპირობებს ყოველი ბარათის“ონლაინ” ავტორიზაციის აუცილებლობობას საგადამხდელო სისტემის მომსახურეობის ნებისმიერ წერტილში. საკრედიტობარათებთან ოპერაციების დროს კი ავტორიზაცია ყოველთვისარ არის აუცილებელი, მაგრამ მაგალითად ბანკომატებში ფულისმიღების დროს ავტორიზაცია ყოველთვის ტარდება.

1.4. არსებული სტანდარტების განხილვა ელექტრონული ანგარიშსწორების სისტემისა და ორგანიზაციული სტრუქტურის მიმართულებით

ინფორმაციული უსაფრთხოების მიზანია ყველა სახის და წარმომავლობის ინფორმაციის დაცვა. ეს ინფორმაცია შეიძლება ინახებოდეს როგორც ქაღალდზე, ასევე კომპიუტერულ სისტემებში, ან თუნდაც მომხმარებელთა გონებაში. IT-უსაფრთხოება დაკავებულია პირველ რიგში ელექტრონულად შენახული ინფორმაციის უსაფრთხოებაზე და მის დამუშავებაზე.

ინფორმაციული უსაფრთხოების კლასიკური საბაზო ფასეულობებია კონფიდენციალობა, მთლიანობა და წვდომა. ბევრი მომხმარებელი თავიანთ წამოდგენებში განიხილავენ ასევე სხვა ფასეულობებსაც. ეს შეიძლება სასარგებლოც იყოს ინდივიდუალური აპლიკაციების თვალსაზრისით ინფორმაციული უსაფრთხოების სხვა გენერირებული ზოგადი ტერმინებია, მაგალითად, აუთენთიციტეტი, პასუხისმგებლობა, საიმედოობა და უმტყუნობა. ინფორმაციის უსაფრთხოებას ემუქრება არა მხოლოდ განზრახ ქმედებები (მაგალითად, კომპიუტერული ვირუსები, ინფორმაციის წართმევა/მოსმენა, კომპიუტერის ქურდობა). შემდეგი მაგალითები იძლევა ამის ილუსტრაციას:

- დაუძლეველი ძალის მიერ (როგორიცაა ცეცხლი, წყალი, ქარიშხალი, მიწისძვრა) მედია–მატარებლები და IT-სისტემები დაზარალებულია ან ჩაშლილია ხელმისაწვდომობა მონაცემთა ცენტრში. დოკუმენტები, IT-სისტემები ან სამსახურები აღარაა სურვილისამებრ ხელმისაწვდომები;
- მას შემდეგ, რაც მოხდა წარუმატებელი პროგრამული განახლება, აპლიკაციები აღარ ფუნქციონირებს ან მონაცემები შეუმჩნევლად შეიცვალა;
- მნიშვნელოვანი ბიზნეს პროცესი ჭიანურდება, რადგან ერთადერთი ადამიანი, ვინც იცნობს პროგრამებს, ავადაა;
- კონფიდენციალური ინფორმაცია შემთხვევით გადაეცა არასანქცირებული პირს, რადგან დოკუმენტები ან ფაილი არ იყო მონიშნული, როგორც „საიდუმლო". გერმანულენოვან ლიტერატურაში ტერმინები „საინფორმაციო ტექნოლოგიები", „საინფორმაციო და საკომუნიკაციო ტექნოლოგიები" ან „საინფორმაციო და სატელეკომუნიკაციო ტექნოლოგიები" ხშირად გამოიყენება როგორც სინონიმები.

ამ ტერმინების სხვადასხვა სიგრძეების გამო, მიღებულია შესაბამისი შემოკლებების გამოყენება. ვინაიდან ინფორმაციის ელექტრონული დამუშავება გავრცელებულია ცხოვრების თითქმის ყველა სფეროში, აღარ აქვს მნიშვნელობა განსხვავებას, ინფორმაცია მუშავდება ინფორმაციული ტექნოლოგით, საკომუნიკაციო ტექნოლოგიით თუ ქაღალდზე.

ტერმინი საინფორმაციო უსაფრთხოება, ნაცვლად IT უსაფრთხოებისა, ყოვლისმომცველია და ამიტომ უფრო შესაფერისი. თუმცა, ლიტერატურაში გამოიყენება ძირითადად ტერმინი „IT უსაფრთხოება" (რადგან ეს მოკლეა).

წინამდებარე ნაშრომშიც იქნება გამოყენებული ეს ტერმინი, ან შესაბამისი ტერმინი „IT საბაზო დაცვა“. ინფორმაციული უსაფრთხოების სფერში სხვადასხვა სტანდარტები შემუშავდა, რომლებშიც ნაწილობრივ სხვადასხა მიზნობრივი ჯგუფები ან თემატური სფეროები არის წინა პლანზე წამოწეული. უსაფრთხოების სტანდარტების გამოყენება ბიზნესში ან ხელისუფლებაში არა მხოლოდ აუმჯობესებს უსაფრთხოების დონეს, ის ასევე ხელს უწყობს სხვადასხვა დაწესებულებებს შორის კოორდინაციას, რომლებშიც უსაფრთხოების ზომები უნდა განხორციელდეს ნებისმიერი ფორმით. ქვემოთ, შემდეგი მიმოხილვა გვიჩვენებს ყველაზე მნიშვნელოვანი სტანდარტების მიმართულებებს. ISO და IEC საერთაშორისო ნორმების ორგანიზაციებში გადწყდა, რომ ინფორმაციული

ეს სტანდარტი იძლევა ზოგად მიმოხილვას ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემების (ISMS) და მათი ურთიერთდამოკიდებულების შესახებ ISO 2700 x –ოჯახის სხვადასხვა სტანდარტებს შორის. აქვე გადმოცემულია ISMS–ის ძირითადი პრინციპები, კონცეფციები, ტერმინები და განსაზღვრებანი. ISO 27001 საინფორმაციო ტექნოლოგიების სირთულისა და სერთიფიკატებზე მოთხოვნების გამო მრავალი ინსტრუქცია, სტანდარტი და ინფორმაციული უსაფრთხოების ეროვნული სტანდარტები წარმოიშვა ბოლო წლებში. სტანდარტი ISO 27001 – "ინფორმაციული ტექნოლოგია - უსაფრთხოების ტექნიკა - ინფორმაციული უსაფრთხოების მართვის სისტემის მოთხოვნების სპეციფიკაცია" არის პირველი საერთაშორისო სტანდარტი ინფორმაციული

უსაფრთხოების მართვაში, რომელიც ასევე სერტიფიცირების საშუალებას იძლევა. ISO 27001 იძლევა 10 გვერდიან ზოგად რეკომენდაციებს, მათ შორის შესავლის (დანერგვის), ექსპლუატაციის და დოკუმენტირებული ინფორმაციის უსაფრთხოების მართვის სისტემის სრულყოფისთვის, ასევე რისკების გათვალისწინებით. ნორმატიულ დანართში მოხსენიებულია კონტროლი ISO / IEC 27002 –დან. თუმცა, მკითხველი არ იღებს დახმარებას პრაქტიკული განხორციელებისთვის. უსაფრთხოების სტანდარტები გაერთიანებულიყო 2700x სერიაში, რომელიც მუდმივად იზრდება. მნიშვნელოვანი სტანდარტებია: ISO 27002–ის (ყოფილი ISO 17799:2005) "ინფორმაციული ტექნოლოგიები - ინფორმაციული უსაფრთხოების მენეჯმენტის საპროცესო კოდექსი" მიზანია ინფორმაციული უსაფრთხოების მენეჯმენტის ჩარჩოს განსაზღვრა. ამიტომაც ISO 27002 პირველ რიგში ეხება აუცილებელ ბიჯებს (ეტაპებს), ფუნქციონირებადი უსაფრთხოების მენეჯმენტის ასაგებად და ორგანიზაციაში მიმაგრებას. აუცილებელი უსაფრთხოების ზომები მოკლედაა აღწერილი ISO-სტანდარტის ISO/IEC 27002–ში, დაახლოებით 100 გვერდზე. რეკომენდაციები, რომელიც განკუთვნილია მართვის დონისთვის და, შესაბამისად, შეიცავს მცირე კონკრეტულ ტექნიკურ შენიშვნებს. უსაფრთხოების ISO 27002–ის რეკომენდაციების რეალიზაცია არის ერთ–ერთი გზა მრავალი შესაძლებლობიდან, რომლებიც აკმაყოფილებს ISO სტანდარტის 27001–ის მოთხოვნებს.

ISO 17799 სტანდარტი 2007 წლის დასაწყისში გადაეცა არსებითი ცვლილებების გარეშე ISO 27002–ს, იმისათვის, რომ ხაზი გაესვათ მის მიკუთვნებაზე ISO 2700x სერიისთვის.

ISO-27005–სტანდარტი „ინფორმაციული უსაფრთხოების რისკების მენეჯმენტი“ შეიცავს ძრითად რეკომენდაციებს რისკების მართვის შესახებ ინფორმაციული უსაფრთხოებისთვის. მათ შორის იგი მხარს უჭერს ISO/IEC 27001 სტანდარტის მოთხოვნების რეალიზაციას. ოღონდ აქ არავითარი მეთოდი რისკების მართვისთვის არაა მოცემული. ISO/IEC 27005 ცვლის ISO 13335-2 სტანდარტს. ეს სტანდარტი ISO 13335-2 „უსაფრთხოების

ინფორმაციულ–კომუნიკაციური ტექნოლოგიები, ნაწ.2: რისკების მენეჯმენტის მეთოდები ინფორმაციულ უსაფრთხოებაში“, იძლეოდა ინსტრუქციებს ინფორმაციული უსაფრთხოების მენეჯმენტისთვის

ISO-სტანდარტი 27006 „ინფორმაციული ტექნოლოგია – უსაფრთხოების უზრუნველყოფის მეთოდები – მოთხოვნები სერტიფიცირების აკრედიტაციული ორგანოების მიმართ ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემებში“, განსაზღვრავს აკრედიტაციის მოთხოვნებს სერტიფიცირების ორგანოებისთვის ISMS–ში და განიხილება ამ სერტიფიცირების პროცესების თავისებურებანი. ISO-2700x- რიგის სხვა სტანდარტები ISO 2700x სტანდარტული სერია სავარაუდოდ გრძელვადიან პერსპექტივაში ISO სტანდარტების 27000-27019 27030-27044 სახით დაკომპლექტდება. ამ სერიის ყველა სტანდარტი მოიცავს უსაფრთხოების მართვის სხვადასხვა ასპექტებს და ეფუძნება ISO 27001–მოთხოვნებს. სხვა სტანდარტების მიზანია გააუმჯობესოს გაგება და პრაქტიკული გამოყენების ISO 27001–ის. ეს შეთანხმებაა, მაგალითად, ISO 27001–ის პრაქტიკული განხორციელებისთვის, ანუ რისკების შეფასება ან რისკების მართვის მეთოდებია. BSI–ის ყველაზე ცნობილი გამოცემა ინფორმაციულ უსაფრთხოებაში იყო 2005 წლამდე IT–საბაზო დაცვის სახელმძღვანელო, რომელშიც 1994 წლიდან აღწერილი იყო დეტალურად არა მხოლოდ ინფორმაციული უსაფრთხოების მენეჯმენტის, არამედ დეტალური უსაფრთხოების ზომები ტექნოლოგიის, ორგანიზაციის, პერსონალის და ინფრასტრუქტურის სფეროებში [29-32]. IT საბაზო დაცვის სახელმძღვანელო 2005–ში არა მარტო განახლდა, არამედ რესტრუქტურიზებაც განიცადა. ამასთანავე IT–საბაზო–დაცვის და IT–საბაზო–დაცვის–კატალოგების პროცესების აღწერა გამოეყო ერთმანეთს IT–საბაზო–დაცვის–კატალოგები აგებულია მოდულარულად და შეიცავს ტიპური პროცესების, პროგრამების და IT–კომპონენტების სამშენებლო ბლოკებს (მოდულებს). თითოეული თემისთვის რეკომენდებულია არა მხოლოდ უსაფრთხოების ზომების დასახელებები, არამედ აგრეთვე აღიწერება მნიშვნელოვანი (ძირითადი საფრთხეები) რისკებიც,

რომელთაგანაც უნდა დაიცვას თავი დაწესებულებამ. მომხმარებლებს შეუძლიათ ამით ფოკუსირება კონკრეტულად სამშენებლო ბლოკებზე, რომლებიც ფაქტობრივად, შეესაბამება მათი სფეროებს.

IT–საბაზო–დაცვის–კატალოგების სამშენებლო ბლოკები რეგულარულად აქტუალიზდება და ფართოვდება, ახალი ტექნიკური განვითარების გათვალისწინებით. ამიტომაც ისინი პუბლიცირდება როგორც თავისუფალი ფურცლების კოლექცია, CD/DVD-ის სახით და ამასგარდა ინტერნეტშიც.

IT–საბაზო–დაცვის–მეთოდები აღწერს, თუ როგორ შეირჩევა სტანდარტული–უსაფრთხოების ზომებით უსაფრთხოების გადაწყვეტები, როგორ აიგება და გამოიცდება. ეს მეთოდები გამოქვეყნებულია როგორც BSI-Standard 100-2 სტანდარტი ინფორმაციული უსაფრთხოებისთვის.

100-1 ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემები **(ISMS)** ეს სტანდარტი განსაზღვრავს ISMS–ის ზოგად მოთხოვნებს. ეს არის სრულად თავსებადი ISO სტანდარტის 27001 და კვლავაც გაითვალისწინებს რეკომენდაციებს ISO სტანდარტების 27000 და 27002. იგი სთავაზობს მკითხველს ადვილად გასაგებ და სისტემატურ ინსტრუქციებს, მიუხედავად იმისა, თუ რომელი მეთოდის საშუალებით სურთ მათ მოთხოვნების განახორციელება.

BSI წარმოადგენს ISO სტანდარტის შინაარსს საკუთარ BSI სტანდარტში, გარკვეული საკითხების უფრო დეტალურად აღსაწერად, და ამით შინაარსის დიდაქტიკური წარმოდგენის საშუალება მიეცეს. გარდა ამისა, სტრუქტურა იყო ისე დამუშავებული, რომ იგი თავსებადია IT-საბაზო დაცვის მეთოდებთან. უნიფიცირებული სათაურების საშუალებით აღნიშნულ დოკუმენტებში მკითხველისთვის ძალიან მარტივია ორიენტაირება. **100-2 IT-**საბაზო დაცვა–მეთოდკა IT–საბაზო–დაცვა–მეთოდიკა აღწერს ეტაპობრივად, ნაბიჯ–ნაბიჯ, თუ როგორ უნდა აიგოს ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემა პრაქტიკულად და როგორ მოხდეს მისი ექსპლუატაცია. ინფორმაციული უსაფრთხოების მენეჯმენტის ამოცანები და ორგანიზაციული სტრუქტურის აგება

ინფორმაციული უსაფრთხოებისთვის ძალზე მნიშვნელოვანი თემებია. IT–საბაზო–დაცვა–მეთოდიკა დეტალურად განიხილავს იმას, თუ როგორ შეიძლება უსაფრთხოების კონცეფციის (პოლიტიკის) დამუშავება პრაქტიკაში, როგორ აირჩევა შესაბამისი უსაფრთხოების ზომები და რა შეიძლება ჩაითვალოს უსაფრთხოების კონცეფციის რეალიზაციად. ასევე საკითხი, როგორ ხდება ინფორმაციული უსაფრთხოების მხარდაჭერა და სრულყოფა ექსპლუატაციის პირობებში, არის ამომწურავად პასუხგაცემული.

IT–საბაზო–დაცვა BSI-Standard 100-2 სტანდარტთან კავშირში, ახდენს აქამდე დასახელებული 27000, 27001 და 27002 ISO-სტანდარტების ძალზე ზოგადად მიღებული მოთხოვნების ინტერპრეტირებას და ეხმარება მომხმარებლებს პრაქტიკაში რეალიზაციის დროს, მრავალი შენიშვნით, საცნობარო ინფორმაციით და მაგალითით.

IT–საბაზო–დაცვის–კატალოგები ხსნიან არა მხოლოდ იმას, თუ რა უნდა გაკეთდეს, არამედ იძლევა ძალიან კონკრეტულ შენიშვნას, თუ როგორ უნდა გამოიყურებოდეს რეალიზაცია (ასევე ტექნიკურ დონეზე). პროცესი IT–საბაზო–დაცვის მიხედვით არის აპრობირებული და ეფექტური შესაძლებლობა, ზემოჩამოთვლილ ISO-სტანდარტის ყველა მოთხოვნის შესასრულებლად. **100-3** რისკების ანალიზი IT–საბაზო–დაცვის საფუძველზე BSI–მ დაამუშავა რისკების ანალიზის მეთოდიკა IT–საბაზო–დაცვის საფუძველზე. მის გამოყენებას აზრი აქვს მაშინ, როცა კომპანიები ან სახელმწიფო დაწესებულებები მუშაობენ წარმატებით IT–საბაზო–დაცვასთან და უჩნდებათ სურვილი დამატებითი უსაფრთხოების ანალიზის ჩასატარებლად, საგანგებო სიტუაციათა მენეჯმენტი BSI Standard 100-4 სტანდარტში ახსნილია სახელმწიფო დაწესებულებათა ან კომპანიების მასშტაბებში საგანგებო სიტუაციათა მენეჯმენტის აგების და ექსპლუატაციის მეთოდიკა. აქ აღწერილი მეთოდიკა ეფუძნება BSI-Standard 100-2 სტანდარტის IT–საბაზო–დაცვის–მეთოდიკას და აფართოვებს მას სასარგებლოდ. **ISO 27001** სერტიფიცირება IT–საბაზო–დაცვის საფუძველზე BSI ახდენს საინფორმაციო ქსელების სერტიფიცირებას, ანუ

ინფრასტრუქტურული, ორგანიზაციული, პერსონალური და ტექნიკურიმ კომპონენტების ურთიერთმოქმედებას, რომლებიც გამოიყენება ბიზნეს–პროცესების და ტაქნიკური დავალებების სარეალიზაციოდ. BSI სერტიფიცირება მოიცავს როგორც გამოცდას ინფორმაციული უსაფრთხოების მენეჯმენტის სისტემებში, ასევე გამოცდას კონკრეტულ უსაფრთხოებიზ ზომებში IT–საბაზო–დაცვის საფუძველზე.

BSI სერტიფიცირება ამასთანავე ყოველთვის მოიცავს ოფიციალურ ISO–სერტიფიცირებას ISO 27001–ის მიხედვით, მაგრამ ბევრად მნიშვნელოვანია, ვიდრე უბრალოდ ISO–სერტიფიცირება, დამატებითი კვლევით–ტექნიკური ასპექტების გამო. უსაფრთხოების მენეჯმენტის გამოცდის ძირითადი მოთხოვნები აუდიტის ჩარჩოებში (კონტექსტში) აღმოცენდება უსაფრთხოების მენეჯმენტის საბაზო დაცვის ბლოკის (B 1.0) ღონისძიებებიდან. ამ ბლოკის ეს ზომები ისეა დაწერილი, რომ ISMS-ის BSI–სტანდარტის მნიშვნელოვანი მოთხოვნები სწრაფად იყოს იდენტიფიცირებული (განსაზღრული). 1იძლევა BSI–დოკუმენტების ზოგადი სტრუქტურის ილუსტრაციას. ISO 27001 სტანდარტთან ადაპტირებისათვის ჩატარდა კორექტირებები სერტიფიცირების სქემაში ინფორმაციული.

COBIT (Control Objectives for Information and related Technology – კონტროლის მიზნები ინფორმაციული და დაკავშირებული ტექნოლოგიებისთვის) აღწერს რისკების კონტროლის მეთოდს, რომელიც ხორციელდება IT–დანერგვის საშუალებით კრიტიკული ბიზნეს–პროცესების შესრულების მხარდასაჭერად [4]. COBIT–დოკუმენტები გაიცემა საინფორმაციო სისტემების აუდიტის და კონტროლის ასოციაციის (ISACA– Information Systems Audit and Control Association) IT მართვის ინსტიტუტის (ITGI – IT Governance Institute) მიერ. COBIT–ის დამუშავების დროს ავტორები ორიენტირებულნი იყვნენ უსაფრთხოების მენეჯმენტის არსებულ სტანდარტებზე, როგორიცაა ISO 27002.

IT Infrastructure Library (ITIL – IT ინფრასტრუქტურის ბიბლიოთეკა) არის IT სერვის მენეჯმენტის რამდენიმე წიგნის კოლექცია [3]. იგი

შემუშავებულ იქნა გაერთიანებული სამეფოს სახელმწიფო კომერციის მთავრობის მიერ (OGC). ITIL განიხილავს IT–სერვისების მენეჯმენტს IT–მომსახურების თალსაზრისით. IT–მომსახურება შეიძლება იყოს როგორც შიგა IT–დეპარტამენტის ან გარე სერვისის პროვაიდერის. საერთო მიზანი არის ოპტიმიზაცია და ხარისხის გაუმჯობესების IT მომსახურების და ხარჯების ეფექტურობის.

ITIL ბიბლიოთეკა და და COBIT სტანდარტი განხილულ იქნება წიგნის მომდვნო თავებში.

სახელმწიფო დაწესებულებას და ყოველ კომპანიას აქვს მენეჯმენტი, რომელიც შემდგომში მოხსენიებულ იქნება როგორც „ხელმძღვანელობის დონე“, თუ პასუხისმგებელად ხელმძღვანელი ძალაა მოაზრებული და უწესრიგობის რისკი „მენეჯმენტზე“ არსებობს, როგორც მართვის პროცესზე (Leiten-ხელმძღვანელობა, Lenken-გაძღოლა და Planen - დაგეგმვა) [29]. მენეჯმენტის სისტემა მოიცავს ყველა წესს, რომლებიც ორგანიზაციის მიზნის მიღწევისთვის კონტროლზე და მართვაზე ზრუნავს. მენეჯმენტის სისტემის ნაწილი, რომელიც დაკავებიულია ინფორმაციული უსაფრთხოებით, ISMS უწოდებენ.

ISMS ამტკიცებს, თუ რომელი ინსტრუმენტებით და მეთოდებით მართავს (გეგმავს, ნერგავს, ასრულებს, აკონტროლებს და სრულყოფს) მენეჯმენტი ინფორმაციულ უსაფრთხოებაზე მიმართულ ამოცანებს და ქმედებებს მიზანმიმართულად. ISMS–ს მიეკუთვნება შემდეგი ძირითადი კომპონენტები (ნახ.2):

მენეჯმენტის პრინციპები;

 რესურსები;

 თანამშრომლები;

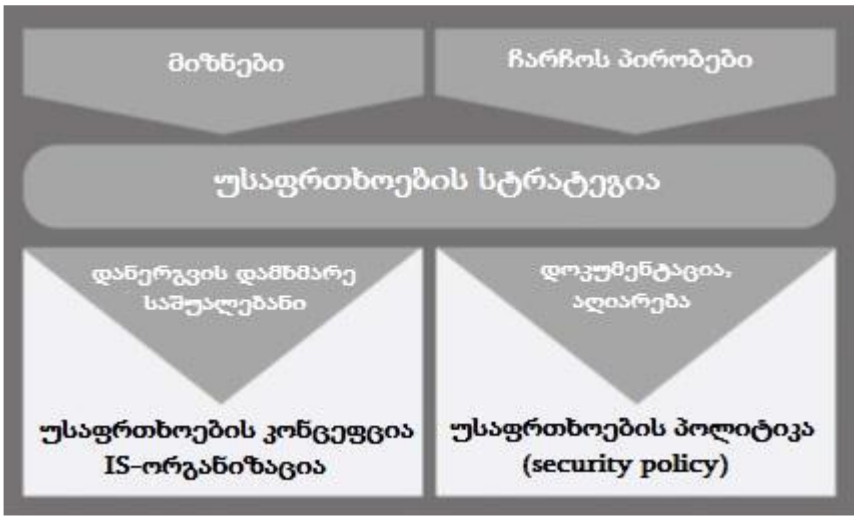
 უსაფრთხოების პროცესი;

 ხელმძღვანელობა ინფორმაციული უსაფრთხოებისათვის, რომელშიც უსაფრთხოების მიზნები და სტრატეგია მისი რეალიზაციისთვის დოკუმენტირებულია;

 უსაფრთხოების კონცეფცია (პოლიტიკა);

 ინფორმაციული უსაფრთხოების ორგანიზაცია.

ინფორმაციული უსაფრთხოების ორგანიზაცია და უსაფრთხოების კონცეფცია არის მენეჯმენტის ინსტრუმენტი მისი უსაფრთხოების სტრატეგიის დასანერგად. მე–3 და მე–4 ნახაზები ამ დამოკიდებულებას ნათელს ჰფენს.



უსაფრთხოების სტრატეგიის ძირითადი პუნქტები დოკუმენტირებულ იქნება სახელმძღვანელო პრინციპებში ინფორმაციის უსაფრთხოებისათვის. უსაფრთხოების პოლიტიკას ცენტრალური მნიშვნელობა აქვს, რადგან იგი შეიცავს ხელმძღვანელობის ხილულ აღიარებას მათი სტრატეგიის შესახებ.
სასიცოცხლო ციკლი ინფორმაციულ უსაფრთხოებაში
უსაფრთხოება არ არის უცვლელი მდგომარეობა, რომელიც მიიღწევა ერთხელ და არასდროს იცვლება შემდეგ. ყოველი დაწესებულება ექვემდებარება მუდმივ დინამიურ ცვლილებებს ბევრი ეს ცვლილება დაკავშირებულია ბიზნეს–პროცესების, სპეციალიზებული ამოცანების, ინფრასტრუქტურის, ორგანიზაციული სტრუქტურების IT–ის და საინფორმაციო უსაფრთხოების ცვლილებებთან.

შესამჩნევ ცვლილებებთან ერთად დაწესებულების ფარგლებში ასევე იცვლება გარე პირობები, როგორიცაა სამართლებრივი ან ხელშეკრულებით გათვალისწინებული მოთხოვნები, აგრეთვე არსებული ინფორმაციის ან საკომუნიკაციო ტექნოლოგიებიც შეიძლება შეიცვალოს რადიკალურად. აქედან გამომდინარე, აუცილებელია უსაფრთხოების აქტიური მართვა, რათა შენარჩუნებულ იქნას უსაფრთხოების მიღწეული დონე. არ არის საკმარისი, მაგალითად, რომ ბიზნეს–პროცესების დაგეგმვა ან ახალი IT-სისტემის დანერგვა და მიღებული უსაფრთხოების ზომები განხორციელდს მხოლოდ ერთხელ. უსაფრთხოების ზომების განხორციელების შემდეგ ისინი რეგულარულად უნდა იყოს გამოკვლეული ეფექტურობასა და

მიზანშეწონილობაზე, ასევე მათ გამოყენებადობასა და ფაქტობრივ გამოყენებაზე. უნდა მოიძებნოს სუსტი წერტილები ან გაუმჯობესების შესაძლებლობები, უნდა მოხდეს ღონისძიებათა ადაპტირება და გაუმჯობესება.

ეს ადაპტაციის საჭიროებით მოითხოვნილი ცვლილებები უნდა იყოს თავიდან დაგეგმილი და განხორციელებული. თუ ბიზნეს–პროცესები მთავრდება ან კომპონენტები ან IT–სისტემები იცვლება, ან ამოიღება მომსახურებიდან, მაშინ არსებული უსაფრთხოების ასპექტები უნდა გადაიხედოს (მაგალითად, პრივილეგიების ამოღება ან მყარი დისკების უსაფრთხო წაშალა). IT-საბაზო–დაცვის კატალოგებში უსაფრთხოების ზომები გადანაწილდება მკითხველის უკეთესი სიცხადისთვის შემდეგ ფაზებში: დაგეგმვა და კონცეფცია; შესყიდვა (საჭიროების შემთხვევაში); დანერგვა; ექსპლუატაცია (ზომები ქსპლუატაციაში ინფორმაციის უსაფრთხოების მხარდასაჭერად მოიცავს მონიტორინგს და შდეგების ონტროლს); გამოყოფა (საჭიროების შემთხვევაში) და საგანგებო სიტუაციებისადმი მზადყოფნა.

მოცემულია ახალი მიდგომა ელექტრონული გადახდის სისტემებში უსაფრთხოების საკითხების გადასაჭრელად, რომელიც დაფუძნებულია არსებული სტანდარტების გამოყენებასა და გაუმჯობესებაზე.

1.5. ამოცანის დასმა

ზემოთ თქმულიდან გამომდინარე, საბარათე და ელექტრონული ანგარიშსწორების სისტემა არის ფართო სფერო მისი უწყვეტი ფუნქციონირება საკმაოდ დიდ რესურსებთან არის დაკავშირებული რაც რიგ შემთხვევევებში აისახება მისსავე უსაფრთხოებაზე

ამრიგად, საბარათე დაცვის სისტემების პრობლემატიკაში

აუცილებელია შემდეგი ამოცანების გადაწყვეტა:

1. პაროლის ფორმირების სისტემის შემუშავება
2. ალტერნატიული მონაცემთა ბაზების ფორმირება
3. დაშიფრვის ალტერნატიული მეთოდიკის შემუშავება

პირველი თავის დასკვნები

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

თავი II. ელექტრონული ანგარიშსწორების სისტემისათვის ინფრასტრუქტურის აგება

ელექტრონული ანგარიშსწორების სისტემის მნიშვნელობა საქართველოს მოსახლეობისთვის ნაკლებად არის ცნობილი. მოსახლეობის ნაწილისთვის ის მხოლოდ გადასახადებთან ასოცირდება, რაც მცდარი წარმოდგენაა ამ სფეროზე. ჩემი მიზანია, არსებული ნაშრომით საშუალებით ავუხსნა დაინტერესებული მხარეებს რიგით მკითხველს რა არის ელექტრონული ანგარიშსწორების სისტემა რა სახის ინფრასტრუქტურა მისი უსაფრთხოთ ფუნქიონირებისათვის საჭირო და როგორ უნდა განხორციელდეს მისი შერჩევა დანერგვა და ექსპლუატაცია.

2.1. ქსელის ინფრასტრუქტურის მოწყობა

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; ურ.1.2. 1 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. ლოკალური ქსელები შეიძლება შედიოდეს რეგიონულ ქსელებში კომპონენტების სახით; რეგიონალური ქსელები - გაერთიანდნენ გლობალური ქსელის შემადგენლობაში; გლობალურმა ქსელებმა შეიძლება შექმნან უფრო მსხვილი სტრუქტურები. პლანეტა დედამიწის მასშტაბით დღეისათვის კომპიუტერული ქსელების ყველაზე დიდი გაერთიანებაა ’’ქსელთა ქსელი’’ - ინტერნეტი. გლობალური, რეგიონალური და ლოკალური ქსელების გაერთიანება იძლევა მრავალდონიანი იერარქიების შექმნის საშუალებას, რომლებიც თავის მხრივ იძლევა მონაცემთა უზარმაზარი მასივების დამუშავებისა და ინფორმაციული რესურსებისადმი პრაქტიკულად შეუზღუდავი ხელმისაწვდომობის მძლავრ საშუალებებს ლოკალური და გლობალური ქსელების გაერთიანების საინტერესო მაგალითია

ვირტუალური კერძო ქსელი (Virtual Private Network, VPN). ასე ეწოდება ორგანიზაციის ქსელს, რომელიც მიიღება ორი ან რამოდენიმე ტერიტორიულად განცალკევებული ლოკალური ქსელის გაერთიანებით საყოველთაოდ ხელმისაწვდომი გლობალური ქსელების არხების დახმარებით, მაგალითად, ინტერნეტით. ქსელური მოწყობილობები ურთიერთდაკავშირებულნი არიან სხვადასხვა ტიპის კავშირის საშუალებებით: – სპილენძის კაბელებით - მოწყობილობებს შორის მონაცემთა გადასაცემათ იყენებს დენის სიგნალს. – ოპტიკურ-ბოჭკოვანი კაბელებით - იყენებს შუშას და პლასტმასის სადენს, ე.წ. ბოჭკოვანს, რათა გადასცეს სინათლის სხივის იმპულსების მეშვეობით ინფორმაცია. – უკაბელო კავშირი - იყენებს რადიო სიგნალებს, ინფრაწითელ ტექნოლოგიას (ლაზერებს), ან სატელიტურ კავშირებს. ინფორმაციის გადაცემის სიჩქარის მიხედვით ქსელები შეიძლება დავყოთ დაბალი, საშუალო, და მაღალი სიჩქარის ქსელებად ერთრანგიანი ქსელები - ერთრანგიან ქსელში ყველა კომპიუტერი თანასწორუფლებიანია. ყოველ მათგანს შეუძლია შეასრულოს როგორც სერვერის როლი, ე. ი. მიაწოდოს ფაილები და აპარატურული რესურსები (დამგროვებლები, პრინტერები და სხვა) დანარჩენ კომპიუტერებს, ასევე კლიენტის როლი, რომელიც სარგებლობს სხვა კომპიუტერების რესურსე ქსელები გამოყოფილი სერვერით (’’კლიენტ-სერვერ’’ ტიპის ქსელები) - ასეთ ქსელებში ხდება ერთი ან რამოდენიმე კომპიუტერის გამოყოფა - სერვერების სახით, რომელთა ამოცანაც მდგომარეობს სხვა კომპიუტერების - კლიენტების მრავალრიცხოვანი მოთხოვნების სწრაფ და ეფექტურ დამუშავებაში. ამავე დროს კლიენტური მოთხოვნები შეიძლება იყოს სრულიად განსხვავებული, დაწყებული უმარტივესით - სისტემაში შესვლისას მომხმარებლის სახელის და პაროლის შემოწმებით, დამთავრებული მონაცემთა ბაზებისადმი რთული საძიებო მოთხოვნებით. სერვერი - სპეციალურად გამოყოფილი მაღალმწარმოებლური კომპიუტერი, აღჭურვილი შესაბამისი სერვერული პროგრამული უზრუნველყოფით, რომელიც ცენტრალიზებულად მართავს ქსელის მუშაობას და/ან აწვდის ქსელის სხვა კომპიუტერებს თავის

რესურსებს კლიენტური კომპიუტერი (კლიენტი, მუშა სადგური) - ქსელის რიგითი მომხმარებლის კომპიუტერი, რომელიც ღებულობს დაშვებას სერვერის (სერვერების) რესურსებისადმი. ქსელის უპირატესობები: – ქსელში საჭიროა ნაკლები პერიფერიული მოწყობილობა. ი იმის გამო რომ ქსელში გვაქვს შესაძლებლობა გავანაწილოთ რესურსები და მივცეთ დაშორებულ კომპიუტერებს წვდომა ჩვენს პერიფერიულ მოწყობილობებზე, გამოირიცხა მიზეზი, რომ თითოეულ კომპიუტერს შეიძლებოდა დასჭირვებოდა ცალკე პრინტერი თუ სკანერი ან სხვა მოწყობილობა – ქსელის მეშვეობით იზრდება კავშირგაბმულობის შესაძლებლობები ი ქსელი გვაძლევს სხვადასხვა ტიპის ხელსაწყოების გამოყენების შესაძლებლობას კავშირგაბმულობისათვის - იქნება ეს ფორუმები, ჩეთები, იმეილები, აუდიო თუ ვიდეო კავშირის საშუალებები, ამ ხელსაწყოების გამოყენებით ადამიანებს შეუძლიათ გაცვალონ ინფორმაცია, დაუკავშირდნენ თავიანთ მეგობრებს, ოჯახის წევრებსა და კოლეგებს. – ფაილების დუბლირებისა და დაზიანებისაგან დაცვა ი სერვერი განაგებს ქსელურ რესურსებს, ის ინახავს მონაცემებს და ანაწილებს მათ მომხმარებლებს შორის, კონფიდენციალური მონაცემების დაცვა შეიძლება განხორციელდეს და მასზე წვდომა იყოს დაშვებული მხოლოდ განსაკუთრებული მომხმარებლებისათვის. – ლიცენზირების უფრო დაბალი ფასი ი პროგრამების ლიცენზიები ხშირად უფრო ძვირია ინდივიდუალურ მანქანებზე დასაყენებლად. ბევრი მწარმოებელი კომპანია იძლევა ე.წ. ”Site license”-ის შემოთავაზებას - ლიცენზია ქსელებისათვის, რაც ნიშნავს რომ ერთი კონკრეტული ფასით, ადამიანთა რაიმე ჯგუფს ან კომპანიის ყველა თანამშრომელს შეძლია ჰქონდეს წვდომა შესაბამის პროგრამულ უზრუნველყოფაზე – ცენტრალიზირებული ადმინისტრირება ი ცენტრალიზირებული ადმინისტრირება ამცირებს ხალხის რაოდენობას, რომელიც საჭიროა ქსელური მოწყობილობებისა და ქსელში მონაცემების სამართავად, რაც თავის მხრივ ამცირებს კომპანიის დანახარჯებსროგორც ფინანსურს ასევე დროითს, ინდივიდუალურ მომხმარებლებს არ სჭირდებათ თავიანთი მონაცემებისა და მოწყობილობების მართვა, ერთ

ადმინსიტრატორს შეუიძლია მართოს მონაცემები, მოწყობილობები და მომხმარებლების დაშვების უფლებები ქსელში, მონაცემების რეზერვირებაც მარტივდება, რადგან ისინი სრულად ინახება ერთ ცენტრალურ ადგილზე. – რესურსების ეკონომია o სამუშაო შეიძლება იქნას გადანაწილებულ იქნას რამოდენიმე კომპიუტერს შორის და შედეგად არ მოხდეს ინფორმაციის გადამუშავებით არცერთი ცალკე აღებული კომპიუტერის გადატვირთვა უზრუნველყოფს ერთ ქსელში რამოდენიმე კომპიუტერის ჩართვას(პორტების რაოდენობის მიხედვით) ჰაბისაგან განსხვავებით კომუტატორს შეუძლია პაკეტის თავსართში ამოიკითხოს MAC მისამართი, გაარკვიოს რომელი ქსელის ადაპტერს(NIC) ეკუთვნის პაკეტი და გაუგზავნის ადრესატ კომპიუტერს. ანუ სვიჩი მონაცემებს უგზავნის იმ კომპიუტერს, რომლისთვისაცაა განკუთვნილი. არსებობს ორი სახის სვიჩი: გამჭოლი და შემნახველი. გამჭოლი სვიჩები ჩვეულებრივ მიიღებენ პაკეტებს და გადაუგზავნიან შესაბამის კომპიუტერებს, ხოლო შემნახველ სვიჩებს აქვთ საკუთარი პროცესორი და მეხსიერების ბუფერი. ისინი აგროვებენ შემოსულ პაკეტებს, ამოწმებენ შეცდომებს, შემდეგ ისევ ანაწილებენ და გადასცემენ შესაბამის კომპიუტერებს. მუშაობის პრინციპიდან გამომდინარე, სვიჩებს უფრო მეტი შესაერთებლები აქვთ და ჰაბების მსგავსად მათი ერთმანეთთან მიერთებაც შეიძლება. მარშრუტიზატორი (Router) გამოიყენება სხვადასხვა ქსელების ერთმანეთთან დასაკავშირებლად, განსაზღვრავს მარშრუტს დაშორებულ ქსელებში ინფორმაციის გადაცემისას კოაქსიალური კაბელი ყველაზე მეტად იყო გავრცელებული თავისი ფასის, წონისა და პრაქტიკულობის და ასევე დაყენების სიმარტივის გამო. მარტივი კოაქსიალური კაბელი შედგება სპილენძის გამტარისაგან, ირგვლივ შემოხვეული საიზოლაციო შრისაგან, მეტალის წნულისაგან (ეკრანისაგან) და გარე გარსისაგან. ზოგჯერ მეტალის წნულის გარდა აქვს ფოლგის ფენაც და ასეთს ეწოდება კაბელი ორმაგი ეკრანიზაციით. კოაქსიალური კაბელი შეფერხებების მიმართ უფრო გამძლეა, ვიდრე ხვეულა წყვილი და სიგნალების მილევაც ნაკლებია მასში. სიგნალის მილევა არის კაბელში გავლისას სიგნალების შესუსტება.

კოაქსიალური კაბელის ორი ტიპი არსებობს: წვრილი კოაქსიალური კაბელი (thinnet) და მსხვილი კოაქსიალური კაბელი (thicknet). წვრილი კაბელი მოქნილია, ასეთ კაბელებს ინფორმაციის დაუმახინჯებლად გადაცემა შეუძლია 185 მ-მდე. სქელი კოაქსიალური კაბელი შედარებით ხისტია, დიამეტრი 1 სმ-მდე აქვს. სქელ კოაქსიალური კაბელს მონაცემთა დაუმახინჯებლად გადაცემა შეუძლია 500 მ-დე მანძილზე. UTP კაბელით მონაცემთა გადაცემა შესაძლებელია 100 მეტრამდე მანძილზე, უფრო შორს სიგნალების გადასაცემად საჭიროა ყოველ 100 მეტრში ჩავაყენოთ ქსელური მოწყობილობა, თუმცა 500 მეტრზე შორს ამ კაბელის გამოყენება აღარ შეიძლება, ანუ ერთ გზაზე შეგვიძლია ჩავაყენოთ მხოლოდ 4 ქსელური მოწყობილობა. ამ კაბელებს ხვიურ წყვილებს იმიტომ უწოდებენ, რომ შედგება სადენთა 4 წყვილისაგან, რომელთაგან თითოეული ერთმანეთზეა დახვეული. ეს შემთხვევით არ არის ასე, ცნობილია, რომ სადენთა ერთმანეთზე გადახვევა ხელს უშლის ელექტრო-მაგნიტური ველის შექმნას, ე.ი. კაბელში მონაცემთა დამახინჯებას. თითოეული წყვილი განსხვავდება თავისი ფერით. ერთმანეთზე დახვეულია ლურჯი და თეთრი-ლურჯი ზოლით, მწვანე და თეთრი-მწვანე ზოლით, ნარინჯისფერი და თეთრი-ნარინჯისფერი ზოლით, ყავისფერი და თეთრი-ყავისფერი ზოლით. ფერთა ეს განლაგება ყველა კაბელში ერთნაირია და ამას თავისი მიზეზი აქვს, რასაც მოგვიანებით გავიგებთ. UTP 5e-ს განსხვავებით UTP 5-ისგან მეტი გრეხილი აქვს. ხოლო UTP 6 კაბელი შეიცავს „პლასტიკურ გამყოფს“ წყვილებს შორის. რაც ხელს უშლის ხარვეზებს (დაბრკოლებებს).ოპტიკურ-ბოჭკოვან კაბელში მონაცემთა გადაცემა ხდება მოდულირებული სინათლის იმპულსების სახით. იგი მონაცემთა გადაცემის შედარებით დაცული ხერხია. ასეთი ტიპის ხაზები გამოიყენება დიდი მოცულობის მონაცემების გადასაცემად დიდი სისწრაფით (10 გიგაბიტი/წამამდე). მათში სიგნალების მილევა და დამახინჯება თითქმის არ ხდება. ოპტიკური ბოჭკო წვრილი შუშის ცილინდრია (5-60 მიკრონი), რომელსაც ქვია შუშის ფენით დაფარული სასიგნალო გამტარი. ყოველი ოპტიკური ბოჭკო სიგნალს გადაცემს ერთი მიმართულებით, ამიტომ ყოველი კაბელი შედგება ორი

ოპტიკური ბოჭკოსგან, რომლებსაც აქვთ დამოუკიდებელი კონექტორები; ერთი მათგანი გამოიყენება გადასაცემად, მეორე – მიმღებად. დღესდღეობით კომპიუტერულ ქსელებში გამოიყენება სამივე ტიპის კაბელი, მაგრამ ყველაზე პერსპექტიულია ოპტიკურ-ბოჭკოვანი, ის გამოიყენება მაგისტრალების ასაგებად ოპტიკურ-ბოჭკოვანი კაბელით ინფორმაციის გადაცემის დროს მასზე არ მოქმედებს ელექტრული შეფერხებები, არ ხდება სიგნალის დამახინჯება და მილევა, ამიტომ გადაცემა ხდება ძალიან დიდი, წამში ასობით მეგაბიტი, სიჩქარით, რომლის თეორიული ზღვარი 200000 მგბტ/წმ-ის ტოლია. არსებობს ორი ტიპის ოპტიკურ-ბოჭკოვანი კაბელი: • Multimode - ამ ტიპის კაბელს სქელი „გული“ აქვს, შესაბამისად მისი დამზადება უფრო ადვილია. სინათლის წყაროდ შესაძლებელია გამოვიყენოთ უფრო მარტივი წყარო (შუქდიოდი). ის კარგად მუშაობს რამდენიმე კილომეტრზე. • Singlemode - მას გააჩნია ძალიან თხელი „გული“ აქვს და შესაბამისად მისი დამზადებაც უფრო ძვირია. ის სინათლის წყაროდ იყენებს ლაზერს და თავისუფლად შეუძლია გადასცეს ინფორმაცია ათეულობით კილომეტრზე. მცირე ზომის ქსელებში სადენის სახით უმრავლეს შემთხვევაში გამოიყენება სპილენძის გრეხილი წყვილი – TP (Twisted Par). ამ კაბელებს ხვიურ წყვილებს იმიტომ უწოდებენ, რომ შედგება სადენთა 4 წყვილისაგან, რომელთაგან თითოეული ერთმანეთზეა დახვეული. ეს შემთხვევით არ არის ასე, ცნობილია, რომ სადენთა ერთმანეთზე გადახვევა ხელს უშლის ელექტრო-მაგნიტური ველის შექმნას, ე.ი. კაბელში მონაცემთა დამახინჯებას. თითოეული წყვილი განსხვავდება თავისი ფერით. ერთმანეთზე დახვეულია ლურჯი და თეთრი-ლურჯი ზოლით, მწვანე და თეთრი-მწვანე ზოლით, ნარინჯისფერი და თეთრი-ნარინჯისფერი ზოლით, ყავისფერი და თეთრი-ყავისფერი ზოლით. ფერთა ეს განლაგება ყველა კაბელში ერთნაირია სიიაფის, დაყენების სიმარტივისა და უნივერსალურობის გამო (შეიძლება გამოვიყენოთ ქსელური ტექნოლოგიების უმრავლესობაში), ამჟამად ლოკალური ქსელების აგებისას ყველაზე გავრცელებული ტიპის კაბელია არაეკრანირებული ხვეული წყვილი. მიუხედავად ხელშეშლების წინააღმდეგ მდგრადობისა, მონტაჟის

სირთულის გამო (საჭიროა ზრუნვა დამიწებაზე), არაეკრანირებულ ხვეულ წყვილთან შედარებით, ეკრანირებული ხვეული წყვილი მეტი სიხისტის გამო არ არის ფართოდ გავრცელებული. ხვეული წყვილი უერთდება კომპიუტერსა და სხვა მოწყობილობებს რვაკონტაქტიანი გასართით (კონექტორით) RJ-45 (Registered Jack 45). ეს კონექტორი ჰგავს სატელეფონო ქსელებში გამოყენებად RJ-11 კონექტორს, ოღონდ მასზე ცოტათი მოზრდილია. სურათზე მოყვანილია RJ-45 კონექტორში ”ხვეული წყვილი” კაბელის ჩამაგრების ხერხები EIA/TIA 568A და EIA/TIA 568 B სტანდარტების შესაბამისად; ეს ოპერაცია სრულდება სპეციალური დასაწნეხი ინსტრუმენტით. (თუ გასართს განვალაგებთ კონტაქტებით ზემოთ და მივმართავთ ჩვენგან, მაშინ კონტაქტები უნდა დაინომროს მარცხნიდან მარჯვნივ 1-ნ 8-დე). უკაბელო ქსელები, რომლებიც 802.11 (Wi-Fi) ოჯახის ერთ-ერთი სტანდარტით მუშაობენ, უფრო და უფრო ფართო გავრცელებას პოულობენ მოწყობილობის ხელმისაწვდომობის, მომართვის სიმარტივით და შემაერთებელი კაბელების არ არსებობის წყალობით. მაგრამ ამ ქსელებს აქვთ გარკვეული ნაკლოვანებებიც. მაგალითად, მონაცემთა გადაცემის დაბალი სიჩქარე, საკაბელო ქსელებთან შედარებით და მგრძნობელობა სხვადასხვა სახის შეფერხებებისა და წინაღობის დროს. ამ მიზეზით მხოლოდ პერსონალური კომპიუტერების არსებობისას უმჯობესია საკაბელო ქსელის შექმნა, რომელიც იმუშავებს სწრაფად და საიმედოდ. პრაქტიკულად თითქმის ყველა თანამედროვე მობილურ კომპიუტერულ სისტემაში არის ჩაშენებული Wi-Fi ადაპტერი და მისი საკაბელო ქსელთან მიერთება ძალიან მოუხერხებელია. ამიტომ მათთვის უკაბელო ქსელი ხშირად წარმოადგენს ოპტიმალურ ვარიანტს. პერსონალური კომპიუტერის უკაბელო ქსელში ჩასართავად საჭიროა სისტემურ ბლოკში Wi-Fi ადაპტერის დაყენება გაფართოებული პლატის სახით ან/და გამოყენებულ იქნეს USB-პორტში ჩასართავი ადაპტერი ცალკე მოწყობილობის სახით. უკაბელო ქსელის შექმნისას ასევე საჭიროა ერთ-ერთი შემდეგი მოწყობილობა: • წვდომის უკაბელო წერტილი (Wireless Access Point) - გამოიყენება რამდენიმე კომპიუტერის უკაბელო ქსელში

გასაერთიანებლად და უკაბელო ქსელის საკაბელოსთან მისაერთებლად. იმისათვის რომ უკაბელო ქსელის ყველა მომხმარებელი შევიდეს ინტერნეტში, ქსელში ასევე უნდა არსებობდეს მოწყობილობა, რომელიც როუტერის ფუნქციას შეასრულებს (ეს შეიძლება იყოს ADSL- მოდემი). • უკაბელო როუტერი (მარშრუტიზატორი) - წვდომის წერტილისაგან განსხვავებით, ქსელში აერთიანებს არა მარტო რამდენიმე უკაბელო მომხმარებელს, არამედ ასევე საშუალებას აძლევს, რომ მათ მიიღონ ინტერნეტი ერთი ჩქაროსნული შეერთებიდან. • უკაბელო ADSL-როუტერი - ეს მოწყობილობა ითავსებს ADSL- მოდემისა და უკაბელო როუტერის ფუნქციებს. ასეთი მოწყობილობის შეძენა ხელსაყრელია ინტერნეტში საერთო წვდომის მქონე უკაბელო ქსელის შესაქმნელად ბინაში ან მცირე ოფისში. თანამედროვე უკაბელო მოწყობილობები მომართულია ვებ-ინტერფეისის საშუალებით. ამისათვის საჭიროა მოწყობილობის კომპიუტერთან მიერთება საკაბელო ქსელის დახმარებით, Internet Explorer-ის სამისამართო სტრიქონში უნდა შევიტანოთ მოწყობილობის მისამართი, შემდეგ მივუთითოთ მომხმარებლის სახელი და პაროლი. ყველა ამ მონაცემის გაგება შესაძლებელია მოწყობილობაზე თანდართული დოკუმენტაციიდან, სადაც ასევე მოცემულია უკაბელო ქსელის დაყენების წესები თანმიმდევრობით. უკაბელო მოწყობილობის კონფიგურირებისათვის ასევე შესაძლებელია სპეციალური უტილიტების გამოყენება მოწყობილობაზე თანდართული კომპაქტ- დისკიდან. უკაბელო მოწყობილობის მომართვის შემდეგ, შესაძლებელია კომპიუტერის ან ნოუთბუქის მიერთება შექმნილ ქსელთან. ამისათვის შევასრულოთ შემდეგი მოქმედებები: 1. Control panel-ის დათვალიერების არეში დავაწკაპუნოთ ქსელის ნიშანზე. 2. გამოსულ ფანჯარაში გამოჩნდება არსებული ადაპტერის რადიუსის ყველა ქსელის ჩამონათვალი. 3. დააწკაპუნეთ საჭირო ქსელის დასახელებაზე და დააჭირეთ ღილაკს შეერთება. იმისათვის რომ შემდეგში შეერთება მოხდეს ავტომატურად, თქვენ ასევე შეგიძლიათ დააყენოთ შესაბამისი ალამი მიერთების ღილაკის გვერდით. 4. შემდეგ ფანჯარაში აუცილებლობის შემთხვევაში შეიყვანეთ

უსაფრთხოების გასაღები და დააჭირეთ ღილაკს OK. ეს გასაღები ჩვეულებრივ გამოდის ქსელის დაყენებისას წვდომის წერტილზე ან უკაბელო როუტერთან. მას შემდეგ რაც, მოხდება მიერთება ახალ უკაბელო ქსელთან, გამოჩნდება ფანჯარა ქსელის განთავსების ასარჩევად. პრაქტიკული სამუშაო გაამზადეთ TP კაბელები შესაბამისად Crossover და Straight შეერთებებისთვის დაუკავშირეთ კომპიუტერები კომუტატორს, მიანიჭეთ ლოგიკური მისამართები, შეამოწმეთ კავშირი დაუკავშირეთ კომპიუტერი მრავალფუნქციურ მოწყობილობას, შეცვალეთ მოწყობილობის ქსელური სახელი და პაროლი, დაუკავშირეთ უკაბელო ქსელის ადაპტერით აღჭურვილი მოწყობილობები მრავალფუნქციურ მოწყობილობას პრაქტიკული სამუშაო - პირდაპირი შეერთების (Straight-Through) და ჯვარედინი შეერთების (Crossover) UTP კაბელების აწყობა შესავალი დაბეჭდეთ და შეავსეთ მოცემული ლაბორატორიული სამუშაო ამ დავალებაში თქვენ უნდა აწყოთ და შეამოწმოთ პირდაპირი (Straight-Through) და ჯვარედინი (Crossover) შეერთების არაეკრანირებული, გრეხილი წყვილი (UTP) Ethernet ქსელის კაბელი. შენიშვნა: პირდაპირი შეერთების (Straight-through) კაბელის დროს, სადენის ფერი, რომელიც გამოყენებულია ერთი მხარის დაბოლოების პირველ კონტაქტზე არის იგივე ფერის, რომელიც გამოყენებულია მეორე მხარის დაბოლოების პირველ კონტაქტზე. ასევეა დანარჩენი შვიდი კონტაქტიც. კაბელი შეიძლება შექმნილი იყოს TIA/EIA T568A ან T568B Ethernet სტანდარტის გამოყენებით, რომელიც განსაზღვრავს სადენის ფერს, რაც გამოყენებულია თითოეულ შესასვლელში. პირდაპირი შეერთების (Straight-Through) კაბელები როგორც წესი გამოიყენება ჰოსტის უშუალოდ დასაკავშირებლად კონცენტრატორთან (Hub), კომუტატორთან (Switch) ან კედელზე დასამაგრებელ აუთლეტთან ოფისში. ჯვარედინი შეერთების (Crossower) კაბელის დროს, მეორე და მესამე წყვილები კაბელის ერთი ბოლოს RJ-45 კონექტორზე არის საპირისპირო კაბელის მეორე ბოლოზე. კაბელის ერთი მხარის კონტაქტები არის T568A სტანდარტის, ხოლო მეორე მხარეს - T568B სტანდარტი. ჯვარედინი შეერთების კაბელი (Crossower) როგორც წესი

გამოიყენება კონცენტრატორების (Hub) და კომუტატორების (Switch) დასაკავშირებლად ან ორი კომპიუტერის პირდაპირ შესაერთებლად, მარტივი ქსელის შექმნისთვის. რეკომენდებული მოწყობილობები: • ორი 0.6-დან 0.9 მეტრამდე სიგრძის 5 ან 5e კატეგორიის (Cat5, Cat5e) კაბელი • მინიმუმ ოთხი ცალი RJ-45 კონექტორი (მეტი შეიძლება საჭირო გახდეს არასწორად დამზადების შემთხვევაში) .

SNMP განვითარდა იმისათვის, რომ ადმინისტრატორებს ჰქონდეთ საშუალება მართონ სერვერები, სამუშაო სადგურები (Workstations), მარშრუტიზატორები, კომუტატორები და უსაფრთხოების ტექნიკა, IP ქსელში. ის საშუალებას აძლევს ქსელის ადმინისტრატორებს მართონ ქსელის წარმადობა, იპოვონ და აღმოფხვრან ქსელური პრობლემები და დაგეგმონ ქსელის გაზრდა. SNMP არის გამოყენებითი დონის პროტოკოლი, რომელიც უზრუნველყოფს შეტყობინების ფორმატს, მენეჯერებსა და აგენტებს შორის კომუნიკაციისთვის. SNMP სისტემა შედგება სამი ელემენტისაგან: • SNMP მენეჯერი • SNMP აგენტი (მართვადი კვანძი) • მართვის საინფორმაციო ბაზა (MIB) ქსელურ მოწყობილობაზე SNMP-ს კონფიგურაციისთვის, პირველ რიგში აუცილებელია განისაზღვროს ურთიერთობა მენეჯერსა და აგენტს შორის. SNMP მენეჯერი არის ქსელის მართვის სისტემის (NMS) ნაწილი. SNMP მენეჯერი უშვებს SNMP-ის მართვის პროგრამულ უზრუნველყოფას. როგორც 5.1 სურათზეა მოცემული, SNMP მენეჯერს შეუძლია შეაგროვოს ინფორმაცია SNMP აგენტებიდან „get (მიღება)“ მოქმედების გამოყენებით და შეუძლი კონფიგურაციის შეცვლა აგენტზე „Set (გაშვება)“ მოქმედების გამოყენებით. დამატებით, SNMP აგენტებს შეუძლიათ ინფორმაციის გადაგზავნა პირდაპირ ქსელის მართვის სისტემასთან (NMS), „traps (მახეები)”-ის გამოყენებით. SNMP აგენტი და მართვის საინფორმაციო ბაზა (MIB) მიეკუთვნება ქსელური მოწყობილობების კლიენტებს. ის ქსელური მოწყობილობები, რომელთა მართვაც შეიძლება, კომუტატორების, მარშრუტიზატორების, სერვერების, ფაიერვოლების და სამუშაო სადგურების ჩათვლით, აღჭურვილია SNMP აგენტი პროგრამული

უზრუნველყოფის მოდულით. მართვის საინფორმაციო ბაზა (MIB) ინახავს მონაცემებს მოწყობილობის მუშაობის შესახებ და განკუთვნილია იმისთვის რომ იყოს ხელმისაწვდომი ავტორიზებული დაშორებული მომხმარებლებისთვის. SNMP აგენტი პასუხისმგებელია ლოკალური მართვის საინფორმაციო ბაზის წვდომის უზრუნველყოფაზე ობიექტებთან, რომლებიც ასახავენ რესურსებსა და საქმიანობას. SNMP განსაზღვრავს თუ როგორ იცვლება სამართავი ინფორმაცია ქსელის მართვის აპლიკაციებსა და მართვად აგენტებს შორის. SNMP იყენებს UDP პროტოკოლს, პორტის ნომრით 162, რათა მიიღოს და გააგზავნოს მართვის ინფორმაცია. 5.1.1 SNMP კონფიგურაციის ეტაპები ქსელის ადმინისტრატორს შეუძლია SNMPv2-ის კონფიგურაცია ქსელური მოწყობილობებიდან ქსელის ინფორმაციის მისაღებად. როგორც 5.1.1 სურათზეა ნაჩვენები, SNMP-ს კონფიგურაციის ყველა ბაზისური ეტაპი არის საერთო კონფიგურაციის რეჟიმში. პირველი ეტაპი. (აუცილებელი) დააკონფიგურეთ მწკრივების ერთობა (Community String) და დაშვების დონე (მხოლოდ ნახვა ან ნახვა-ჩაწერა) snmp-server community string ro | rw ბრძანებით. მეორე ეტაპი. (დამატებითი) მოახდინეთ მოწყობილობის ადგილმდებარეობის დოკუმენტირება snmp-server location text ბრძანების გამოყენებით. მესამე ეტაპი. (დამატებითი) მოახდინეთ სისტემური კონტაქტების დოკუმენტირება მეოთხე ეტაპი. (დამატებითი) აკრძალეთ SNMP-ს წვდომა ქსელის მართვის სისტემის (NMS) ჰოსტებთან (SNMP მენეჯერები), რომლებიც დაშვებულნი არიან ACL-ის მიერ: განსაზღვრეთ ACL და შემდეგ მიუთითეთ ACL snmp-server community string access-listnumber-or-name ბრძანების გამოყენებით. მოცემული ბრძანება გამოიყენება როგორც მწკრივების მისათითებლად, ისე SNMP წვდომის აკრძალვისთვის ACL-ების მეშვეობით. სურვილის შემთხვევაში პირველი და მეოთხე ეტაპი შეიძლება გაერთიანდეს ერთ ეტაპად. Cisco ქსელური მოწყობილობა აერთიანებს ორ ბრძანებას ერთში, თუ ისინი შეტანილია ცალ- ცალკე. მეხუთე ეტაპი. (დამატებითი) მიუთითეთ SNMP trap ოპერაციების მიმღები snmp-server host host-id [version {1 | 2c | 3 [auth | noauth | priv]}] community-string ბრძანების

გამოყენებით. ნაგულისხმევად trap მენეჯერ არ არის მითითებული. მეექვსე ეტაპი. (დამატებითი) ჩართეთ traps (მახეები) SNMP აგენტზე snmp-server enable traps notification-types ბრძანებით. თუ მოცემულ ბრძანებაში არცერთი trap შეტყობინების ტიპი არ არის მითითებული, მაშინ ყველა ტიპის trap-ი იქნება გაგზავნილი. ამ ბრძანების განმეორებითი გამოყენება მოითხოვება, მაშინ თუ განსაზღვრული ტიპის trap ქვეჯგუფებია სასურველი. შენიშვნა: ნაგულისხმევად, SNMP-ს არ აქვს არანაირი trap-ები მომართული. ამ ბრძანების გარეშე, SNMP მენეჯერებს შეუძლიათ ამოირჩიონ ყველა მართებული ინფორმაცია. Simple Network Management Protocol (SNMP) არის ქსელის მართვის პროტოკოლი და IETF სტანდარტი, რომელიც შეიძლება გამოყენებულ იქნას ქსელში კლიენტების მონიტორინგისა და მართვისათვის. SNMP შეიძლება გამოყენებულ იქნას ცვლადების მიღებისა და დაყენებისათვის, რომლებიც დაკავშირებულია ქსელური ჰოსტების მდგომარეობასა და კონფიგურაციაზე, როგორიცაა მარშრუტიზატორები და კომუტატორები, ასევე კლიენტი კომპიუტერების ქსელი. SNMP მმართველმა შეიძლება შეაგროვოს SNMP აგენტები მონაცემებისათვის, ან მონაცემები შეიძლება ავტომატურად იქნას გაგზავნილი SNMP მმართველთან, SNMP აგენტებზე trap-ების კონფიგურაციით. ამ ლაბორატორიულ დავალებაში თქვენ გადმოიწერთ, დააინსტალირებთ და დააკონფიგურებთ SNMP მართვის პროგრამულ უზრუნველყოფას PC-A-ზე. თქვენ ასევე დააკონფიგურებთ Cisco მარშრუტიზატორებს და Cisco კომუტატორებს, როგორც SNMP აგენტებს. SNMP აგენტიდან მოსული SNMP შეტყობინების დაჭერის შემდეგ, თქვენ უნდა მოახდენთ MIB/Object ID კოდების კონვერტაციას, შეტყობინების დეტალების შესასწავლად Cisco SNMP Object Navigator-ის გამოყენებით მარშრუტიზატორები, რომლებიც გამოიყენება CCNA-ს პრაქტიკული სამუშაოებისთვის, არის Cisco 1941 ინტეგრირებული სერვისების მარშრუტიზატორები (ISRs) Cisco IOS Release 15.2(4)M3 (universalk9 image) ვერსიასთან ერთად. გამოყენებული კომუტატორები არის Cisco Catalyst 2960s ვერსია, Cisco IOS Release 15.0(2) (lanbasek9 image) ოპერაციული სისტემით. შესაძლოა გამოყენებულ იქნას სხვა

მარშრუტიზატორები, კომუტატორები და Cisco IOS ვერსიებიც. მოდელისა და Cisco IOS ვერსიის მიხედვით ხელმისაწვდომი ბრძანებები და მიღებული შედეგები შეიძლება იყოს განსხვავებული იმისგან, რაც ნაჩვენებია ამ ლაბორატორიულ სამუშაოში. მიაქციეთ ყურადღება მარშრუტიზატორის ინტერფეისის შემაჯამებელ ცხრილს ამ დავალების ბოლოში, სწორი ინტერფეისის იდენტიფიკატორებისათვის. შენიშვნა: snmp-server ბრძანებები ამ ლაბორატორიულ დავალებაში გამოიწვევს Cisco 2960 კომუტატორზე გამაფრთხილებელი შეტყობინების გაშვებას, კონფიგურაციის ფაილის NVRAM-ში შენახვის დროს. გამაფრთხილებელი შეტყობინების თავიდან ასაცილებლად შეამოწმეთ კომუტატორი იყენებს თუ არა lanbase-routing შაბლონს. IOS შაბლონი იმართება კომუტატორის მონაცემთა ბაზის მმართველის (Switch Database Manager - SDM)-ის მიერ. სასურველი შაბლონის შეცვლის შემდეგ ახალი შაბლონი გამოყენებული იქნება გადატვირთვის შემდეგ, მაშინაც კი თუ კონფიგურაცია არ არის შენახული. S1# show sdm prefer გამოიყენეთ ქვემოთ მოცემული ბრძანებები lanbase-routing შაბლონის ნაგულისხმევ SDM შაბლონად მითითებისთვის. S1# configure terminal S1 (config) # sdm prefer lanbase-routing S1 (config) # end S1 # reload მოთხოვნილი რესურსები: • ორი მარშრუტიზატორი (Cisco 1941 Cisco IOS Release 15.2(4)M3 უნივერსალი იმიჯით ან მსგავსით) • ერთი კომუტატორი (Cisco 2960 Cisco IOS Release 15.0(2) lanbasek9 იმიჯით ან მსგავსით) • ერთი პერსონალური კომპიუტერი (Windows ოპერაციული სისტემა ტერმინალის ემულაციის პროგრამასთან ერთად, როგორიცაა Tera Term) • ერთი პერსონალური კომპიუტერი (Windows ოპერაციული სისტემა ინტერნეტთან წვდომით) • კონსოლის კაბელები Cisco IOS მოწყობილობების კონსოლის პორტებით კონფიგურაციისათვის. • Ethernet და სერიალური კაბელები, როგორც ნაჩვენებია ტოპოლოგიაზე • SNMP მართვის პროგრამული უზრუნველყოფა (PowerSNMP უფასო მმართველი Dart Communication-სგან, ან SolarWinds Kiwi Syslog Server-ის 30 დღიანი საცდელი ვერსია). ნაწილი №1: ქსელის აწყობა და მოწყობილობის ბაზისური პარამეტრების კონფიგურაცია ამ ნაწილში თქვენ მომართავთ ქსელის

ტოპოლოგიას და დააკონფიგურებთ მოწყობილობას ბაზისური პარამეტრებით. პირველი ეტაპი: ქსელის კაბელებით დაკავშირება, როგორც ნაჩვენებია ტოპოლოგიაზე. მეორე ეტაპი: PC ჰოსტის კონფიგურაცია მესამე ეტაპი: მარშრუტიზატორებისა და კომუტატორის ინიციალიზაცია და ხელახლა ჩატვირთვა აუცილებლობის შემთხვევაში მეოთხე ეტაპი: ბაზისური პარამეტრების კონფიგურაცია მარშრუტიზატორებისა და კომუტატორისთვის. ა. გათიშეთ DNS lookup ბ. მომართეთ მოწყობილობების სახელები ისე როგორც ნაჩვენებია ტოპოლოგიაზე გ. დააკონფიგურეთ IP მისამართები მისამართების ცხრილის მიხედვით. ზ. Ping ბრძანების გაშვებით შეამოწმეთ LAN მოწყობილობებს შორის წარმატებული კავშირი. თ. გადაიტანეთ გაშვებული კონფიგურაციის ასლი საწყის კონფიგურაციაში. ნაწილი №2: SNMP მმართველისა და აგენტების კონფიგურაცია მეორე ნაწილში, PC-A-ზე მოხდება SNMP მართვის პროგრამული უზრუნველყოფის ინსტალაცია და კონფიგურაცია, ასევე R1 და S1 იქნება დაკონფიგურებული, როგორც SNMP აგენტები. პირველი ეტაპი: SNMP მართვის პროგრამის ინსტალაცია ა. გადმოწერეთ და დააინსტალირეთ Dart Communications-ის მიერ გამოშვებული PowerSNMP Free Manager პროგრამა ქვემოთ მოცემული მისამართიდან: http://www.dart.com/snmp-free-manager.aspx. ბ. გაუშვით PowerSNMP Free Manager პროგრამა. გ. დააჭირეთ No ღილაკს თუ შემოთავაზებულ იქნა ხელმისაწვდომი SNMP აგენტების აღმოჩენა. თქვენ აღმოაჩენთ SNMP აგენტებს, R1 მარშრუტიზატორზე SNMP-ს კონფიგურაციის შემდეგ. PowerSNMP Free Manager მხარს უჭერს SNMP-ს 1, 2 და 3 ვერსიებს. მოცემულ ლაბორატორიულ სამუშაოში გამოყენებულია SNMPv2. : თუ შემოთავაზებულ იქნა ხელმისაწვდომი SNMP აგენტების აღმოჩენა, დააჭირეთ No ღილაკს და გადადით ამ დავალების შემტებ ეტაპზე. მეორე ეტაპი: SNMP აგენტის კონფიგურაცია ა. R1 მარშრუტიზატორზე გლობალური კონფიგურაციის რეჟიმიდან შეიყვანეთ ქვემოთ მოცემული ბრძანებები, მარშრუტიზატორის როგორც SNMP აგენტის კონფიგურაციისათვის. პირველ სტრიქონზე SNMP რიგების ერთობა (Community string) არის ciscolab, მხოლოდ დათვალიერების

პრივილეგიებით და SNMP_ACL სახელის მქონე წვდომის სია, რომელიც განსაზღვრავს თუ რომელი ჰოსტები არიან დაშვებული რომ მიიღონ SNMP ინფორმაცია R1 მარშრუტიზატორიდან. მეორე და მესამე სტრიქონებზე SNMP მმართველის location და contact ბრძანებები იძლევიან აღწერილობით საკონტაქტო ინფორმაციას. მეოთხე სტრიქონი განსაზღვრავს ჰოსტის IP მისამართს, რომელიც მიიღებს SNMP შეტყობინებებს, SNMP ვერსიას და რიგების ერთობას (Community string). მეხუთე სტრიქონი რთავს ყველა ნაგულისხმევ SNMP trap-ს, ხოლო მე-6 და მე-7 სტრიქონები ქმნიან დასახელებულ წვდომის სიას, რათა აკონტროლოს თუ რომელი ჰოსტები არიან დაშვებული მარშრუტიზატორიდან SNMP ინფორმაციის მისაღებად. R1 (config) # snmp-server community ciscolab ro SNMP_ACL R1 (config) # snmp-server location snmp_manager R1 (config) # snmp-server contact ciscolab_admin R1 (config) # snmp-server host 192.168.1.3 version 2c ciscolab R1 (config) # snmp-server enable traps R1 (config) # ip access-list standard SNMP_ACL R1 (config-std-nacl) # permit 192.168.1.3 ბ. ამ ეტაპზე თქვენ შეიძლება გაფრთხილებულ იქნათ, რომ PowerSNMP Free Manager იღებს შეტყობინებებს R1 მარშრუტიზატორიდან. თუ ასე არაა, მაშინ თქვენ ა. PC-A-ზე დაყენებული PowerSNMP Free Manager პროგრამიდან, გახსენით Discover > SNMP Agents ფანჯარა. შეიყვანეთ IP მისამართი 192.168.1.255. იგივე ფანჯარაში დააჭირეთ Properties ღილაკს და მომართეთ ciscolab community და SNMP ვერსია ორი, შემდეგ დააჭირეთ OK ღილაკს. ახლა თქვენ შეგიძლიათ დააწვეთ Find ღილაკს, ყველა SNMP აგენტის აღმოსაჩენად 192.168.1.0 ქსელში. PowerSNMP Free Manager-მა შეიძლება იპოვოს R1 მარშრუტიზატორი 192.168.1.1-ზე. დააწექით მონიშვნას და შემდეგ Add ღილაკს, R1 მარშრუტიზატორის როგორც SNMP აგენტის დასამატებლად.

2.2. სერვერების ინფრასტრუქტურის მოწყობა

კომპიუტერული ლოკალური ქსელისა და სასერვერო ინფრასტრუქტურის არსებობა აუცილებელია თანამედროვე

ორგანიზაციებისათვის, სადაც მნიშვნელოვანია, რომ ოპერატიულად და ცენტრალიზებულად მოხდეს ინფორმაციის დამუშავება და შესაბამისად, ინფორმაციას განესაზღვროს გრიფი. იმავდროულად, ლოკალური ქსელი რთული საკაბელო სისტემაა, რომლის გაერთიანებისა და ფუნქციონირებისთვის უამრავი კომპონენტია საჭირო. აქედან გამომდინარე, აუცილებელია კვალიფიციური და სწორი მიდგომა ინფორმაციული ინფრასტრუქტურის დაპროექტებისა და შემდგომ, მისი მონტაჟის დროს.

ლოკალური გამომთვლელი ქსელი (LAN) აპარატურებისა და პროგრამული მომსახურების ერთობლიობაა, რომელიც კომპიუტერებს აერთიანებს ერთიან გამანაწილებელ სისტემად, ინფორმაციის დამუშავებისა და შენახვის საშუალებად. აპარატურულ უზრუნველყოფად შეიძლება ჩაითვალოს კომპიუტერები, რომლებსაც აქვთ ქსელური ადაპტერები, სვიჩები, როუტერები, IP ტელეფონები, სერვერები და ყველა ის მოწყობილობა, რომელსაც ამა თუ იმ გზით აქვს ქსელში წვდომა და შეუძლია ინფორმაციის დამუშავებაში გარკვეული მონაწილეობის მიღება. პროგრამულ უზრუნველყოფას წარმოადგენს ყველა ის პროგრამა, რომელიც გამოიყენება ინფორმაციის დამუშავების, გადაცემის, შიფრაციისა და სხვა სამუშაოებისთვის. მაგალითისთვის შეიძლება მოვიყვანოთ: VPN (ვირტუალური კერძო ქსელი) – პროგრამული უზრუნველყოფა, რომელიც მოშორებული კომპიუტერისთვის ინფორმაციის უსაფრთხოდ გადაცემის საშუალებას იძლევა, ამ ტიპის ქსელი სპეციალური შიფრაციის მეთოდებითაა დაცული; Microsoft SQL Server – პროგრამული პროდუქტი, რომელიც ცენტრალიზებულად და ონლაინ რეჟიმში ინფორმაციის დამუშავების საშუალებას იძლევა. ინფორმაციის დამუშავების და შენახვის ეს პროგრამული პროდუქტი ძალიან ეფექტურად გამოიყენება მცირე და საშუალო ზომის დაწესებულებებში.

დღეისათვის ინფორმაციული ტექნოლოგიები აქტიურად გამოიყენება თითქმის ყველა სფეროში. ყველა ორგანიზაციასა და დაწესებულებას გააჩნია გარკვეული საინფორმაციო ბაზა, რომლითაც ისინი

ხელმძღვანელობენ და იღებენ გადაწყვეტილებებს. ხშირ შემთხვევებში ეს ინფორმაცია კონფიდენციალურია, რომელზეც მხოლოდ გარკვეულ პირებს აქვთ წვდომა.

ეფექტური, უსაფრთხო და დაცული ინფორმაციული ინფრასტრუქტურის შესაქმნელად აუცილებელია თანამედროვე ორგანიზაციებში შესაბამისი ინფორმაციული სისტემების დანერგვა. ინფორმაციის დამუშავების ავტომატიზება, ინფორმაციის დამუშავების მეთოდებისა და ფორმების გართულება პირდაპირპროპორციულად არის დამოკიდებული მომხმარებლის მიერ მოთხოვნილ უსაფრთხოების საიმედოობაზე. რაც უფრო საიმედოა ინფორმაციის დაცვის სისტემა, მით უფრო რთულია დაცვის მეთოდები და ფორმები. ყოველგვარი ინფორმაციული უსაფრთხოების მხარდაჭერა პირდაპირ არის დაკავშირებული ორგანიზაციის ინფორმაციული უსაფრთხოების პოლიტიკასთან.

ჩატარებულმა კვლევებმა აჩვენა, რომ ჯერ კიდევ ბოლომდე არ არის შესწავლილი და დადგენილი ის სტანდარტები, რომლებიც სრულად უზრუნველყოფს ინფორმაციის უსაფრთხოებას. ინფორმაციის უსაფრთხოების საკითხები სულ უფრო და უფრო აქტუალური ხდება თითქმის ყველა თანამედროვე ორგანიზაციისთვის. ამის გამო, ორგანიზაციები ხშირად ქირაობენ სპეციალურ კომპანიებს/სპეციალისტებს თავიანთი ორგანიზაციების უსაფრთხოების შემოწმების მიზნით. გარკვეული ტიპის დაწესებულებებს, მაგალითად სააქციო საზოგადოებებს, ხშირ შემთხვევაში, მთელი რიგი განყოფილებები აქვთ დაკომპლექტებული პროფესიონალებით, რომლებიც უზრუნველყოფენ უსაფრთხოების ნორმების, ჩარჩოების გამართვას და მათ სრულფასოვან ფუნქციონირებას. დღეისათვის ეს სფერო ჯერ კიდევ განვითარების ეტაპზეა და საგრძნობი პოპულარობით განსაკუთრებით დიდ ორგანიზაციებში სარგებლობს.

იმისათვის რომ შესაძლებელი იყოს ინფორმაციაზე წვდომის კონტროლი, აუცილებელია როგორც აპარატურული, ისე პროგრამული საშუალებების ეფექტურად ფუნქციონირება. ნახ.1-ზე ნაჩვენებია, როგორ

უნდა იყოს გამართული ინფორმაციული ინფრასტრუქტურა მცირე ორგანიზაციებში, აპარატურული და პროგრამული საშუალებების მინიმალური ნაკრების გამოყენებით.

ნახ. 1–ზე ნაჩვენები სისტემა იდეალურია მცირე ზომის ობიექტისთვის, რომლებსაც სავსებით დააკმაყოფილებს გამოყენებული აპარატურის წარმადობა. მოკლედ დავახასიათოთ თითოეული მათგანი:

1. Firewall არის აპარატურული ან პროგრამული უზრუნველყოფა, რომელიც ახორციელებს მასში შემავალი პაკეტების ტრაფიკის კონტროლს და ფილტრაციას. მისი ძირითადი ამოცანა ლოკალური ქსელის ან მისი ცალკეული კვანძების არასანქცირებული წვდომისგან დაცვაა. ის კრძალავს არაავტორიზირებულ წვდომას და ნებას რთავს მხოლოდ ავტორიზებულ კავშირს როგორც ქსელიდან გამავალ პაკეტებზე, ასევე ქსელში შემავალ პაკეტებზე. ორგანიზაციამ, რომელსაც ჯერ კიდევ არა აქვს ჩამოყალიბებული ინფორმაციული უსაფრთხოების ინფრასტრუქტურა, სწორედ ამ მექანიზმის დანერგვით უნდა დაიწყოს.

2. აუტენტიფიკაციის სერვერი (Authentication server) შესაძლებლობას გვაძლევს შევქმნათ მოქნილი იერარქია ჩვენი გარემოსათვის. მთავარ ადმინისტრატორს, მისი გამოყენებით, შეუძლია გარკვეული უფლებების დელეგირება მოახდინოს ადგილობრივ ადმინისტრატორებზე, გუნდის წევრებზე ან ჯგუფებზე; შესაძლებელია იერარქია აიგოს ნებისმიერი სასურველი გზით - გეოგრაფიული ადგილების, ქვეგანყოფილებების, ზოდიაქოს ნიშნების და ა.შ. მიხედვით; აგრეთვე უზრუნველყოფს ქსელში კომპიუტერებისა და მომხმარებლების კონტროლს.

3. სვიჩი (Switch) სხვადასხვა ქსელური მოწყობილობის ქსელში ჩართვის საშუალებას იძლევა. გარდა ამისა, მისი ერთ-ერთი ფუნქციაა დეტექტირება მოახდინოს და ქსელში შეუშვას მხოლოდ საჭირო აპარატურა.

4. როუტერი (Router) ქსელში არსებული პაკეტების მარშრუტიზებას უზრუნველყოფს, რაც მთელი სისტემისთვის უმთავრეს ამოცანას

წარმოადგენს. ის მაქსიმალურად ძლიერი უნდა იყოს იმისათვის, რომ შეძლოს მასთან მისული ინფორმაციის სრულად დამუშავება.

5. DBA სერვერზე ინახება ყველა ის ინფორმაცია რომელიც გააჩნია დაწესებულებას.

6. App სერვერის არსებობა მნიშვნელოვანია ინფორმაციის შეგროვება – დამუშავებისთვის.

ზემოთ განხილული კომპონენტების გარეშე ინფორმაციული ინფრასტრუქტურის აგების დაწყება შეუძლებელია. ამ კომპონენტებზე უნდა მოხდეს რესურსის კონცენტრირება და შეირჩეს მაქსიმალურად სწორად, რათა შემდგომი ინფრასტრუქტურული განვითარება წარმატებით დასრულდეს.

თანამედროვე ორგანიზაციებისათვის ინფორმაციული ინფრასტრუქტურის განვითარება პირველ რიგში გულისხმობს ქაღალდის დაზოგვას, რადგანაც ინფორმაციის გადაცემა შესაძლებელი ხდება ელექტრონულად, ეს უკანასკნელი უკვე თავისთავად გულისხმობს იმას რომ რამდენჯერმე იზრდება ინფორმაციის გადაცემის სისწრაფე; შესაძლებელი ხდება პრინტერებისა და სხვა აპარატურული მოწყობილობების ქსელში გაზიარება, რაც ამცირებს არასასურველი აპარატურის რაოდენობას. გარდა ამისა, შესაძლებელი ხდება შეიქმნას ელექტრონული საფოსტო სისტემა, რაც ბევრად ამარტივებს და აჩქარებს კომპანიაში მიმდინარე თითქმის ყველა პროცესს. ინფორმაციული ინფრასტრუქტურის განვითარების შედეგად მარტივდება კომუნიკაცია თანამშრომლებს შორის, გადაწყვეტილებების მიღების პროცესი ბევრად უფრო ეფექტურად და სწრაფად მიმდინარეობს, გაცილებით ადვილია შექმნილ ელექტრონულ საბუთებთან ურთიერთობა და შემდგომში მათი მოძიება.

ხშირად სისტემის ექსპლუატაციის გაშვების მომენტში ფაქტიური დატვირთვა, როგორც წესი მოსალოდნელზე დაბალია და ასევე მცირეა საბოლოო დატვირთვის მნიშვნელობა. გათვალისწინებულ უნდა იქნეს, ის რომ ექსპლუატაციაში მყოფი აპარატურის ნომინალური სიმძლავრეების

ჯამი შესაძლებელია მეტი იყოს დადგენილ სიმძლავრეზე რეზერვის გამოყენების ხარჯზე ან დაბალ სიმძლავრეზე მუშაობის გამო) იმისათის, რომ შეგვეფასებინა ინფრასტრუქტურული რესურსების სიჭარბის რეალური მასშტაბები ჩატარდა გამოკითხვა შემკვეთებს შორის და გამოკვლეულ იქნა რეალური ობიექტების გარკვეული რაოდენობა. აღმოჩნდა, რომ მოსალოდნელი დატვირთვის საბოლოო მნიშვნელობის ზრდა ექსპლუატაციის საწყის პერიოდში 30%-მდეა. შემდგომში გამორკვეულ იქნა, რომ გაშვების მომენტში ფიზიკური დატვირთვა შეადგენს მოსალოდნელიდან 30%–ს, ხოლო საბოლოო ფიზიკური დატვირთვა კი 30%–ს დაყენებული სიმძავრიდან. ყველა ეს მონაცემი ასახულია ნახატ 1–ზე. ამრიგად, ტიპიური გამოყენების , % წლები ფაქტიური დატვირთვა მოსალოდნელი დატვირთვა დაყენებული სიმძლავრე სრული სიმძლავრე 102 გამოთვლითი ცენტრი პროექტირდება ინფრასტრუქტურული რესურსების გასამმაგებული ნამატით.ექსპლოატაციაში მიღების მომენტისათვის ეს ნამატი არის ხოლმე უფრო მეტად მნიშვნელოვანი – როგორც წესი, მიახლოებული ათმაგს შეიძლება გამოვყოთ ორი შემადგენელი ხარჯი, რომელიც ხორციელდება მონაცემთა დაცვის ცენტრის საციცოცხლო ციკლის განმავლობაში, რომლებიც დაკავშირებული არიან ინფრასტრუქტურული რესურსების სიჭარბესთან: ესენია კაპიტალური და მიმდინარე. კაპიტალური ხარჯები, დაკავშირებულნი ინფრასტრუქტურული რესურსების სიჭარბესთან, წარმოდგენილია დამუქებული უბნით ნახ.65–ზე. ეს უბანი შეესაბამება რესურსების წილს, რომლებიც არ გამოიყენება ტიპიურ 103 შემთხვევაში. ჭარბი რესურსები უშუალოდ გადაიანგარიშება ჭარბ კაპიტალურ დანახარჯებში. ელექტროკვებისა და კონდიცირების ჭარბი მოწყობილობების დანახარჯების ჩათვლით და პროექტირებისა და ინსტალაციების სამუშაოთა კაპიტალური ხარჯების გათვალისწინებით, რომელიც მოიცავს ელექტროგაყვანილობისა და ჰაერსატარების მოწყობასაც. ტიპიური გამოთვლითი ცენტრის ელექტროკვებისა და კონდიცირების სისტემები, დაყენებული აპარატურის საერთო სიმძლავრით 100კვტ, მოითხოვს

კაპიტალურ დანახარჯებს 500 000 დოლარის ოდენობით, ან 5 დოლარი/ვატი. რეალურმა ანალიზმა აჩვენა, რომ ამ ინვესტიციის 70%–ს , ანუ 350 000 დოლარს არ მოაქვს არავითარი სარგებლობა. წინა წლებში ასეთი უსარგებლო ხარჯი იყო უფრო მეტი.ფულადი საშუალებების გამოყენების ღირებულების გათვალისწინებით, ინფრასტრუქტურული რესურსების სიჭარბიდან გამომდინარე, დანაკარგები მონაცემთა დამუშავების ცენტრების აგებისათვის ტიპიურ შემთხვევაში შეადგენენ კაპიტალური დანახარჯების თითქმის 100%–ს! ანუ, პირველადი ჩადებული კაპიტალის მხოლოდ 30% თითქმის საკმარისია ფაქტიური მოთხოვნილებების სრული დაკმაყოფილებისათვის. ექსპლუატაციის მთელი ვადის განმავლობაში განხორციელებული და ინფრასტრუქტურული რესურსების სიჭარბესთან დაკავშირებული ზედმეტი დანახარჯები მოიცავენ აგრეთვე საექსპლოატაციო ხარჯებს.ესაა მომსახურების, სახარჯი მასალებისა და ელექტროენერგიის კონტრაქტების ღირებულება. მოწყობილობების მწარმოებელთა ყველა ინსტრუქციის შესრულების შემთხვევაში, მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის სასიცოცხლო ციკლის განმავლობაში მომსახურებაზე დანახარჯების ჯამი როგორც წესი, აღმოჩნდება ხოლმე არაფრით ნაკლები კაპიტალურ დანახარჯებზე. რამდენადაც მომსახურებას ყველა დაყენებული მოწყობილობა მოითხოვს, და არამარტო ფაქტიური მოთხოვნილობების უზრუნველსაყოფად საჭირო მოწყობილობები, ამ ხარჯების მნიშვნელოვანი ნაწილი ტყუილად გაწეულნი აღმოჩნდება ხოლმე. ასე, მაგალითად, მოყვანილ მონაცემთა დაცვის ცენტრის მაგალითზე, საერთო სიმძლავრით 100კვტ, ტყუილად გაწეული ხარჯებს შეუძლია მიაღწიოს თითქმის 250 000 დოლარს. ამის გარდა, მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის ჭარბი ინფრასტრუქტურა მოიხმარს ელექტროენერგიას. მათი ხალასტოი რეჟიმში მოხმარებული სიმძლავრე შეადგენს ნომინალური სიმძლავრის საშუალოდ 5%– ს. ჰაერის კონდიცირებაზე დახარჯული ენერგიის გათვალისწინებით, უნდა ვილაპარაკოთ 10%–ზე. ამგვარად, მონაცემთა დაცვის ცენტრისათვის, საერთო მოხმარებული სიმძლავრით

100კვტ, ინფრასტრუქტურული რესურსების სიჭარბის ტიპიური დონით, ელექტროენერგიის ზედმეტი დანახარჯი მთელი10 წლიანი ექსპლოატაციის ვადის განმავლობაში შეადგენს მიახლოებით 600 000 კვტ/სთ–ს, რომლის ღირებულებაცაა მიახლოებით 55 000 დოლარი. ერთობლიობაში, მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის ექსპლოატაციის ვადის განმავლობაში ზედმეტი ხარჯები შეადგენენ ელექტროკვებისა და კონდიცირების ინფრასტრუქტურის ღირებულების საშუალოდ 70%–ს. ეს არის ის თანხა ეკონომიისა, რომელიც თეორიულად შესაძლებელია მიღებულ იქნას ინფრასტრუქტურის გამოყენების ხარჯზე, რომელსაც შეუძლია მოერგოს ფაქტიურ მოთხოვნილებებს. ბევრ კომპანიას ასეთი კაპიტალური და საექსპლოატაციო ხარჯები შეიძლება დაუჯდეს განუხორციელებელ ახალ პროექტებად და ინვესტიციებად, რაც რეალურად პირდაპირ დანაკარგებზე გაცილებით ძვირია. როგორც შეგროვილი მონაცემებიდანირკვევა, მონაცემთა დამუშავების ცენტრების ან საქსელო კვანძების ინფრასტრუქტურული რესურსების სიჭარბის რეალური სიდიდე საკმაოდ მნიშვნელოვანია და გააჩნია დიდი გაბნევა . ბუნებრივია, წარმოიშობა კითხვა, იგეგმება და მოსალოდნელია თუ არა ეს სიჭარბე თავიდანვე? თუ ის წარმოიშობა შეცდომების გამო, ან იქნებ არსებობს გარკვეული პრინციპული მომენტები, რომლებიც განსაზღვრავენ მათ გარდაუვალობას. გამოთვლითი ცენტრები გეგმარდება აპარატურის მიერ, მომავალში მოხმარებული მაქსიმალური შესაძლო სიმძლავრეების გათვალისწინებით. სრული და გამოყენებული სიმძლავრეების მნიშვნელობები იღება საბოლოოდ მოსალოდნელი დატვირთვასთან შედარებით მეტობით. ხშირად, პრაქტიკაშია ელექტროკვების ქვესისტემის არასრულ სიმძლავრეზე გათვლა – მაგალითად 80%–ზე, გამოდიან რა მოსაზრებიდან, რომ ამგვარად მაღლდება მისი მუშაობის საიმედოობა. გამოთვლითი ცენტრის პროექტირებისას გამოყენებული სიმძლავრის საბოლოო მოსალოდნელი დატვირთვაზე მეტის არჩევის პრაქტიკა ნაჩვენებია ნახატ 1–ზე. ესაა ინფრასტრუქტურული რესურსების მოცულობის გეგმიური ან განზრახ მომატება. მას გააჩნია განსაზღვრული

მნიშვნელობა, თუმცა, მისი წილი საერთო ზედმეტ ხარჯებში არაა ყველაზე დიდი. დაგეგმარების პროცესი და მისი შეცდომები მონაცემთა დამუშავების ცენტრების ან საქსელო კვანძების დაგეგმარების ტიპიური პროცესი ეყრდნობა რიგ დაშვებებს,სამომავლო მოთხოვნილებებთან მიმართებაში. კერძოდ: ინფრასტრუქტურული რესურსების არასაკმარისობის გამოვლენის შემთხვევაში, დანაკარგები იმდენად მაღალია, რომ მსგავსი მოვლენის რისკი უნდა გამოვრიცხოთ; სასიცოცხლო ციკლის განმავლობაში რესურსების გაზრდა ჯდება უაღრესად ძვირი. სამუშაოების ჩატარება, რომლებიც დაკავშირებულია მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის სასიცოცხლო ციკლის განმავლობაში რესურსების გაზრდასთან, ქმნის სერიოზულ და მიუღებელ გაცდენების რისკს. მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის ინფრასტრუქტურის სრული დაპროექტება და კონფიგურაციის დაგეგმარება უნდა შესრულდეს წინასწარ. დროთა განმავლობაში მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის ინფრასტრუქტურის რესურსების ფაქტიური მოთხოვნილება იზრდება, თუმცაღა, წინასწარ განსაზღვრო ამ ზრდის რაოდენობრივი მაჩვენებლები შეუძლებელია. ამ დაშვებებიდან გამომდინარე, მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის ინფრასტრუქტურის დაგეგმარება, დაპროექტება და აგება ხორციელდება წინასწარ, მომავლის პროგნოზების საფუძველზე, რომლებიც ყოველთვის არ ხორციელდა ცხოვრებაში. დაგეგმარების აღწერილი პროცესი წარმოშობს ძალიან დაბალ, საშუალო, რესურსების გამოყენების პროცენტს, რასაც შეიძლება დავაკვირდეთ ფაქტიური მონაცემების მაგალითზე, რაც უნდა განვიხილოთ ეკონომიური თვალსაზრისით ნეგატიურ მოვლენად. მიუხედავად ამისა, ზემოთ განხილულ დაგეგმარების პროცესში არანაირი ნაკლი არ არის. ეს ხილული წინააღმდეგობა შეიძლება გადაიჭრას მონაცემთა უფრო დეტალური შესწავლის გზით და პროცესის შეზღუდვით. ნახ.66–ზე წარმოდგენილია რესურსების გამოყენების ჯამური პროცენტის სტატისტიკური განაწილება . ამ მონაცემების გამოკვლევა გვაძლევს საშუალებას გავაკეთოთ შემდეგი დასკვნები: საშუალოდ, ფაქტიურად

გამოყენებული რესურსების წილი შეადგენს მიახლოებით 30%–ს; საშუალოდ, ზედმეტი რესურსების ან ელექტროკვების ინფრასტრუქტურის არამოთხოვნადი სიმძლავრის წილი შეადგენს მიახლოებით 70%–ს.; ფაქტიურად გამოყენებული რესურსების წილი აქტიურად იცვლება, ვარირების საზღვრები დიდია,რაც მეტყველებს საკმაოდ შეზღუდულ, მომავალი პროგნოზირების შესაძლებლობაზე პროექტირების მიზნებისთვის. დაყენებული სიმძლავრის სიდიდის შემცირება 30%–მდე ტიპიურად გამოყენებადი მნიშვნელობებიდან, მიგვიყვანს ინფრასტრუქტურის შესაძლებლობების საზღვრებიდან ფაქტიური დატვირთვის გამოსვლის 50%– იან ალბათობამდე. გათვლების თანამედროვე მეთოდიკა დაფუძნებულია კომპრომისზე, რომლის ჩარჩოებშიც, რესურსების სიჭარბის მაღალი დონე გამოიყენება როგორც დაცვა საბოლოო ფაქტიური დატვირთვის მნიშვნელობების დიდი დაფანტვისაგან. (აზრი მდგომარეობს ამ პარამეტრის გამოსვლის ალბათობის შემცირებაში სისტემის შესაძლებლობების საზღვრებიდან სასიცოცხლო ციკლის განმავლობაში) ზემოთხსენებულიდან გამომდინარეობს, რომ პროექტირების პროცესის არსებულ შეზღუდვებისას და რესურსების მოთხოვნილებების მომავალი ცვლილებების წინასწარ განსაზღვრის შეუძლებლობის პირობებში, მონაცემთა დამუშავების ცენტრის დაგეგმარების ეხლანდელი მეთოდი სრულიად ლოგიკურია. თუ ფაქტიური მოთხოვნილებების ინფრასტრუქტურის შესაძლებლობების საზღვრებს გარეთ გასვლის ფასი მაღალია, მაშინ, მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის აგების ჩვეულებრივ ვარიანტში საუკეთესო ვარიანტია, მოხდეს მოსალოდნელი ხარჯების მინიმიზაცია – ჩაიდოს სისტემაში დიდი ზედმეტობა. არქიტექტურა, რომელიც გვაძლევს საშუალებას, ავიცილოთ ზედმეტი დანახარჯები პრინციპიალური შეუძლებლობა, მონაცემთა დამუშავების ცენტრის დაგეგმარების ეტაპზე ზუსტად განისაზღვროს მომავალი მოთხოვნილებები, დარჩება გადაულახავ წინაღობად, თუკი ჩვენ ვერ ვისწავლით ვიწინასწარმეტყველოთ მომავალი. ზემოთთქმულიდან გამომდინარე

პრობლემის გადასაჭრელად შეიძლება გამოყენებულ იქნას მონაცემთა დამუშავების ცენტრის ან საქსელო კვანძის ინფრასტრუქტურა,რომელსაც შესწევს უნარი,რეაგირება მოახდინოს მოთხოვნილებათა მოულოდნელ ცვლილებებზე ინფრასტრუქტურული რესურსების სიჭარბის პრობლემების მასშტაბების შეფასება ბუნებრივია წარმოშობს კითხვას: რატომაა აუცილებელი თავიდანვე მთლიანად აიგოს მონაცემთა დამუშავების ცენტრის ინფრასტრუქტურა იმის ნაცვლად, რომ ნელ–ნელა გაიზარდოს აპარატურის პარკის გაზრდის ადექვატურად. რეალობაში, მრავალი გამოთვლითი ცენტრი იგება ამა თუ იმ მრავალეტაპიანი სქემით, რომლებიც გათვლილია თანდათანობით ზრდაზე. მაგალითად, სამონტაჟო კარადების მოწყობილობებით შევსება ხშირად ხორციელდება რამოდენიმე ეტაპად. შიდა ელექტროქსელის განშტოებების გაყვანა რამდენიმე რიგად იყოფა. ზოგიერთ შემთხვევაში, დროში ნაწილდება უწყვეტი კვების წყაროს სარეზერვო მოდულების დაყენება. ყველა ეს მეთოდი გვაძლევს საშუალებას მივიღოთ საერთო დანახარჯების გარკვეული ეკონომია გამოთვლითი ცენტრის სასიცოცხლო ციკლის განმავლობაში. თუმაცაღა, ხშირ შემთხვევებში, დამატებითი მოწყობილობების დაყენების გადადება ჯდება იმდენად ძვირი, რომ გამოთვლითი ცენტრის აგების დაგეგმარებისას, აძლევენ უპირატესობას ბოლო ვარიანტს. ამგვარად, მოცემულ მიმართულებაში, იდეალური იქნებოდა ისეთი მეთოდისა და არქიტექტურის გამოყენების შემთხვევა, რომლებიც უზრუნველყოფდნენ ცვლადი მოთხოვნილებებისადმი უწყვეტ შეთავსებას. ასეთ მეთოდს და არქიტექტურას უნდა გააჩნდეთ შემდეგი მახასიათებლები: ინჟინერულ გადაწყვეტილებათა რაოდენობა, რომლებიც მიიღებიან მონაცემთა დამუშავების ცენტრის აგების პერიოდში, ერთხელ და საბოლოოდ უნდა მნიშვნელოვნად შემცირდეს ან სულაც ნულს გაუტოლდეს. მონაცემთა დამუშავების ცენტრის ელექტროკვების ინფრასტრუქტურა უნდა შედგებოდეს სიღრმისეულად ინჟენერულად გათვლილი მზა მოდულებისაგან, რომლებშიც წინასწარ გათვლილი იქნება მათი გამოყენების ყველა შესაძლო ვარიანტი. ეს მოდულები გათვლილი უნდა

იყვნენ სტანდარტული კარის ღიობებში ტრანსპორტირებისათვის და სამგზავრო ლიფტების გამოყენებით. ისინი უნდა ირთვებოდნენ სისტემაში ძაბვის ქვეშ მყოფ წრედებში რაიმე სახის ოპერაციების შესრულების გარეშეც. აუცილებელია გამოირიცხოს ფართობზე რაიმე სახის სპეციალური მომზადება – აწეული იატაკის მსგავსი. სისტემა გათვლილი უნდა იყოს კონფიგურაციის არჩევაზე რეზერვირების გარეშე ან რეზერვირებით N+1 ან 2N მასში რაიმე სახის მოდიფიკაციების შეტანის გარეშე ინსტალაციის პროცესიდან გამორიცხული უნდა იყოს ისეთი სახის სამუშოები, როგორებიცაა გაყვანილობის მოწყობა, კედლებისა და გადახურვების ხვრეტა და ჭრა. სიმძლავრეების ზრდა არ უნდა მოითხოვდეს რაიმე სახის სპეციალური ნებართვების მიღებას და სპეციალური პროცედურების შესრულებას. ელექტროკვების მოდულური სისტემის ღირებულება არ უნდა აღემატებოდეს ტრადიციული ცენტრალიზირებული სისტემის ღირებულებას. ელექტროკვების მოდულური სისტემის ექსპლოატაციის ხარჯები არ უნდა აღემატებოდეს შესაბამის ხარჯებს ტრადიციულ ცენტრალიზირებული სისტემის შემთხვევაში. ადაპტიურობის გონივრული და მიღწევადი დონეები ფიზიკური ინფრასტრუქტურის ადაპტიური სისტემების განხორციელებისას, საშუალებათა ზედმეტი ხარჯი, რომელიც მოცემულია ნახ.67-ზე დამუქებული უბნით, შესაძლებელია მნიშვნელოვნად შემცირდეს. ეს ეკონომია გამოსახულია ქვემოთ მოყვანილ ნახ.67–ზე. მიაქციეთ ყურადღება, რომ დასაწყისში დაყენებული სიმძლავრე შეადგენს სრული სიმძლავრის მხოლოდ მცირე ნაწილს და იმას, რომ ის დროთა განმავლობაში ფაქტიურ დატვირთვის გაზრდის შესაბამისად იზრდება. მონაცემთა დაცვის ცენტრებისათვის ერთ-ერთი აქტუალური საკითხია მათი ელექტროენერგიით უწყვეტად მომარაგება მიწოდებული ნორმირებული ცვლადი დენის ხარისხის მაღალი მოთხოვნით. იმის გამო რომ ცვლადი დენის სამომხმარებლო ქსელში ხშირად არსებობს ხელშეშლები-ძაბვის ამოვარდნები, ძაბვის ვარდნები, ძაბვის სინუსოიდალური ფორმის მკვეთრი დამახინჯებები (ქსელის ძაბვის ამპლიტუდური მნიშვნელობა შეიძლება იყოს ნომინალურზე როგორც

რამდენადმე მეტი, ასევე ნაკლებიც) ყოველივე ეს უარყოფით გავლენას ახდენს აპარატურის უტყუარ მუშაობაზე და ასეთმა ხელშეშლებმა შესაძლებელია გამოიწვიოს ინფორმაციის ნაწილობრივი ან მთლიანი დაკარგვა. მონაცემთა დაცვის ცენტრები, როგორც ცნობილია, მოიხმარენ საკმაოდ დიდ სიმძლავრეს (5-200 კვტ–მდე) რაც გასათვალისწინებელია ელექტროენერგიის უწყვეტად მიწოდების მოწყობილობისა და აგრეგატების შერჩევისას. ამას სჭირდება ანალიზი და გამოსავლის ძიება - ისეთი ელექტრომომარაგების არჩევა, რომელიც აგვაცილებს ქსელში არსებულ ხელშეშლებს და უზრუნველყოფს მონაცემთა ცენტრებში ინფორმაციის დაცვის ხარისხის ამაღლებას. დასმული ამოცანის გადასაჭრელად გთავაზობთ ჩვენს მიერ შემოთავაზებულ მოწყობილობას [1,2] რომლის შემადგენლობაში შედის შემდეგი ძირითადი კვანძები: ასინქრონული სამფაზა ძრავი, რომელიც ლილვითა და მქნევარით მჭიდროდაა დაკავშირებული სამფაზა ელექტროგენერატორის ლილვთან, ხოლო ელექტროგენერატორი თავის მხრივ, ელექტრომაგნიტური მუფტის მეშვეობით დაკავშირებულია შიდაწვის ძრავის ლილვთან. ასეთი სქემა საშუალებას იძლევა მივიღოთ მძლავრი ელექტროკვების მოწყობილობა მუშაობს შემდეგნაირად: ქსელი 4 -დან სამფაზა ძაბვა ელექტროძრავა 1-ს მიეწოდება რელე 3-ის კომტაქტების საშუალებით (კონტაქტები აღნიშნულია 2-ით) , ირთვება ძრავი და გარკვეული დროის შემდეგ მისი ლილვის კუთხური სიჩქარე მიაღწევს ნომინალურ მნიშვნელობას (აჩქარდება ნომინალურ სიჩქარემდე- დაახლოებით 3000 ბრ./წთ.) ამ დროისათვის მართვის სქემა იმყოფება საწყის მდგომარეობაში: სიგნალები ელემენტ 19-ის შესასვლელებზე და გამოსასვლელებზე, აგრეთვე ზღურბლოვან ელემენტების 15 და 16 ისა და ერთვიბრატორ 24 -ის გამოსასვლელებზე, ტოლია „0—-ის, გასაღებები 17, 18, 25 და 37 გამორთულებია, რელე 3 გამორთულია, აღგზნების გრაგნილის 28 დამატებითი წრედი გამორთულია, ელექტრომაგნიტური მუფტა 7 განრთულია, შწძ 9 გამორთული, ამასთან, გამათბობელი ელემენტი 12, რომელიც იკვებება ქსელი 4-დან, და ტემპერატურის მარეგულირებელი 13

უზრუნველჰყოფენ შიდაწვის ძრავის სწრაფი გაშვების (ამუშავების) რეჟიმს. ძაბვის მარეგულირებელი 32 უზრუნველყოფს ძაბვის ნომინალური მნიშვნელობას სალტეებზე 30 ოპერატიული წრედების დატვირთვის ცვალებადობის პირობებში [1]. სამფაზა ქსელ 4 -ის ნებისმიერ ფაზაზე ძაბვის გარკვეულ მნიშვნელობამდე დაწევისას ამუშვდება შესაბამისი კომპარატორები 20-22 და ელემენტ „ან— -ის გამოსასვლელზე ფორმირდება სიგნალი , რომლის მნიშვნელობაა „1—. ამასთან, ირთვება ავტომატური ჩართვის ბლოკი და ძრავი 9 ჩაირთვება. ერთდროულად ჩაირთვება ერთვიბრატორი 24, ამასთან იხსნება გასაღები 25 და დამატებითი აღგზნების გრანილი რეზისტორ 27-ის გავლით უერთდება აკუმულატორულ ბატარეა 26-ს, ახორციელებს რა გენერატორ 6-ის სწრაფად აღგზნებას (ფორსირებას). ძაბვის სტაბილიზაცია სალტეებზე 30 ხორციელდება ძაბვის მარეგულირებელი 32-ით. ძრავის სიჩქარის გარკვეულ მნიშვნელობამდე დაწევისას ამუშავდება ზღურბლოვანი ელემენტი 16 და გასაღები 18 იხსნება, აშუნტებს რა რეზისტორ 27-ს. ამასთან იზრდება დენი აღგზნების დამატებით გრაგნილში 28, რაც უზრუნველჰყოფს ძაბვის შენარჩუნებას სალტეებზე 30 მოცემულ ზღვრებში. ძრავის სიჩქარე შემცირდება დაახლოებით 2950 ბრ/წთ- მდე. სიჩქარის შემცირება მოცემულ მნიშვნელობამდე ხორციელდება დროში, რომელიც აღემატება ძრავ 9-ს გაშვების დროს. როდესაც ძრავ 9-ს სიჩქარე (ლილვზე, რომელიც მიერთებულია მუფტა 7-თან) აღწევს დაახლოებით 3000 ბრ/წთ მნიშვნელობას, ამუშავდება ზღურბლოვანი ელემენტი 35 და —და-არა— ელემენტის 23 მეორე შესასვლელზე ფორმირდება ლოგ. „1— ის შესაბამისი სიგნალი. რამდენადაც განხილულ რეჟიმში ამ ელემენტის პირველ შესასვლელზე უკვე არსებობს ლოგ. 1-ის შესაბამისი ძაბვის დონე, მის გამოსასვლელზე ფორმირდება ნულოვანი სიგნალი. ამასთან, კონვერტორ 36 - ის გამოსასვლელზე სიგნალი ტოლია „1—-ის, და გასაღები 37 იხსნება, რთავს რა ელექტრომაგნიტური მუფტა 7-ის გრაგნილს. ეს უკანასკნელი ირთვება და გენერატორ 6-ის მამოძრავებელი (წამყვანი) ძალის გადაცემა ხორციელდება შწძ 9-სგან, რომლის ნომინალური კუთხური სიჩქარის

შენარჩუნდება ხდება მარეგულირებლ 11-ის მეშვეობით. ქსელ 4 ის ძაბვის აღდგენისას მოწყობილობა ავტომატურად გადადის საწყის ნორმალურ რეჯიმში. სალტე 30 -ზე დატვირთვის მნიშვნელოვანი შემცირებისას, ხდება ძრავის აჩქარება და თუ სიჩქარე აღემატება განსაზღვრულ მნიშნელობას, ამუშავდება ზღურბლოვანი ელემენტი 15. ამასთან გაიხსნება გასაღები 17 და ირთვება რელე 3, ხოლო მისი კონტაქტები 2 ძრავ 1-ს გამორთავენ ქსელ 4 დან. სიჩქარის ნომინალურ მნიშვნელობამდე შემცირებისას, ზღურბლოვანი ელემენტი 15 ბრუნდება საწყის მდგომარეობაში, გასაღები 17 იკეტება, რელე 3 განირთვება და მყარდება ნორმალური რეჟიმი [2]. ანალოგიური დანიშნულების ცნობილი მოწყობილობები - უწყვეტი კვების აგრეგატები დამატებით შეიცავენ ისეთ რთულ ბლოკს, როგორიცაა ჰიდროგადაცემის მქონე დამაკავშირებელი რგოლი სიჩქარის გადაცემის კოეფიციენტის ავტომატური რეგულირებით. მითითებული ჰიდროგადაცემის მუდმივი ენერგოდანახარჯები შეადგენენ საათში დაახლოებით 7კვტ-ს, ხოლო შემოთავაზებული მოწყობილობისა კი - არაუმეტეს 0,06კვტ.საათს. შემოთავაზებული მოწყობილობის ძირითად უპირატესობას წარმოადგენს სპეციალური დანიშნულების წრედების დიდი მოხმარებული სიმძლავრის გამომუშავების შესაძლებლობა, მოწყობილობის მიერ მოხმარებული სიმძლავის შემცირება და აგრეგატის კონსტრუქციის გამარტივება არსებულ ცნობილ მოწყობილობებთან შედარებით. შემოთავაზებულ მოწყობილობამ შეიძლება ჰპოვოს გამოყენება ელექტროსადგურებში, ქვესადგურებში, წევის ქვესადგურებში, ავტომატურ სატელეფონო სადგურებში, მეტროპოლიტენის სისტემებში, როგორც მძლავრი ოპერატიული დენის წყარო. ტემპერატურის და ერთი ჰაერის ფარდობითი ტენიანობის გამზომი სენსორი, ხოლო კონდიცირების აგრეგატების მუშაობის გამართულობაზე თვალთვალი ხდება ორი სპეციალური ციფრული გადამწოდის გამოყენებით. ორი ასეთი ციფრული გადამწოდი გამოყენებულ იქნება ხანძარარმოჩენის სისტემის ფუნქციონირების მონიტორინგისთვის. გარდა აღნიშნულისა საკუთრივ გაგრილების კარადებს გააჩნიათ მონიტორინგის ბლოკები, რომლითაც ხდება თვითოეული მათგანის მუშაობის პარამეტრების დეტალური

მონიტორინგი. აღნიშნული სისტემა ფუნქციონირებს შემდეგნაირად: სენსორებიდან ამა თუ იმ სიდიდის გაზომვის შედეგები გადაეცემა შეტანა–გამოტანის მოდულს, შემდეგ ეს ინფორმაცია თავს იყრის პროცესორულ ბლოკში, სადაც ხდება მიღებული ინფორმაციის კლასიფიკაცია და ერთიანი ინტერფეისის საშუალებით მისი გადმოცემა. პროცესორული ბლოკის ფუნქციაში ასევე შედის სხვადასხვა დარღვევის აღმოჩენის დროს ელექტრონული ფოსტით შეტყობინებების დაგზავნა წინასწარ გაწერილ მისამართებზე, ხოლო GSM მოდულის წყალობით იგივე შეტყობინებები ეგზავნება SMS სახით წინასწარ მითითებულ ოთხ აბონენტს. GSM მოდულის ფუნქციონირებისთვის აუცილებელია ე.წ. SIM ბარათი, რომელიც არ შედის კომპლექტაციაში; პროცესორულ ბლოკში სრულად არის რეალიზებული WEB/SNMP/SMTP ინტერფეისები, მისი ერთ–ერთი სამუშაო ეკრანის მაგალითი ნაჩვენებია Error! Reference source not found.–ზე ამ მონიტორინგის სისტემაში ასევე გაერთიანებულია RITTAL–ის წარმოების დაშვების კონტროლის სისტემაც. ეს სისტემა ფუნქციონირებს შემდეგნაირად: სენსორებიდან ინფორმაცია გადაეწოდება სენსორულ ბლოკებს, შემდეგ ის თავს იყრის პროცესორულ ბლოკში, სადაც ხდება ამ ინფორმაციის კლასიფიკაცია დახარისხება და ერთიანი WEB ინტერფეისის საშუალებით წარმოდგენა. მონიტორინგის ცენტრალური კონსოლის საშუალებით მოხდება რამოდენიმე პროცესორული ბლოკის გაერთიანება, ამასთან მას აქვს საშუალება მიუერთდეს ლოკალური მონიტორი მონაცემების ვიზუალურად წარმოდგენისთვის. ოთახში და მის გარეთ ტერიტორიაზე განთავსდება ტემპერატურის, ჰაერის ფარდობითი ტენიანობის და გაჟონვის სენსორები. (ნახ.35.). მათი განთავსების ადგილი განისაზღვრება პროექტის განხორციელებისას. დაცულ სასერვერო ოთახში განთავსდება სამი ცალი კვამლის.

სანქცირებული დაშვების სისტემა შედგება დაშვების კონტროლისა და ვიდეოთვალის სისტემებისაგან. მონაცემთა დაცვის ცენტრებში დაშვების კონტროლის სისტემებში გამოიყენება ბარათით გაღების სისტემა, კოდური საკეტით გაღების სისტემა, და სკანირების მეთოდით იდენტიფიცირების

შესაძლებლობების მქონე საკეტებით გაღების სისტემები. ასევე შესაძლებელია კომბინირებული მიდგომაც. დაშვების სისტემა რეალიზებულია კომპანია RITTAL–ისმიერ წარმოებულ CMC-TC–ის მეშვეობით, რომლის მართვა ხორციელდება ციფრული კლავიატურის საშუალებით ეს სისტემა ფუნქციონირებს შემდეგნაირად: ბარათების წამკითხველიდან ინფორმაცია გადაეცემა დაშვების ბლოკს, შემდეგ ის თავს იყრის პროცესორულ ბლოკში, სადაც ხდება ბარათის კოდის შემოწმება და კარის გაღებაზე ბრძანების გაცემა, ასევე ელექტრონული ფოსტით შეტყობინებების დაგზავნა წინასწარ გაწერილ მისამართებზე. დაშვების პროცესორულ ბლოკში სრულად არის რეალიზებული WEB/SNMP/SMTP ინტერფეისები; ბარათით გაღების სისტემაში, გასაღებად გამოიყენება როგორც უკონტაქტო, ასევე კონტაქტიანი მაგნიტური ბარათები, ბარათების წამკითხველი მონტაჟდება სასერვერო ოთახის შესასვლელ კართან . წამკითხველი ქსელის საშუალებით დაკავშირებული იქნება ცენტრალურ მართვის ბლოკთან, რომელშიც მოხდება მონაცემების დაგროვება გადაცემა სერვერზე დაინსტალირებული პროგრამული უზრუნველყოფისკენ. სასერვერო ოთახის კარზე მონტაჟდება სპეციალური ელექტრო მექანიკური საკეტი, რომელიც შეუნარჩუნებს არსებულ ანტი პანიკ გასასვლელ სახელურს თავის ფუნქციონალურ დანიშნულებას დაშვების სისტემა პროგრამულად მიერთებულია მონაცემთა დაცვის ცენტრის სერვერული პროგრამული უზრუნველყოფის ტექნოლოგიაზე, ამასთან შესაძლებელია პირდაპირი წვდომა დაშვების სისტემის ბლოკთან WEB ინტერფეისის დახმარებით. სისტემის გაფართოება, ანუ წამკითხველების დამატება ადვილადაა შესაძლებელი, ასევე ბარათების რაოდენობის გაზრდაც. მთლიანად დაშვების კონტროლი ინტეგრირდება RITTAL-ის მონიტორინგის სისტემასთან და მუშაობს მასთან ერთად, იმ შემთხვევაში თუ ეს უკანასკნელი არსებობს.

2.3. კიბერშეტევებისაგან დამცავი ინფრასტრუქტურის შექმნა

გარკვეული პერიოდის განმავლობაში, საზოგადოებრივი კეთილდღეობა და ეკონომიკური სტაბილურობა ეყრდნობოდა გადაცემის ქსელების მონაცემებისა და გამოთვლითი მომსახურების გამართულ მუშაობას, რომლის სანდოობის მაჩვენებელი საკმაოდ დიდი იყო. საერთო მოხმარების ინფორმაციული სისტემების ფუნქციონირებაზე დიდი გავლენა აქვს ისეთ ფაქტორებს, როგორებიც არის ინტერნეტზე შეტევა (attack), ფიზიკური ზემოქმედების შედეგად მიყენებული დარღვევები, პროგრამული და აპარატული უზრუნველყოფის მწყობრიდან გამოსვლა, ადამიანის როგორც მომხმარებლის მიერ მუშაობის პროცესში დაშვებული შეცდომები. ჩამოთვლილი ფაქტორები ნათლად აჩვენებს იმ გარემოებას, თუ რამდენად არის დამოკიდებული თანამედროვე საზოგადოება ინფორმაციული სისტემების სტაბილურ მუშაობაზე. მოცემულს ნათლად ასახავს კიბერუსაფრთხოების გერმანული სტრატეგია, კერძოდ: „კიბერსივრცეზე დაშვების უზრუნველყოფა, ასევე ინფორმაციის კონფიდენციალობა და სანდოობა კიბერსივრცეში გახდა ერთერთი მნიშვნელოვანი პრობლემა 21 - ე საუკუნეში. ამიტომ კიბერსივრცის დაცვა ხდება მთავარი ამოცანა სახელმწიფოს, ეკონომიკისა და საზოგადოების, როგორც ქვეყნის, ისე საერთაშორისო დონეზე

ევროკომისიის ზოგიერთ შეხვედრაზე2 არაერთხელ განიხილებოდა და ამჟამადაც აქტიურად განიხილება ქსელისა და ინფორმაციული უსაფრთხოების მნიშვნელობა. ამ მიზნით, ასევე აქტიური განხილვის საგანია ერთიანი ევროპული ინფორმაციული სივრცის შექმნა.

ევროკომისიის ბოლო შეხვედრებზე მიღებული ნორმატიული და სამართლებრივი აქტები3 ინფორმაციული ინფრასტრუქტურის (CII – Critical Information Infrastructure Protection) დაცვის შესახებ, გვთავაზობს პრაქტიკულ ზომებსა და რეგულაციებს ქსელების საერთო მოხმარების უსაფრთხოებისა და სანდოობის თაობაზე. კიბერუსაფრთხოება ხშირად განიხილება როგორც სახელმწიფო მნიშვნელობის სტრატეგიული პრობლემა, რომელიც ეხება საზოგადოების ყველა ფენას. კიბერუსაფრთხოების სახელმწიფო პოლიტიკა (NCSS - National Cyber Security Strategy) არის საშუალება, რომელიც ემსახურება სახელმწიფოს ინფორმაციული სისტემებისა და მთლიანად ინფრასტრუქტურის უსაფრთხოებისა და სანდოობის გაზრდის შესაძლებლობას, რომელიც ამავდროულად მაქსიმალურად ამცირებს რისკებს. კიბერუსაფრთხოების სტრატეგიაში გამოიყენება პრობლემისადმი მაღალი დონის მიდგომა, კერძოდ: გამოიყოფა სახელმწიფოს მთელი რიგი მიზნები, ამოცანები და პრიორიტეტები, რომლებიც აუცილებელია მოცემული დროის მონაკვეთში მისაღწევად. ფაქტიურად, სტრატეგია ეს არის მოდელი, რომელიც

საშუალებას იძლევა კიბერუსაფრთხოების საკითხების მოგვარებას ქვეყნის შიგნით.
ევროკავშირის წევრ - ქვეყნებში კიბერუსაფრთხოების უზრუნველყოფის გაუმჯობესებისა და კოორდინირებული მუშაობის, ასევე, საერთო პოლიტიკის შემუშავების მიზნით, შექმნილია სპეციალური სააგენტო European Union Agency for Network and Information Security – ENISA4.
ENISA ამუშავებს სპეციალურ სახელმძღვანელოს Good Practice Guide5, რომელიც წარმოადგენს ევროკავშირის წევრი ქვეყნების მხარდამჭერ დოკუმენტს მათი მხრიდან კიბერუსაფრთხოების სახელმწიფო პოლიტიკის შემუშავების მთავარ მისიაში. მოცემული სახელმძღვანელო ევროკავშირის თითოეული წევრი ქვეყნისთვის იძლევა რეკომენდაციებსა და არსებულ მოწინავე პრაქტიკას კიბერუსაფრთხოების სტრატეგიის შემუშავებასა და დანერგვაში.

წინამდებარე დოკუმენტში მოკლედ არის განხილული ევროკავშირის წევრი ქვეყნების კიბერუსაფრთხოებისა და ზოგადად ევროკავშირის ინტერნეტის უსაფრთხოების სტრატეგიები, მასთან დაკავშირებული საკითხები და არსებული ვითარება. საკითხის მიმართ დიდი ინტერესიდან გამომდინარე, ქვემოთ განხილულია ასევე შეერთებული შტატების, კანადისა და იაპონიის კიბერუსაფრთხოების სტრატეგიის ძირითადი მიმართულებები. დოკუმენტში ასევე მოცემული არის სტრატეგიების საერთო მახასიათებლები, განსხვავებები, დასკვნა, რეკომენდაციები და წარმოდგენილია საქართველოს კიბერუსაფრთხოების პოლიტიკისა და სტრატეგიის მიმართულებები.

კიბერშეტევებისაგან დაცვის უზრუნველსაყოფად კვლევების და ლაბორატორიული ცდების შედეგების შესაბამისად რეკომენდირებულია შმედეგი ტექნიკური ღონისძიებებისა და კონფიგურაციის უზრუნველყოფა რასაც ადასტურებს მითითებული კონფიგურაციის შემდგომ ჩატარებული ლაბორატორიული ცდა.

Secure Shell (SSH) არის პროტოკოლი, რომელიც უზრუნველყოფს დაშორებული მოწყობილობის დაცულ (შიფრირებულ) მართვად კავშირს. მართვადი კავშირისთვის SSH-ი ცვლის Telnet-ს. Telnet არის ძველი პროტოკოლი, რომელიც იყენებს დაუცველ, ღია ტექსტით გადაცემას შესვლის აუთენტიფიკაციის (მომხმარებლის სახელი და პაროლი) და ურთიერთმოქმედ მოწყობილობებს შორის მონაცემების გადაცემის დროს.

SSH იძლევა დაშორებული კავშირის უსაფრთხოებას ძლიერი შიფრირების უზრუნველყოფით, როდესაც მოწყობილობა არის ავტორიზებული (მომხმარებლის სახელი და პაროლი) და ასევე დაკავშირებულ მოწყობილობებს შორის მონაცემთა გადაცემის დროს. SSH-ს მინიჭებული აქვს TCP-ის 22 პორტი ნომერი, ხოლო Telnet-ს - TCP 23 პორტის ნომერი.
Catalyst 2960 კომუტატორზე SSH-ის ჩასართავად, კომუტატორი უნდა იყენებდეს IOS სისტემის იმ ვერსიას, რომელიც შეიცავს დაშიფვრის ფუნქციებს და შესაძლებლობებს. იმის სანახავად თუ რომელი IOS ოპერაციული სისტემაა გაშვებული, გამოიყენეთ show version ბრძანება კომუტატორზე. ასევე ამ ბრძანებით შეგვიძლია ვნახოთ ფაილის სახელი, რომელიც მოიცავს „K9", შიფრაციის მხარდაჭერის ფუნქციებისა და შესაძლებლობების კომბინაციას კონფიგურირებული უნიკალური სახელით და სწორი ქსელის კავშირის პარამეტრებით. პირველი ეტაპი. SSH მხარდაჭერის შემოწმება. გამოიყენეთ show ip ssh ბრძანება, კომუტატორზე SSH მხარდაჭერის შესამოწმებლად. თუ კომუტატორზე არ არის გაშვებული ის IOS ოპერაციული სისტემა, რომელიც მხარს უჭერს შიფრაციის ფუნქციებს, მოცემული ბრძანება სისტემისთვის იქნება გაუგებარი.

მეორე ეტაპი. IP დომეინის კონფიგურაცია დააკონფიგურეთ ქსელის IP დომეინის სახელი ip domain-name domain-name ბრძანების გამოყენებით, საერთო კონფიგურაციის რეჟიმში. 3.2.5.2,1 სურათზე domain-name მნიშვნელობა არის cisco.com. მესამე ეტაპი. RSA წყვილი გასაღების გენერაცია არა ყველა ვერსიის IOS ოპერაციულ სისტემაში, ნაგულისხმევად SSHv2-ში, და SSHv1-ში არის უსაფრთხოების ნაცნობი ხარვეზები. SSH ვერსია 2-ის კონფიგურაციისთვის გაუშვით ip ssh version 2 საერთო კონფიგურაციის რეჟიმის ბრძანება. RSA წყვილი გასაღების გენერაცია ავტომატურად რთავს SSH-ს. გამოიყენეთ crypto key generate rsa საერთო კონფიგურაციის რეჟიმის ბრძანება კომუტატორზე SSH სერვერის ჩასართავად და RSA წყვილი გასაღების გენერაციისთვის. როდესაც ხდება RSA გასაღებების გენერაცია, ადმინისტრატორმა უნდა მიუთითოს მოდულის სიგრძე. Cisco იძლევა რეკომენდაციას, რომ მინიმალური

მოდულის სიგრძე იყოს 1024 ბიტი (იხილეთ მარტივი კონფიგურაცია 3.2.5.1 სურათზე). რაც მეტია მოდულის სიგრძე, მივიღებთ მეტ უსაფრთხოებას, მაგრამ მის გენერაციას და გამოყენებას მიაქვს დიდი დრო. SSH სერვერს შეუძლია მომხმარებლების აუთენტიფიკაცია ლოკალურად ან აუთენტიფიკაციის სერვერის გამოყენებით. ლოკალური აუთენტიფიკაციის მეთოდის გამოყენებისთვის შექმენით მომხმარებლის სახელისა და პაროლის წყვილი username username secret password საერთო კონფიგურაციის რეჟიმის ბრძანების გამოყენებით. მაგალითზე admin მომხმარებელს მინიჭებული აქვს ccna პაროლი. მეხუთე ეტაპი. vty ხაზების კონფიგურაცია ჩართეთ SSH პროტოკოლი vty ხაზებზე transport input ssh ხაზის კონფიგურაციის რეჟიმის ბრძანების გამოყენებით. Catalyst 2960 კომუტატორს აქვს vty ხაზების ზღვარი 0-დან 15-მდე. მოცემული კონფიგურაცია კრძალავს არა-SSH (Telnet-ის ჩათვლით) შეერთებებს და შეზღუდვას უწესებს კომუტატორს, რომ დაეთანხმოს მხოლოდ SSH კავშირებს. გამოიყენეთ line vty საერთო კონფიგურაციის რეჟიმის ბრძანება და შემდეგ login local ხაზის კონფიგურაციის რეჟიმის ბრძანება, რათა მოთხოვნილ იქნას ლოკალური აუთენტიფიკაცია SSH კავშირებისთვის, ლოკალურ მომხმარებელთა მონაცემთა ბაზიდან ნაგულისხმევად SSH მხარს უჭერს ორივე ვარიანტს: ვერსია 1 და ვერსია 2. როცა მხარდაჭერილია ორივე ვერსია, ეს ნაჩვენებია show ip ssh ბრძანების გაშვების შედეგზე, როგორც მხარდაჭერილი 1.99 ვერსია. ვერსია 1 ცნობილია თავისი ხარვეზებით, ამიტომ რეკომენდებულია მხოლოდ ვერსია 2-ის ჩართვა. ჩართეთ SSH ვერსია 2 ip ssh version 2 საერთო კონფიგურაციის ბრძანების გამოყენებით.

3.2.5.3 SSH-ის შემოწმება კომპიუტერზე, SSH კლიენტი, PuTTY-ს ჩათვლით, გამოიყენება SSH სერვერთან დასაკავშირებლად. მაგალითისთვის სურათებზე, მომართულია შემდეგი: • SSH ჩართულია S1 კომუტატორზე

• VLAN 99 (SVI) ინტერფეისი 172.17.99.11 IP მისამართით S1 კომუტატორზე

• PC1 IP მისამართით 172.17.99.21 3.2.5.3.1 სურათზე PC1 კომპიუტერი ინიციალიზაციას უკეთებს SSH შეერთებას, S1 კომუტატორის SVI VLAN IP მისამართთან. ქსელის წარმადობა მნიშვნელოვანი ფაქტორია ორგანიზაციის

პროდუქტიულობაში. ერთ-ერთი ტექნოლოგია, რომელიც გამოიყენება ქსელის წარმადობის გასაზრდელად არის დიდი ფართომაუწყებლობითი დომენების დაყოფა პატარა ნაწილებად. როგორც წესი, მარშრუტიზატორები ბლოკავენ ფართომაუწყებლობით ტრაფიკს ინტერფეისზე. ამასთან, მარშრუტიზატორებს აქვთ შეზღუდული რაოდენობის ლოკალური ქსელის (LAN) ინტერფეისები. მარშრუტიზატორის მთავარი როლი არის ინფორმაციის გადატანა ქსელებს შორის, და არ უზრუნველყოფს საბოლოო მოწყობილობების ქსელთან წვდომის საშუალებას.

ლოკალურ ქსელში წვდომის უზრუნველყოფა, როგორც წესი ეკუთვნის წვდომის დონის კომუტატორს. მსგავსად მესამე დონის მოწყობილობისა, ვირტუალური ლოკალური ქსელის (VLAN) შექმნა შესაძლებელია მეორე დონის კომუტატორზეც, ფართომაუწყებლობითი დომენების ზომების შესამცირებლად. ვირტუალური ლოკალური ქსელები როგორც წესი ჩართულნი არიან ქსელის დაგეგმვაში, რაც აადვილებს ორგანიზაციის მიზნების განხორციელებას ქსელთან მიმართებაში. ვირტუალური ლოკალური ქსელები ძირითადად გამოიყენება კომუტირებულ ლოკალურ ქსელებში, მაგრამ ვირტუალური ქსელების თანამედროვე რეალიზაცია საშუალებას აძლევს მათ იმუშაონ MAN და WAN ქსელებშიც. მომხმარებლის პროდუქტიულობა და ქსელთან ადაპტაცია არის აუცილებელი ბიზნესის ზრდისა და წარმატებისთვის. VLAN-ები აადვილებს ქსელის შექმნას, მთელი ორგანიზაციის მხარდაჭერისთვის. ვირტუალური ლოკალური ქსელების გამოყენების მთავარი უპირატესობებია:

უსაფრთხოება - ჯგუფებს, რომელთაც აქვთ მნიშვნელოვანი ინფორმაცია, გამოყოფილნი არიან დანარჩენი ქსელის ნაწილისაგან, რაც ამცირებს არსებობს განსხვავებული ტიპის VLAN-ების მთელი რიგი, რომელიც გამოყენებულია თანამედროვე ქსელებში. ზოგიერთი VLAN-ის ტიპი განსაზღვრულია ტრაფიკის კლასებით. სხვა ტიპის VLAN-ები განისაზღვრებიან კონკრეტული ფუნქციებით, რომლითაც ისინი ემსახურებიან ქსელს.

მონაცემთა VLAN მონაცემთა VLAN არის VLAN, რომელიც დაკონფიგურებულია მომხმარებლის მიერ დაგენერირებული ტრაფიკის გადასაგზავნად. VLAN ქსელს, რომელსაც გადააქვს ხმა ან მართავს ტრაფიკს, არ იქნება მონაცემთა VLAN-ის ნაწილი. ეს არის ჩვეულებრივი პრაქტიკა, რათა გაყოფილ იქნას ხმა და მართვის ტრაფიკი მონაცემთა ტრაფიკისაგან. მონაცემთა VLAN-ს ზოგჯერ მოიხსენიებენ როგორც მომხმარებლის VLAN-ს. მონაცემთა VLAN გამოიყენება ქსელის დასაყოფად მომხმარებლების ჯგუფებად ან მოწყობილობებად. ნაგულისხმევი VLAN კომუტატორის ყველა პორტი ხდება ნაგულისხმევი VLAN-ის ნაწილი მას შემდეგ რაც კომუტატორის საწყისი ჩატვირთვა გაუშვებს ნაგულისხმევ კონფიგურაციას. კომუტატორის პორტები, რომლებიც მონაწილეობენ ნაგულისხმევ VLAN-ში, იგივე ფართომაუწყებლობითი დომეინის ნაწილი არიან. ეს საშუალებას აძლევს ნებისმიერ მოწყობილობას, რომლებიც შეერთებულნი არიან კომუტატორის ნებისმიერ პორტთან, დააკავშიროს სხვა მოწყობილობები სხვა კომუტატორის პორტებთან. Cisco კომუტატორებისთვის ნაგულისხმევი VLAN არის VLAN 1. 3.3.4.1 სურათზე ნაგულისხმევი კონფიგურაციით მართვად კომუტატორზე გაშვებულია show vlan brief ბრძანება. აღსანიშნავია, რომ ნაგულისხმევად ყველა პორტი მიკუთვნებულია VLAN 1-ზე. მიღებულია მრავალი VLAN-დან (დანიშნული ტრაფიკი), ასევე ტრაფიკს, რომელიც არ მოდის VLAN-დან (დაუნიშნავი ტრაფიკი). 802.1Q trunk პორტი განათავსებს დაუნიშნავ ტრაფიკს ადგილობრივ VLAN-ზე, რომელიც ნაგულისხმევად არის VLAN 1.

საუკეთესო პრაქტიკაა, რომ დაკონფიგურდეს ადგილობრივი VLAN-ი, როგორც გამოუყენებელი VLAN-ი, რომელიც განსხვავდება VLAN 1-სა და სხვა VLAN-ებისგან. ფაქტობრივად ის არ არის გამოუყენებელი ფიქსირებული VLAN-ის გამოსაყოფად, რათა შეასრულოს ადგილობრივი VLAN-ის როლი ყველა trunk პორტისთვის, კომუტირებულ დომეინში.

მართვადი VLAN მართვადი VLAN არის ნებისმიერი VLAN, რომელიც დაკონფიგურებულია კომუტატორის მართვის შესაძლებლობებზე წვდომისთვის. ნაგულისხმევად VLAN 1 არის მართვადი VLAN-ი. მართვადი

VLAN-ის შესაქმნელად, კომუტატორის ვირტუალური ინტერფეისი (SVI), რომლის VLAN-საც მინიჭებული აქვს IP მისამართი და ქვექსელის ნიღაბი, საშუალებას აძლევს კომუტატორს იყოს მართული HTTP, Telnet, SSH ან SNMP-ს საშუალებით. იმის გამო, რომ Cisco კომუტატორების სტანდარტულ კონფიგურაციაში VLAN 1 არის ნაგულისხმევი VLAN-ი, VLAN 1 შეიძლება იყოს ცუდი არჩევანი მათვადი VLAN-ისთვის. ადრე, მართვადი VLAN-ი 2960 კომუტატორისთვის იყო მხოლოდ ერთი აქტიური SVI. Catalyst 2960 სერიის კომუტატორების Cisco IOS-ის 15.x ვერსიებში, შესაძლებელია გვქონდეს ერთზე მეტი აქტიური SVI. Cisco IOS 15.x-ით, კონკრეტული აქტიური SVI, რომელიც განკუთვნილია დაშორებული მართვისთვის, უნდა იყოს დოკუმენტირებული. სანამ თეორიულად კომუტატორს შეუძლია ჰქონდეს ერთზე მეტი მართვადი VLAN, ერთზე მეტის არსებობა ზრდის ქსელური თავდასხმების რისკს. ყველა პორტი მინიჭებულია ნაგულისხმევ VLAN 1-ზე. ადგილობრივი VLAN-ი აშკარად არაა მინიჭებული და სხვა VLAN-ებიც არაა აქტიური. მაშასადამე ქსელი შექმნილია ადგილობრივი VLAN-ით, ისე როგორც მართვადი VLAN-ი. ეს განიხილება, როგორც უსაფრთხოების რისკი.

მეორე თავის დასკვნები

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

თავი III. საბარათე დაცვის სისტემების შემუშავება

ამ თავში შემუშავებულია ელექტრონული ანგარიშსწორების საბარათე სისტემა, რომელიც შედგება როგორც ქსელური და სასერვერო ინფრასტრუქტურისაგან ასევე საბარათე წამკითველი და ორ მაგნიტურველიანი სისტემის ფუნქციონირებისათვის საჭირო კომპონეტებისაგან, განხილულია ორ დონიანი სისტემის უპირატესოსბები და შემოთავაზებულია უსაფრთხოების გაუმჯობესების საშუალებები ავტორიზაციისა და შიფრაციის განსხვავებული გაუმჯობესებული მეთოდების გამოყენებით

3.1. ორ მაგნიტურ ზოლიანი სისტემა და მონაცემთა ბაზების ორგანიზება ორდონიანი ავტორიზაციის შემთხვევაში

მოგეხსენებათ ელექტრონული გადახდის სისტემებს ფართო გამოყენება გააჩნია, განსაკუთრებით განვითარებულ ქვეყნებში როგორებიც არის გერმანია, შვეიცარია, საფრანგეთი ამერიკის შეერთებული შტატები და სხვა სახელმწიფოები, მათ გამოყენების აუცილებლობას ვაწყდებით ყოველდღიურ ცხოვრებაში: მეტრო, ავტობუსი, აეროპორტი, მაღაზია და სხვადასხვა ინტერნეტ კომერციულ ვებ გვერდებზე ცხადია გადახდის მეთოლოგია და სისტემა ერთნაირი ვერ იქნება ამ მცირეოდენ ჩამონათვალშიც, სწორედ ბაზრის მრავალფეროვნებამ სპეციფიკამ და სირთულეებმა წარმოაჩინეს ელექტრონული გადახდის სხვადასხვა პრინციპებისა და მეთოდოლოგიის ჩამოყალიბება, რასაც თან ახლავს რისკები ოპერირების დროს წარმოქმნილ უზუსტობებისა და შეცდომების გაუთვლისწინებლობით გამოწვეული დანაკარგების. სწორედ ამ რისკების შესწავლა შეფასება გახლავთ ერთ-ერთი უმთავრესი პრიორიტეტი ამ სირთულეებისა და პრობლემების გადაჭრის გზაზე, რაც შეეხება უკვე არსებულ ელექტრონული გადახდის მეთოდს, ალბათ გაგიკვირდება და

ელექტრონულმა სისტემამ ჩვეულებრივი ქაღალდის ბილეთიც კი ციფრულ გადახდის სისტემაში მოაქცია მაგალითისათვის განვიხილოთ, გერმანიის მიწისქვეშა სალიანდაგო ტრანსპორტის მმართველი კომპანიის დირექტორის კომენტარი რომელიც აღნიშნავს, რომ თანამედროვე ტექნოლოგიებმა მნიშვნელოვანდ გაამარტივა მათი ოპერირება, რამაც მათი შემოსავლის ზრდას და ეფექტურად მუშაობის ორგანიზიებას შეუწყო ხელი თუმცა აქვე აღნიშნავს იმ ფაქტს, რომ კიდევ არსებობს რიგი ტექნიკური საკითხები რომლებიც საჭიროებს დახვეწასა და დაზუსტებას კერძოდ სადებეტო და საკრედიტო ბარათებით გადახდის პროცესი მათთვის სულაც არ არის მომგებიანი და აღნიშნავენ რომ მათი შემოსავლის ერთ ნახევარი პროცენტი გაურკვეველი მიმართულებით არის გაფლანგული, რასაც ე.წ ჰაკერებს აბრალებენ ამონარიდი Simon Nachnames ის გაზეთ Suddeutsche Zeitung -თან მიცემულული ინტერვიუდან (2013 წლის 14 ოქტომბერი).

პროქსიმიტი საბარათე და საბილეთე სისტემა

უკონტაქტო გადახდის სისტემა, საკრედიტო და სადებეტო ბარათები, SmartCard ე.წ ჭკვიანი ბარათი და ასევე სხვა მოწყობილობები რომლებიც უზრუნველყოფენ უსაფრთხო გადახდის მეთოდს რადიო სიხშირეების გამოყენების საშუალებით, აღნიშნული ტექნოლოგია მოხსენიებულია როგორც პროქსიმიტი გადახდის სისტემა.

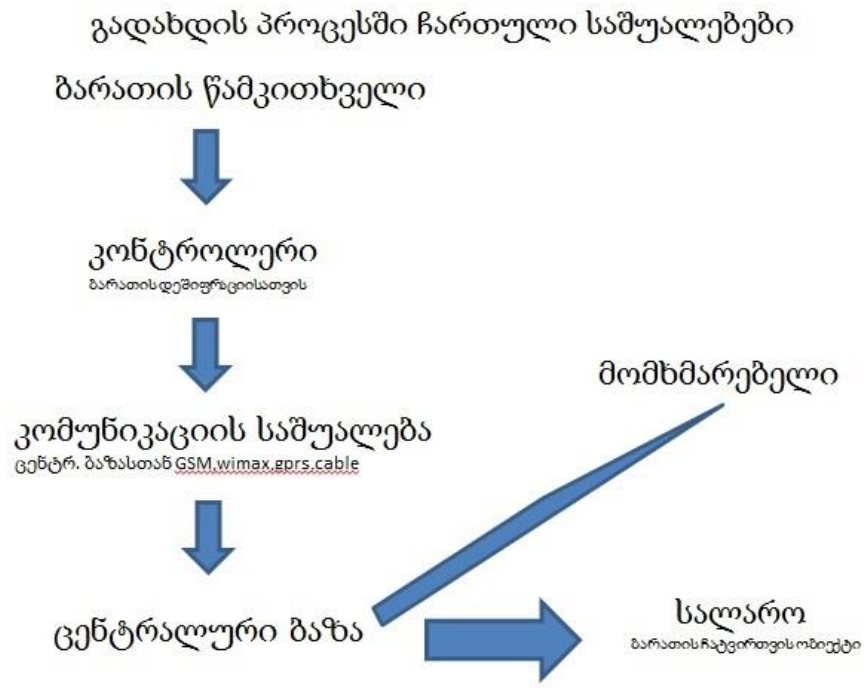
სანამ აღნიშნულია მიმართულების ქვე ტიპებს განვიხილავდეთ მანამდე

ორიოდე სიტყვით შევეცდი წარმოდგენა შეგიქმნათ აღნიშნულ ტექნოლოგიაზე. აღნიშნული ტიპის ბარათებში ჩადებულია ჩიპი, რომელიც დაშიფრულია 16 ბიტიანი კოდირების სისტემით და აღნიშნულ ინფორმაციას წამკითხველ მოწყობილობას გადასცემს მასშივე არსებული ანტენის საშუალებით, აღნიშნული სისტემით რეალიზაცია საქართველოში დიდი ხნის წინ დაიწყო, სისტემა პირველად საქართველოს ბანკმა დანერგა რომელმაც უსაფრთხოების უზრუნველსაყოფად გარკვეული მეთოდები შეიმუშავა მაგლითად ტრანზაქციის შესრულება ანუ პირადი ბარათიდან თანხის მოხსნა შესაძლებელი გახადა ე.წ პროქსიმიტი სისტემით არა უმეტეს ოცი ლარის ოდენობისა ერთი ოპერაციის დროს ყურადსაღებია ის ფაქტიც რომ აღნიშნული მეთოდი მათი მოგონილი არ არის მზგავსი ტიპის შეზღუდვებს იყენებენ სხვა ქვეყნებიც როგორებიც არის ამერიკის შეერთებული შტატები ოცდახუთი დოლარი, ავსტრალია ასი დოლარი, ახალი ზელანდია ოთხმოცი დოლარი ხოლო ევრო ზონის ქვეყნები ოცდა ხუთი ევროთი შემოიფარგლენ, ჩამოთვლილი ქვეყნების თანხობრივი ლიმიტები ერთეული ოპერაციის დროს ცხადყოფს იმ ფაქტს რომ აღნიშნული ტექნოლოგიასა თუ სისტემაში აღინიშნება ხარვეზი ოპერირების ან სისტემური უზრუნველყოფის კუთხით, აღნიშნული ხარვეზი ვერ აიხსნება იმ ფაქტორით, რომ შესაძლოა ანგარიშზე თანხა არ იყოს ან რაიმე მზგავსი ტიპის სხვა ფაქტორით, მისი ერთადერთი მიზეზი არის არასაიმედო ტექნოლოგია რაც საერთოდ საეჭვოს ხდის მის არსებობას, განვითარებული ქვეყნების მაგალითი სწორედ ამ მოსაზრების დასასაბუთებლად არის მოყვანილი, ხოლო რაც შეეხება აღნიშნული ტექნოლოგიის სიღრმისეულად სამეცნიერო კუთხით შესწავლას, ამისათვის საჭიროა გარკვეული ტიპის აპარატურული და პროგრამული უზრუნველყოფით მოწყობილი ლაბორატორია რომელიც ხელს შეუწყობს დარგის სიღრმისეულ შესწავლას ლაბორატორიული ექსპერიმენტების შედეგების შესწავლის საფუძველზე, სანამ საკუთარ ექსპერიმენტების შესწავლა შესრულებას დავიწყებდი მანამდე გავეცანი საერთაშორისო გამოცდილებას, მათ მოსაზრებებებსა და ლაბორატორიული კვლევების

შედეგებს რის შემდეგაც დავიწყე დამოუკიდებელი კვლევების ჩატარება რის შესახებაც შემდეგში უფრო ვრცლად და დეტალურად წარმოგიდგენთ შედეგებსა და დასკვნებს.

საბარათე სისტემები გარდა იმისა, რომ გამოირჩევა ორი ძირითადი ტექნოლოგიით როგორიც არის მაგნიტური და ჩიპიანი ან პროქსიმითი ასევე ხასიათდება ორი ძირითადი თვისებით online და offline პირველი გულისხმობს სისტემის მინდინარე რეჟიმში მუშაობას, კერძოდ საბარათე სისტემა დაკავშირებულია ცენტრალურ ბაზასთან დროის ნებისმიერ მომენტში რაც გულისხმობს სისტემის სინქრონულ მუშაობას, აღნიშნული სისტემის მომსახურება გაცილებით მეტ დროის რესურსსა და მომსახურე პერსონალის საჭიროებას მოითხოვს რადგან მომხმარებელი, ბარათის წამკითხველი, ბარათი, ცენტრალური სერვერი და კომუნიკაციის საშუალება ერთმანეთთან კავშირს არ წყვეტენ ეს ერთის მხრივ კარგია იმ თვალსაზრისით რომ ტრანზაქციის შესრულება ხდება ცოცხალ რეჟიმში და რიგი უსაფრთხოების საკითხები აქედან გამომდინარე უფრო მოწესრიგებულია ვიდრე offline რეჟიმში, რამ განაპირობა ამ რეჟიმის არსებობა? რას გულისხმობს და რა უპირატესობები გააჩნია? პირველ რიგში დაივიწყებ იქიდან რომ აღნიშნული მეთოდის არსებობა მატერიალურ ტექნიკური უზრუნველყოფის პრობლემებმა გამოიწვია როგორც დასაწყისში მოგახსენეთ ონლაინ რეჟიმი ითვალისწინებს და მოითხოვს უწყვეტ კომუნიკაციას რაც არც თუ ისე იაფი და მარტივი მისაღწევია ზოგიერთ შემთხვევაში, მაგალითად ავტობუსში მეტროში ან თვითმფრინავში რა თქმა უნდა აღნიშნულ ობიექტებზე შესაძლებელი ინტერნეტის არსებობა მაგრამ გასათვალისწინებელია, სადგურებისა და ავტობუსების რაოდენობა მათი ე.წ უწყვეთ ქსელში ჩართვა მნიშვნელოვნად გააძვირებდა ტრანსპორტირების ღირებულებას სწორედ ამიტომ მოიფიქრეს შერეული მეთოდი რომელიც უზრუნველყოფს კომუნიკაციის დამყარებას მხოლოდ დროის გარკვეულ მომენტში და ადგილას, ამ შემთხევაში პირველი მიმართულება რომელიც გულისხმობდა კლიენტის მუდმივ კავშირსა და ინფორმაციული მიმოცვლის რეჟიმს საინფორმაციო ბაზასთან

ჩანაცვლდა მორიგეობის მეთოდით, კერძოდ ოფლაინ რეჟიმში, ე.წ კონტროლერი მოიცავს მეხსიერებას რომელიც სინქრონიზაციას აკეთებს განსაზღვრულ დაგეგმილ დროში ცენტრალურ ბაზასთან რაც უსაფრთხოების კუთხით ყოვლად მიუღებელია აღნიშნულ მეთოდს იყენებს მეტრომანი საქართველოში არსებული საბარათე გადახდის სისტემის კომპანია რომელიც უზრუნველყოფს თბილისის ავტობუსებისა და მეტროს გადახდის სისტემის მომსახურებას, იმისათვის რომ მუშაობის პრინციპი უფრო ნათელი და ეფექტურად აღსაქმელი გახდეს წარმოგიდგენთ ნახაზს 1.0



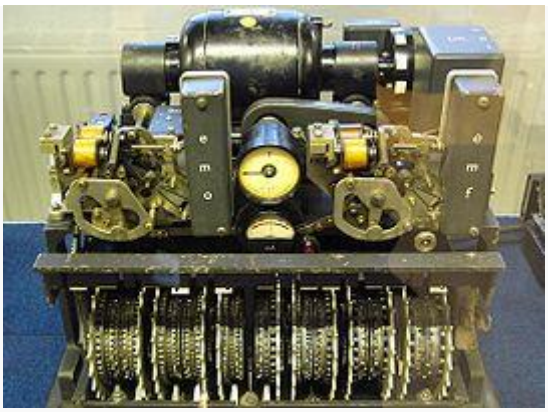
აღნიშნული პროცესი ვფიქრობ ცხადყოფს დროული კომუნიკაციის არსებობის აუცილებლობას, ოფლაინ შემთხვევაში ძალიან მარტივია ბარათის გაყალბება რადგან მას გადახდის მომენტში კავშირი ცენტრალურ ბაზასთან არ გააჩნია სწორედ ამიტომ შესაძლებელია, მოხდეს უკვე დაშიფრული ბარათის კლონირება რამოდენიმე ეგზემპლარად რაც არ მოითხოვს დაშიფრული ინფორმაციის დეშიფრაციას რადგან აღნიშნულ პროცესში ჩადებული არ არის ავტორიზაცია, სწორედ ამიტომ შესაძლებელი მოხდეს ბარათის რამოდენიმეჯერ გამოყენება რის დაცვის მექნიზმიც

აღნიშნულ სისტემას სამწუხაროდ არ გააჩნია, ვინაიდან ერთდროულად მიმართულ ოფლაინი ბაზებს არ აქვთ სინქრონიზაციის შესაძლებლობა ამ შემთხვევაში, შესაძლებელია მოხდეს თანხის არასანქცირებული გადინება ანგარიშებიდან სწორედ ამიტომ გახლავთ აღნიშნული მეთოდი ნაკლებად თანამედროვე და ნაკლებად უსაფრთხო თუმცა სწრაფი და კომფორტული.

მაგნიტურ ველიან ბარათებს რაც შეეხება მათი ტექნოლოგია სრულიად განსხვავებულია ჩამოთვლილი სისტემებიდან მასზე შესაძლებელია ჩაიტვირთოს რამოდენიმე დონის ლეირი რომლებზედაც ინდივიდუალურად მოხდება მაიდენტიფიცირებელი ინფორმაციის ჩაწერა და დაშიფვრა სხვადასხვა მეთოდებით, მნიშვნელოვანია შიფრაციის სწორი მეთოლოგიის არჩევა, ასევე გასათვალისწინებელია თუ კონკრეტულად ბიზნესის რომელ სფეროს უნდა მოემსახუროს არნიშნული გადახდის სისტემა, ბიზნესის ინდივიდუალურობიდან და დატვირთვიდან გამომდინარე უნდა შეირჩეს შესაბამის სისტემა რომელშიც გათვალისწინებული და დაგეგმილი იქნება დაყოვნების დრო, არის შემთხვევები, როდესაც ბიზნესის მფლობელმა შესაძლოა იცოდეს მისი გადახდის სისტემის ხარვეზები მაგრამ სულაც არ ფიქრობდეს მის გამოსწორებას მაგალითისთვის მოვიყვან ერთ-ერთ საკონცერტო დარბაზის ორგანიზატორს რომელმიც ბილეთების სისტემის არჩევის დროს თავიდანვე ფლობდა ინფორმაციას იმის შესახებ რომ სამი დღის განმავლობაში შესაძლებელი იქნებოდა მისი ბილეთების გაყალბება, მან ამ კონკრეტულ შემთხვევაში კონცერტის წინა დღეს დაიწყო ბილეთების გაყიდვა, როდესაც

გადახდის სისტემას ვირჩევთ ასევე უნდა გავითვალისწინოთ მისი ფიზიკური უსაფრთხოებაც რადგან ხშირ შემთხვევაში შესაძლოა არასწორად არჩეული სისტემა ადვილად დაზიანდეს. მაგალითისათვის მაგნიტურ ველიანი ბარათები სწორედ მათ რიცხვს მიეკუთვნებიან, მაგნიტური ველში არსებუული ინფორმაცია ადვილად შეიძლება წაიშალოს მაგნიტის ზემოქმედების დროს, მზის სხივით, მობილური ტელეფონით და კიდევ სხვა მრავალი ადვილად მისაღწევი ფიზიკური ზემოქმედების შედეგად, აქვე აღსანიშნავია ის ფაქტი, რომ მაგნიტურ ველში არსებული ინფორმაციის დუბლირება გაცილებით უფრო მარტივია ვიდრე სხვა დანარჩენ სისტემებში, ამიტომ ავტორიზაციის გარეშე ეს სისტემაც მოუქნელია, რომელსაც რამოდენიმე წლის წინ ბანკებიც კი იყენებდნენ, ასევე აღსანიშნავია ისიც რომ მაგნიტურ ზოლში ინფორმაციის მოთავსებაც სირთულეს წარმოადგენს, კერძოდ ველი შედგენილია თორმეტი ქვედონისაგან, რომელთაგან არცერთი არ არის თავსებადი თანამედროვე შიფრაციის მეთოდებთან.

კრიპტოგრაფია



გერმანული კრიპტოგრაფიული დანადგარი<u>ლორენცის მანქანა</u>, გამოიყენებოდა <u>მეორე მსოფლიო ომის</u> დროს ყველაზე გასაიდუმლოებული შეტყობინების<u>შიფრაციისთვის</u>

კრიპტოგრაფია (წარმოიშვა <u>ბერძნული</u> სიტყვებიდან κρυπτός „კრიპტოს“ — *ფარული*, და ზმნიდან γράφω „გრაფო“ — *წერა*, ანუ *ფარული წერა*) — მეცნიერება ინფორმაციის დაფარვის შესახებ. კრიპტოგრაფია განიხილება,

როგორც მათემატიკისა და კომპიუტერული მეცნიერებების განაყოფი, და მჭიდროდ დაკავშირებულია მეცნიერების ისეთ დარგებთან, როგორებიცაა ინფორმაციის თეორია, კომპიუტერული უსაფრთხოება და ინჟინერინგი დღესდღეობით იგი გამოიყენება ტექნოლოგიურად განვითარებულ სფეროებში, როგორიცაა: საკრედიტო ბარათები, კომპიუტერული პაროლები, ელექტრონული კომერცია და მრავალი სხვა. კრიპტოგრაფიული სისტემა ყოველთვის გულისხმობს 2 ან მეტ მონაწილეს, „გამგზავნს“ და „მიმღებს“, რომელთაც სურთ ერთმანეთს გადასცენ რაიმე სახის ინფორმაცია, ისე რომ ამ სისტემის გარეშე პირმა ვერ შეძლოს ამ ინფორმაციის მოპოვება. (კერძო შემთხვევებში მონაწილე შეიძლება იყოს ერთი პირი, რომელსაც სურს მოახდინოს ინფორმაციის საიმედოდ შენახვა, ანუ ინფორმაცია გადასცეს თავის თავს, ოღონდ მომავალში). თვითონ გადასაცემ ინფორმაციას ეწოდება ღია ტექსტი. ინფორმაციის სახეცვლილებას ისე, რომ დაფარულ იქნას მისი აზრი, შიფრაციას უწოდებენ, უკუპროცესს — დეშიფრაციას, მიღებულ შედეგს — შიფროტექსტს, ხოლო შიფრაცია/დეშიფრაციის ალგორითმს — შიფრს. ეს პროცესი უმეტეს შემთხვევაში დამოკიდებულიაგასაღებზე. ეს არის საიდუმლო პარამეტრი, რომელიც ცნობილია მხოლოდ ურთიერთმოკავშირე მხარეებისათვის. შიფრები გასაღების გარეშე უსარგებლოა, რადგან არსებობს მათი გატეხვის ტრივიალური ხერხები. კრიპტოსისტემა წარმოადგენს შიფრის, ყველა შესაძლო ღია ტექსტის, შიფროტექსტის და გასაღების ერთობლიობას. კრიპტოგრაფიული პროტოკოლები წარმოადგენენ წესების ერთობლიობას, რომლებიც სრულდება კრიპტოგრაფიული სისტემის მონაწილეების მიერ, თანამიმდევრობით და უპირობოდ.

ტერმინი „კოდი“ კრიპტოგრაფიაში აღნიშნავს ჩვეულებრივი ტექსტის ნაწილის შეცვლას კოდურის სიტყვით ან ფრაზით (მაგ. „ხმალი“ შესაძლოა აღნიშნავდეს „გაანადგურე მტერი“). კოდები სერიოზულ კრიპტოგრაფიაში აღარ გამოიყენება რადგან, მისი გამოყენება მოითხოვს, მონაცემთა გადაცემამდე მოკავშირეთა შორის ყველა შესაძლო მონაცემი შესაბამისი

სიტყვებით კოდირებული და ურთიერთშეთანხმებული იქნას . ამავე დროს ყოველთვის არსებობს მონაცემთა სიმრავლე, რომელთათვისაც შესაბამისი კოდური სიტყვა ჯერ არ შეთანხმებულა. შიფრები უფრო მოსახერხებელია და ამავე დროს უფრო მისადაგებული კომპიუტერულ გამოთვლებთან.

კრიპტოგრაფიის და კრიპტოანალიზის ისტორია

ძველ საბერძნეთში გამოყენებული გადანაცვლებადი შრიფი „სკიტალა“, სურათზე ნაჩვენებია მისი თანამედროვე რეკონსტუქცია, შესაძლებელია ეს იყო კრიპტოგრაფიის პირველი ხელსაწყო.

თანამედროვე ერამდე, კრიპტოგრაფია გამოიყენებოდა შეტყობინებათა საიდუმლოების დასაცავად — ტექსტის გარდაქმნით სიმბოლოების გაურკვეველ ნაკრებად, ისე რომ უკუგარდაქმნა იოლი ყოფილიყო მხოლოდ შეტყობინების ადრესატისათვის. უკანასკნელ ათწლეულებში კრიპტოგრაფიამ ისეთი ფუნქციებიც შეიძინა, როგრებიცაა შეტყობინების მთლიანობის შემოწმება, აუთენტიფიკაცია, ციფრული ხელმოწერა, პირადობის შემოწმება, საიდუმლო გამოთვლები და სხვა.

შიფრის კლასიკური ტიპებია გადანაცვლებადი შიფრი (ტექსტში ხდება სიმბოლოების გარკვეული გადაადგილება) და ჩანაცვლებადი შიფრი (ტექსტში ხდება ერთი სიმბოლოს ან სიმბოლოების ჯგუფის სხვებით შეცვლა). ჩანაცვლებადი შიფრის პირველი ცნობილი მაგალითია იულიუს კეისარის შიფრი, რომელშიც ლათინური ანბანის ყოველი ასო იცვლებოდა მისგან მარჯვნივ 3 პოზიციით დაცილებული სიმბოლოთი.

კლასიკური შიფრებით დამუშავებული ტექსტი (შიფროტექსტი) ყოველთვის შეიცავდა გარკვეულ სტატისტიკურ ინფორმაციას, რაც საშუალებას იძლეოდა საწყისი ტექსტის აღდგენისა. IX-ე საუკუნეში არაბი მათემატიკოსის მიერ სიხშირული ანალიზის აღმოჩენის შემდეგ, ასეთი შიფრების გატეხვა გაცილებით იოლი გახდა. 1467 წელს იტალიელმა ლეონ ბატისტა ალბერტიმ გამოიგონა პოლიალფაბეტური შიფრი, რომელითაც ტექსტის სხვადასხვა ნაწილი სხვადასხვა შიფრით იშიფრებოდა. მანვე გამოიგონა პირველი მექანიკური დამხმარე მოწყობილობა (ბორბალი). ვიგენერის პოლიალფაბეტურ შიფრში გამოიყენებოდა პაროლი, რომელიც განსაზღვრავდა, ტექსტის რომელი სიმბოლო შიფრის რომელი სიმბოლოთი უნდა შეცვლილიყო. 1800 წელს ბებიჯმა დაამტკიცა, რომ ასეთი ტიპის პოლიალფაბეტური შიფრებიც ექვემდებარებოდა გარკვეულ სიხშირულ ანალიზს.

მიუხედავად იმისა, რომ სიხშირული ანალიზი საკმაოდ მძლავრი საშუალებაა კრიპტოანალიზისათვის, ის მაინც შედარებით უცნობ მეთოდად რჩებოდა. ამ მეთოდის გარეშე შიფრის გატეხვა მოითხოვდა შიფრის ალგორითმის ცოდნას, რასი მოპოვებაც შპიონაჟით, მოქრთამვებით და გამოძალვებით ხერხდებოდა. XIX საუკუნეში დადგინდა, რომ შიფრის ალგორითმის საიდუმლოდ შენახვა შიფრის დაცულობის გარანტი არ არის და რომ შიფრი დაცული უნდა რჩებოდეს მაშინაც კი, როდესაც მოწინააღმდეგე სრულად ფლობს გამოყენებული შიფრის ალგორითმის შესახებ ინფორმაციას. სხვა სიტვებით, იდეალური შიფრის დაცულობა დამოკიდებული უნდა იყოს შიფრის გასაღების (პაროლის) დაცულობაზე. კრიპტოგრაფიის ეს ფუნდამენტური პრინციპი პირველად ჩამოაყალიბა 1883 წელს ავგუსტ კერჰოფმა („კერჰოფის პრინციპი“), შემდგომში ეს პრინციპი განავრცო კლოდ შენონმა — „მტერი იცნობს სისტემას“.

კრიპტოგრაფიაში მრავალი ხელსაწყო და მექანიზმი იქნა გამოყენებული. პირველი ცნობილი მაგალითია ძველ საბერძნეთში სპარტელების მიერ გამოყენებული ღვედი, გადანაცვლებადი შიფრისათვის. პოლიალფაბეტურ

შიფრებთან ერთად გამოჩნდა ალბერტის შიფრის დისკი, ტრიტემიუსის სქემა და ჯეფერსონის ცილინდრები. რამდენიმე შიფრაცია-დეშიფრაციის მოწყობილობა იქნა გამოგონებული XX საუკუნის დასაწყისში, მათ შორის როტორული მანქანები. მათგან ყველაზე ცნობილი, ენიგმა, გერმანელების მიერ გამოყენებულ იქნა II მსოფლიო ომში. ამ ტიპის მანქანებმა კარდინალურად გაზარდა კრიპტოანალიზის სირთულე.

კომპიუტერების გამოჩენამ შესაძლებელი გახადა შექმნილიყო გაცილებით რთული და დახვეწილი შიფრები. შესაძლებელი გახდა, დაშიფრულიყო ყველანაირი მონაცემი ბინარულ ფორმატში. კომპიუტერული შიფრები უმეტესწილად მანიპულირებენ ბიტებზეან ბიტების ჯგუფებზე, განსხვავებით კლასიკური პოლიალფაბეტური შიფრებისაგან, რომლებიც ტექსტის ცალკეულ სიმბოლოებს ამუშავებდნენ. ამავე დროს გააადვლდა შიფრების კრიპტოანალიზი. მიუხედავად ამისა, თანამედროვე შიფრები მონაცემების დაცვის მაღალდონეს უზრუნველყოფენ, მათი კრიპტოანალიზის გზით გატეხვა იმდენად კოლოსალურ გამოთვლით და დროით რესურსებს მოითხოვს, რომ პრაქტიკულად შეუძლებლად მიიჩნევა.

ინტენსიური ღია კვლევები კრიპტოგრაფიის დარგში შედარებით ახლო პერიოდში დაიწყო — 70-იან წლებში ეს იყო DES-ის (Data Encryption Standard) გამოქვეყნებული სპეციფიკაციები, დიფი-ჰელმანი და RSA ალგორითმი. მას შემდეგ ინტენსიურად დაიწყო კრიპტოგრაფიის გამოყენება კომუნიკაციებში, კომპიუტერულ ქსელებსა და მთლიანად კომპიუტერულ უსაფრთხოებაში. თანამედროვე კრიპტოგრაფიული სისტემების დაცულობა დამოკიდებულია გარკვეულ მათემატიკურ პრობლემებზე, მაგ. რიცხვის ფაქტორიზაცია, დისკრეტული ლოგარითმები და ელიპსური მრუდეები. დამტკიცებულია, რომ ასეთი კრიპტოგრაფიული სისტემა დაცულია, თუ მათემატიკური პრობლემის ეფექტურად და მოკლე დროში გადაჭრა შეუძლებელია. გამონაკლისია „ერთჯერადი ბლოკნოტი“,

არ არსებობს მისი გატეხვის თეორიული გზა, და წარმოადგენს იდეალურ კრიპტოგრაფიულ ალგორითმს.

თუ XX საუკუნემდე კრიპტოგრაფია ძირითადად მანიპულირებდა სიმბოლოებზე და იყენებდა ლინგვისტიკის ელემენტებს, XX საუკუნიდან ხდება მათემატიკის ინტენსიური გამოყენება, ინფორმაციის თეორიის, სტატისტიკის, კომბინატორიკის, აბსტრაქტული ალგებრის და რიცხვთა თეორიის ჩათვლით. ბოლო წლებში მიმდინარეობს კრიპტოგრაფიაში კვანტური ფიზიკის ელემენტების შემოტანაც (იხ. კვანტური კრიპტოგრაფია და კვანტური გამოთვლები)

თანამედროვე კრიპტოგრაფია

სიმეტრიული კრიპტოგრაფია

სიმეტრიული კრიპტოგრაფია იყენებს მეთოდებს, რომლის დროსაც ინფორმაციის გამგზავნი და მიმღები იყენებენ ერთსა და იმავე გასაღებს (იშვიათად სხვადასხვას, მაგრამ ამ შემთხვევაში ერთი გასაღები იოლად გამოითვლება მეორიდან). 1976 წლამდე ეს შიფრაციის ერთადერთი მეთოდი იყო. თანამედროვე სიმეტრიული კრიპტოგრაფია დაკავშირებულია ძირითადად ბლოკურ შიფრებთან, ნაკადურ შიფრებთან და მათ გამოყენებასთან.

ბლოკური შიფრი

ბლოკური შიფრი წარმოადგენს ფაქტობრივად პოლიალფაბეტური შიფრის მოდიფიკაციას: აიღება საწყისი ტექსტის გარკვეული სიგრძის ნაწილი (ბლოკი) და გასაღები, შედეგად მიიღება იგივე (იშვიათად განსხვავებული) სიგრძის შიფროტექსტი. შიფროტექსტის შემადგენელი ბლოკების ერთმანეთთან შერწყმისათვის გამოიყენება სხვადასხვა მეთოდები, რომლებსაც მთლიანობაში ქმედების რეჟიმი ეწოდებათ. მონაცემთა შიფრაციის სტანდარტი (Data Encryption Standard — DES) და გაუმჯობესებული შიფრაციის სტანდარტი (Advanced Encryption

Standard — AES) წარმოადგენენ ბლოკურ შიფრებს. DES (და მისი ნაირსახეობა 3DES) ჯერაც რჩება ერთერთ ყველაზე პოპულარულ ალგორითმად და ფართოდ გამოიყენება. თუმცა მისი გასაღების სიგრძის არასაკმარისობის გამო, ხდება მისი ჩანაცვლება სხვა, უფრო თანამედროვე ალგორითმებით. დღემდე გამოგონილია მრავალი ბლოკური შიფრი, მათი უმეტესობა გატეხილია წარმატებული კრიპტოანალიზის შედეგად.

ნაკადური შიფრი

ნაკადური შიფრი ქმნის განუსაზღვრელი სიგრძის გასაღებს, რომელიც შემდგომ უერთდება საწყის ინფორმაციას (ბიტობრივად ან ბაიტობრივად). გამომავალი ინფორმაცია დამოკიდებულია შიფრის შინაგან მდგომარეობაზე, რომელიც მოქმედების მიმდინარეობისას იცვლება. საწყისი მსგომარეობა დამოკიდებულია შიფრის გასაღებზე (ზოგიერთ ნაკადურ შიფრში ტექსტზეც). ნაკადური შიფრის მაგალითია RC4.

ჰეშ-ფუნქციები

კრიპტოგრაფიული ჰეშ-ფუნქციები (ტექსტის ანაბეჭდის ფუნქციები) წარმოადგენენ კრიპტოგრაფიული ალგორითმების მნიშვნელოვან კლასს. ისინი იღებენ საწყის მნიშვნელობად ტექსტს და უკან აბრუნებენ ფიქსირებული სიგრძის ჰეშს, რომელიც დაკავშირება საწყის მნიშვნელობასთან პრობლემას წარმოადგენს. ასეთ ფუნქციებს ცალმხრივ ფუნქციებსაც ეძახიან. საუკეთესო ალგორითმებისათვის კოლიზიები (ორი ტექსტი, რომელთა ჰეში ერთი და იგივეა) რთული მოსაძებნი უნდა იყოს და ამის ალბათობა მინიმუმამდე უნდა იყოს დაყვანილი.

შეტყობინების აუთენტიფიკაციის კოდები

შეტყობინების აუთენტიფიკაციის კოდები ჰეშ-ფუნქციების მსგავსია, იმ განსხვავებით, რომ ჰეშ-მნიშვნელობის შესამოწმებლად გამოიყენება

საიდუმლო გასაღები.

ასიმეტრიული კრიპტოგრაფია (კრიპტოგრაფია ღია გასაღებით)

სიმეტრიული კრიპტოგრაფია იყენებს 1 გასაღებს შიფრაციისათვის და დეშიფრაციისათვის. ამ მეთოდის უპირველეს ნაკლს გასაღების მართვის აუცილებლობა წარმოადგენს. ქსელში ყოველ სხვადასხვა წყვილს უწევს იქონიოს ცალკე გასაღები, რაც წყვილთა რაოდენობის გაზრდისას გასაღებების რაოდენობის კვადრატული პროპორციით გაზრდას იწვევს. ორ მოკავშირე მხარეს შორის გასაღების გაცვლა, მაშინ როცა ჯერ არ არსებობს დაცული საკომუნიკაციო არხი, კვერცხის და ქათმის პრობლემას ემსგავსება (გასაღების გაცვლა უნდა მოხდეს ფარულად, ფარულად გაცვლა ითხოვს დაშიფრვას, დაშიფრვა თავის მხრივ თხოულობს გასაღების გაცვლას და ა. შ.) 1976 წელს უიტფილდ დიფიმ და მარტინ ჰელმანმა წარმოადგინეს ასიმეტრიული კრიპტოგრაფია — კარდინალურად განსხვავებული კონცეფცია, რომელშიც გამოიყენება ორი სხვადასხვა, მაგრამ მათემატიკურად ერთმანეთთან დაკავშირებული გასაღები — ღია და ფარული გასაღებები. ამავე დროს ფარული გასაღების მიღება ღია გასაღებიდან მოითხოვს კოლოსალურ გამოთვლით რესურსებს. ასიმეტრიულ კრიპტოგრაფიაში ღია გასაღები შეიძლება ყველასთვის ცნობილი იყოს, ამავე დროს ფარული გასაღები საიდუმლოდ უნდა დარჩეს. ტიპიურ შემთხვევაში ფარული გასაღები გამოიყენება შიფრაციის დროს, ხოლო ღია გასაღები დეშიფრაციის დროს. დიფიმ და ჰელმანმა ასევე წარმოადგინეს დიფი-ჰელმანის გასაღების გაცვლის პროტოკოლი. 1978 წელს კრიპტოგრაფების ჯგუფმა რონალდ რივესტის, ადი შამირის და ლენ ედლმანის შემადგენლობით შექმნეს მეორე ასიმეტრიული კრიპტოსისტემა RSA. დიფი-ჰელმანის და RSA ალგორითმები დღეს ფართოდ არის გავრცელებული. არსებობს ასევე რამდენიმე სხვა კრიპტოსისტემა, რომელიც ღია გასაღების კონცეფციას იყენებს.

შიფრაციის გარდა ასიმეტრიული კრიპტოგრაფია ციფრული ხელმოწერებისათვისაც გამოიყენება. ციფრული ხელმოწერა ჩვეულებრივ

ხელმოწერას იმით წააგავს, რომ მისი მფლობელისათვის მისი შექმნა და განკარგვა მარტივია, ხოლო უცხო პირისათვის მისი დუბლირება — შეუძლებელი. ციფრული ხელმოწერები გამოიყენება 2 ალგორითმში: 1)ხელმოწერა, სადაც ფარული გასაღები გამოიყენება ტექსტის ან ტექსტის ჰეშის შიფრაციისათვის, ხოლო 2)შემოწმება, სადაც ღია გასაღების მეშვეობით ხდება დეშიფრაცია, მოწმდება ტექსტის ჰეში და ამდენად ტექსტის მთლიანობა და ხელმოწერის ნამდვილობა. RSA და DSA წარმოადგენენ ციფრული ხელმოწერის ყველაზე გავრცელებულ ალგორითმებს და ფართოდ გამოიყენება ისეთ პროტოკოლებში, როგორებიცაა SSL/TSL, VPN და სხვა.

ღია გასაღების კრიპტოსისტემები დაფუძნებულია „ძნელი“ პრობლემების გამოთვლით სირთულეზე. მაგალითად RSA ემყარება რიცხვის ფაქტორიზაციის პრობლემას (ანუ დიდი რიცხვის დაშლას მარტივ მამრავლებად), ხოლო დიფი-ჰელმანის ალგორითმი ეფუძნება დისკრეტული ლოგარითმების პრობლემას. ასეთი სისტემების უმეტესობაში ინტენსიურად გამოიყენება მოდულით გამრავლება და ახარისხება, შესაბამისად გაცილებით მეტი გამოთვლითი სიმძლავრეა საჭირო, ვიდრე სიმეტრიულ სისტემებში. ამიტომ ღია გასაღების კრიპტოსისტემები ძირითადად გამოიყენება, როგორც ჰიბრიდული სისტემები, სადაც ინფორმაციის შიფრაცია/დეშიფრაციისათვის გამოიყენება სწრაფი სიმეტრიული ალგორითმები, ხოლო მისი გასაღების მართვისა და გადაცემისათვის გამოიყენება შედარებით ნელი ასიმეტრიული ალგორითმები.

კრიპტოანალიზის უმთავრესი ამოცანაა იპოვოს სუსტი წერტილები კრიპტოგრაფიულ სისტემაში, რათა შეძლოს ამ სისტემით დაცული ინფორმაციის მოპოვება. კრიპტოანალიზი შეიძლება გამოყენებულ იქნას, როგორც ბოროტგანმზრახველის მიერ, ასევე კრიპტოსისტემის შემქმნელის მიერ ამ სისტემაში ნაკლის აღმოსაჩენად (გაცილებით იოლია სისტემის ნაკლის პოვნა, ვიდრე მისი სრულყოფილების დამტკიცება). ფართოდ

გავრცელებული (და ამავე დროს მცდარი) აზრია ის, რომ ნებისმიერი შიფრის გატეხვა შესაძლებელია სასრულ დროში. II მსოფლიო ომის პერიოდში კლოდ შენონმა დაამტკიცა, რომ შიფრის გატეხვა თეორიულად შეუძლებელია, თუ მისი გასაღები ნამდვილად შემთხვევითია, არ მეორდება, ტექსტის სიგრძის ტოლი ან მეტია და დაცულია პირდაპირი წვდომისაგან სხვა პირებისაგან. ამ პირობებს მხოლოდ ე.წ. ერთჯერადი ბლოკნოტი აკმაყოფილებს. სხვა შიფრები, გარდა ამ შიფრისა, შეიძლება გატყდეს ე. წ. უხეში ძალის მეთოდით (მიუხედავად მისი დროისა). ამავე დროს შესაბამისი გამოთვლების ოდენობა ექსპონენციურად დამოკიდებულია გასაღების სიგრძეზე. სისტემა ითვლება დაცულად, თუ ამ გამოთვლების ოდენობა აღემატება ნებისმიერი მოწინააღმდეგის შესაძლებლობებს, ამავე დროს თუ არ არსებობს გატეხვის სხვა მეთოდი, რომელიც უფრო სწრაფი იქნებოდა, ვიდრე უხეში ძალის მეთოდი. დღესდღეისობით ერთადერთ თეორიულად გაუტეხელ შიფრად ერთჯერადი ბლოკნოტი რჩება.

არსებობს კრიპტოანალიზის რამდენიმე ტიპი. ძირითადი განსხვავება მათ შორის არის მოწინააღმდეგისათვის ცნობილი ინფორმაციის ოდენობა და სახე, რის საფუძველზეც ხდება შემდეგ ანალიზი. ცნობილი შიფროტექსტის შემთხვევაში კრიპტოანალიტიკოსს ხელთ აქვს მხოლოდ დაშიფრული ინფორმაცია. ცნობილი ღია ტექსტის შემთხვევაში კრიპტოანალიტიკოსს აქვს შიფროტექსტი და მისი შესაბამისი ტექსტი, მაგრამ არ აქვს გასაღები. არჩეული ტექსტის შემთხვევაში ანალიტიკოსს შეუძლია თვითონ შეარჩიოს ტექსტი და მიიღოს მისი შესაბამისი შიფროტექსტი. და ბოლოს არჩეული შიფროტექსტის შემთხვევაში ანალიტიკოსს შეუძლია შეარჩიოს შიფროტექსტები და შეისწავლოს მათი შესაბამისი ტექსტები.

სიმეტრიული კრიპტოსისტემების კრიპტოანალიზი ბლოკურ ან ნაკადურ შიფრებში გატეხვის უფრო ეფექტური მეთოდების პოვნას ემსახურება, ვიდრე გასაღებების სიმრავლის უბრალო გადარჩევა, ანუ უხეში ძალის

მეთოდია. მაგ. უხეში ძალის მეთოდი DES ალგორითმის წინააღმდეგ მოითხოვს 1 ცნობილ ტექსტს და 2^{56} დეშიფრაციის ოპერაციას. ამავე დროს წრფივი კრიპტოანალიზი მოითხოვს 2^{43} ცნობილ ტექსტს და 2^{43} შიფრაციას, რაც უხეში ძალის მეთოდთან შედარებით წინ გადადგმული ნაბიჯია.

ასიმეტრიული ალგორითმები რომელიმე მათემატიკური პრობლემის გამოთვლით სირთულეს ემყარება. მათ შორის ყველაზე ცნობილია რიცხვის მამრავლებად დაშლის პრობლემა, ასევე დისკრეტული ლოგარითმების პრობლემა. მათი კრიპტოანალიზის მეთოდები მოიცავს რამდენიმე მეტნაკლებად ეფექტურ რიცხვით მეთოდს ამ პრობლემების გადასაჭრელად. მაგ. ელიპსური მრუდეების პრობლემის ამოხსნას საუკეთესო ალგორითმით გაცილებით მეტი დრო ესაჭიროება, ვიდრე ექვივალენტური სირთულის რიცხვით ფაქტორიზებას შესაბამისი საუკეთესო ალგორითმით. ამიტომ ბოლო ხანებში ელიპსურ მრუდეებზე დაფუძნებულმა კრიპტოსისტემებმა სულ უფრო მეტი პოპულარობა მოიპოვა.

წმინდა კრიპტოანალიზი იყენებს ალგორითმების სისუსტეებს, მაშინ როდესაც შესაძლებელია კრიპტოსისტემაზე შეტევა განხორციელდეს სხვა კუთხიდანაც, მაგ. კრიპტოანალიტიკოსმა შესაძლოა მოიპოვოს ფიზიკური წვდომა შიფრაციის მოწყობილობაზე და მიიღოს დამატებითი ინფორმაცია ანალიზისათვის, მაგ. შიფრაციის ოპერაციისათვის საჭირო დრო, გატარებული ინფორმაციის სტრუქტურა ან შუალედური მონაცემები. და რა თქმა უნდა რჩება სოციალური ინჟინერია, რაც გულისხმობს ინფორმაციის მოპოვებას თვითონ ადამიანებისგან, ვისაც აქვთ წვდომა კრიპტოსისტემაზე, იქნება ეს შანტაჟით, დაშინებით, მოქრთამვით, შპიონაჟით თუ სხვა. შესაძლოა ეს ყველაზე ეფექტური მეთოდი აღმოჩნდეს ყველა დანარჩენ მეთოდთან შედარებით.

DES	
სრული სახელი	DES (Data Encryption Standard)
გამოშვების თარიღი	1975 (1977 როგორც სტანდარტი)
გამომცემელი	IBM
წინამორბედი	Lucifer
განშტოებები	Triple DES, G-DES, DES-X, LOKI89, ICE
ბლოკის ზომა	64 bits
გასაღების სიგრძე	56 bits
სტრუქტურა Feistel-ის ქსელი	Feistel-ის ქსელი
კრიპტოანალიზი	წრფივი კრიპტოანალიზი,
	დიფერენციალური კრიპტოანალიზი, Brut-force

DES (ინგ. Data Encryption Standard) — მონაცემთა დაშიფრვის სიმეტრიული ალგორითმი, რომელშიც ერთი და იგივე გასაღები გამოიყენება როგორც მონაცემთა დასაშიფრად, აგრთვე მის გასაშიფრად.

DES-ი მუშაობს მონაცემთა 64-ბიტიან ბლოკებზე, დაშიფვისთვის იყენებს 56-ბიტიან გასაღებს, აქვს *ფეისტელის ქსელის* ტიპის 16-ციკლიანი სტრუქტურა. ალგორითმი იყენებს წრფივ (E, P, IP, FP გადანაცვლებები) და არაწრფივ (*S-box*) კომბინირებულ გარდაქმნებს. **DES**-ისთვის რეკომენდებულია რამდენიმე რეჟიმი, მაგ., *Electronic Code Book (ECB)* და *Cipher Block Chaining (CBC)*. აგრეთვე ცნობილია, როგორც მონაცემთა დაშიფრვის ალგორითმი DEA (ინგ. Data Encryption Algorithm). დღესდღეობით მისი გმოყენება აღარ არის რეკომენდებული, მისი შესრულების სინელისა და მოკლე გასაღების გამო, რის გამოც იგი მუდმივი თავდასხმის საშიშროების ქვეშ დგას. **DES**-მეთოდი ძირითადად გამოიყენებოდა Unix-პაროლების დასაშიფრად. მისი ყველაზე გავრცელებული ნაირსახეობა იყო Triple DES. **DES**-ის პირველი სტანდარტი გამოქვეყნდა FIPS(Federal Information Processing Standard)-ის მიერ 1977 წლის 15 იანვარს, ცნობილია "FIPS PUB 46-3"-ის სახელით.

3.2. ალტერნატიული დაშიფრვის მეთოდების გამოყენება

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.

DES-ის ალგორითმი მონაცემთა 64-ბიტიან ბლოკებს გარდაქმნის 64-ბიტიან განსხვავებულ ბლოკად. დასაშიფრად გამოიყენება 56-ბიტიანი სიმეტრიული გასაღები, წარმოდგენილი 64 ბიტში (ყოველი ბაიტის თითო

ბიტი საკონტროლოა). დაშიფრვა ბლოკურ-იტერაციულია, რომელსაც ფეისტელის ქსელის სტრუქტურა აქვს. DES-ში გამოიყოფა 3 ძირითადი ეტაპი: ბლოკის საწყისი და საბოლოო პერმუტაცია. ბიტურ გადანაცვლებათა 16 იტერაციიანი ციკლი, რის შესრულების შემდეგ გენერირდება საბოლოო შედეგი. თითოეულ იტერაციაზე, ალგორითმში წარმოდგენილი *f* - ციკლური ფუნქცია ამუშავებს ბლოკის 32-ბიტს (ნახევარ ბლოკს), და პარამეტრად იყენებს 48-ბიტიან ქვეგასაღებს (*J*). თავდაპირველად ხდება ე.წ. გაფართოება, შემავალი 32 ბიტი გარდაიქმნება 48-ბიტში (ზიგიერთი ბიტი მეორდება).გაფართოების სქემა მოცემულია ქვემოთ(რიცხვები შეესაბაება შემავალ 32-ბიტიან ბლოკში ბიტების რიგით ნომრებს):

32	1	2	3	4	5
4	5	6	7	8	9
8	9	10	11	12	13
12	13	14	15	16	17
16	17	18	19	20	21
20	21	22	23	24	25
24	25	26	27	28	29
28	29	30	31	32	1

შემდეგ მიღებულ 48-ბიტიან ბლოკსა და მიმდინარე ქვეგასაღებზე სრულდება ოპერაცია XOR-ი.

მიღებული 48-ბიტიანი ბლოკი გარდაიკმნება 32-იანად *S*-ბლოკის საშუალებით. შემდეგ სქემის მიხედვით სრულდება კიდევ ერთი გდანაცვლება(რიცხვები წარმოადგენენ ბიტების რიგით ნომრებს):

16	7	20	21
29	12	28	17
1	15	23	26
5	18	31	10
2	8	24	14
32	27	3	9
19	13	30	6
22	11	4	25

შიფრაცია იწყება შემავალ მონაცემთა 64-თანრიგა ბლოკის ბიტების გადანაცლებით (IP - Initial Permutation) : 58-ე ბიტი ხდება პირველი, 50-ე მეორე და ა.შ.

58	50	42	34	26	18	10	2
60	52	44	36	28	20	12	4
62	54	46	38	30	22	14	6
64	56	48	40	32	24	16	8
57	49	41	33	25	17	9	1
59	51	43	35	27	19	11	3
61	53	45	37	29	21	13	5
63	55	47	39	31	23	15	7

მიღებული ბლოკი იყოფა ორ 32-ბიტიან L_0 და R_0 ნაწილად. შემდგომ, 16-ჯერ სრულდება შემდეგი 4 პროცედურა: გსაღების გარდაქმნა *i* ციკლის მთვლელის მნიშვნელობის გათვალისწინებით (ბიტების გადანაცვლება 8 ბიტის ამოგდებით, შედეგად ვიღებთ 48-თანრიგა გასაღებს). დავუშვათ, $A=L_i$, და *J* წარმოადგენს ქვეგასაღებს (გარდაქმნილ, 48-ბიტზე დაყვანილ გასაღებს). *f(A,J)* ფუნქციით გენერირდება ციკლური ფუნქციის 32-ბიტიანი გამოსავალი მნიშვნელობა. სრულდება ოპერაცია *XOR (Ri, f(A,J))*. შედეგი აღინიშნება R_{i+1}. სრულდება ოპერაცია $L_{i+1}=R_i$. ციკლის 16 იტერაციის დატრიალების შემდეგ სრულდება კიდევ ერთი ბიტური გადანაცვლება(საწყისის ინვერსიული). 64 ბიტის გადანაცვლება ხდება შემდეგნაირად (40-ე ხდება პირველ ბიტად ჯდება მე-40, მეორე ბიტად - მე-8 და ა.შ.).

40	8	48	16	56	24	64	32
39	7	47	15	55	23	63	31
38	6	46	14	54	22	62	30
37	5	45	13	53	21	61	29
36	4	44	12	52	20	60	28
35	3	43	11	51	19	59	27
34	2	42	10	50	18	58	26
33	1	41	9	49	17	57	25

S-box წარმოადგენს ცხრილს, რომელიც შემდგარს 4 სტრიქონისა და 16 სვეტისაგან. პირველი S_1 S-ბლოკი წაროდგენილია ქვემოთ:

No.	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13

შემავალი 48-ბიტიანი ბლოკი იყოფა 8 ჯგუფად, თითო 6-ბიტიანად. ჯგუფში პირველი დ ბოლო ბიტი გმოიყენება სტრიქონის მისამართის აღსანიშნავად, შუა 4 ბიტი - სვეტის აღსანიშნავად. შედეგად ყოველი 6 ბიტი გარდაიქმნება 4 ბიტად, ანუ მთელი 48-ბიტიანი კოდი 32-ტანრიგად (ამისათვის საჭიროა 8 S-ბლოკი).

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.

მესამე თავის დასკვნები

დასკვნები

ნაშრომში მიღებული შედეგების მიმართ შეიძლება გაკეთდეს შემდეგი დასკვნები:

ზემოთ თქმულიდან გამომდინარე, საბარათე და ელექტრონული ანგარიშსწორების სისტემა არის ფართო სფერო მისი უწყვეტი ფუნქციონირება საკმაოდ დიდ რესურსებთან არის დაკავშირებული რაც რიგ შემთხვევევბში აისახება მისსავე უსაფრთხოებაზე

ამრიგად, საბარათე დაცვის სისტემების პრობლემატიკაში აუცილებელია შემდეგი ამოცანების გადაწყვეტა:

4. პაროლის ფორმირების სისტემის შემუშავება

5. ალტერნატიული მონაცემთა ბაზების ფორმირება
6. დაშიფრვის ალტერნატიული მეთოდიკის შემუშავება
7. მეორე თავში მოყვანილია ქსელის ინფრასტრუქტურის დაგეგმარების თანამედროვე მეთოდები, განხილულია არსებული სისუსტეები, ზოგიერთ შემთხვევაში ნაჩვენებია პრობლემის გადაწყვეტის მიმართულებები
8. განხილულია სასერვერო ინფრასტრუქტურის მოდელები, შემოთავაზებულია მათი შერჩევის კრიტერიუმები საბარათე სისტემებთან მიმართებაში
9. განხილულია სასერვერო ინფრასტრუქტურის საექსპლუატაციო პირობები და მათი ეფექტური მონიტორინგის საშუალებები
10. განხილულია კიბერუსაფრთხოების მიმართულებები, მოყვანილია სხვადასხვა ქვეყნის მაგალითები, შემოთავაზებულია დამცავი საშუალებები და მათი ეფექტური კონფიგურაციის და გამოყენების მიმართულებები

გამოყენებული ლიტერატურა

1. Addo-Tenkorang R., Helo P.,"Enterprise Resource Planning (ERP): A Review Literature Report", Proceedings of the World Congress on Engineering and Computer Science 2011 Vol II, WCECS 2011, October 19-21, 2011, San Francisco, USA

2. Al-Mashari M., "Enterprise resource planning (ERP) systems:a research agenda", Industrial Management & Data Systems 103/1 [2003] 22-27

3. Winer R. S., "Customer Relationship Management: A Framework,Research Directions, and the Future", Haas School of Business University of California at Berkeley, April 2011

4. Mattews D., "Usability as an ERP Selection Criteria", IFS AB c 2010,

www.ifsworld.com

4. Krigsman M., Fauscette M., Kimberling E., Simon P., Sommer B., " The 2011 Focus Experts' Guide to Enterprise Resource Planning", Focus Research, December 2010

5.Internet is deemed to succeed, The Journal of Internet Banking andCommerce (JIBS), February 2001,pp.88-89.

6. Diniz E. Web Banking in USA. JIBC, June 2001.

7. http://www.commerce.ru/biz_tech/implementation/inet_services/bank_service.html Земсков, В.В. «Банковские услуги в Интернет». Электронная публикация,უკანასკნელადიქნაგადამოწმებული - 21.04.2015

8. http://www.fincen.gov/, უკანასკნელადიქნაგადამოწმებული-21.04.2015

9. Zetteberg Carl D. Estimating e-world auditory ,Web Marketing Today, Issue 103, February, 2004.

10. White L. H. The Technology Revolution and Monetary Evolution, In: The Future of Money in the Information Age. , 2001 Cato Institute's 14th Annual 145 Monetary Conference.

11. Fama E. Banking in the Theory of Finance, Journal of Monetary Economics, 1990 Volume 6, pp. 39-57.

12. Diamond D. and Dybvig P., Bank Runs, Deposit Insurance, and Liquidity,

Journal of Political Economy, 1993, Volume 91, pp. 401-419.
13. . Dewatripont M. and Tirole J. Efficient Governance Structure: Implications

for Banking Regulation, In: C. Mayer and X. Vives, (eds.). Capital Markets and Financial Intermediation. New York: Cambridge University Press. 1993, p.25.
14. Baltensperger E. and Dermine J, European Banking, Prudential and Regulatory

Issues," In: J. Dermine, (ed.), European Banking in the 1990s. Oxford:Basil Blackwell, 1990,pp. 67-68
15. www.economist.com,უკანასკნელადიქნაგადამოწმებული -4.04.2015.

16. Грачева М.В. Центральные банки в эпоху электронных денег: потеря

былого могущества? // Мир электронной коммерции,2000 - №10, 2001- №1, №2. Электроннаяпубликация.
17. Vartanian Thomas P. The Emerging Law of Cyberbanking: Dealing

Effectively with the New World of Electronic Banking & Bank Card Innovations // Fried, Franck, Harris, Shriver &. Jacobson (FFHSJ), 2002.
18. www.bis.org, უკანასკნელადიქნაგადამოწმებული - 02.04.2015.

19. Vartanian Thomas P. The Future of Electronic Payments: Roadblocks and

EmergingPractices.FFHSJ, 2000.
20. Цигер А. Финансовые Интернет-услуги: ставки высоки, Мир

Электроннойкоммерции, №3,2003, ст. 35-38.
21. Strader J.T. The Evolution of Online Investment Banking // JIBC, June 2000.

22. Claessens S., Glaessner T., Klingebiel D. Reshaping the Financial Landscape

around the World. World Bank, 2003.
23. Rhodes D., Rocco I., Buerkner H.-P. Exploiting the Next Wave of Banking Consolidation in Europe, 2002.

24. ზაუტაშვილიდ. ელექტრონულიკომერცია, ქუთაისი, **ISNB** 978-99940- 930-5-2, 2008 წ.

25. http://omedia.ge/portfolio/ufc/, უკანასკნელადიქნაგადამოწმებული -

26. http://daviti.org.ua/eleqtronuli_fuli/sagadasaxado_elektronuli.html, უკანასკნელადიქნაგადამოწმებული - 25.04.2015.

27. http://bankofgeorgia.ge/retail/ge/remote-banking, უკანასკნელადიქნა გადამოწმებული - 2.04.2015.

28.http://www.tbcbank.ge/web/ka/web/guest/remote-channels, უკანასკნელად იქნა გადამოწმებული - 2.04.2015.

29. https://old.emoney.ge/index.php?nav=main/help, eMoney-სთვისებები დაუპირატესობა, უკანასკნელადიქნაგადამოწმებული - 25.04.2015.

30.http://www.navigator.ge/ArticleView.aspx?Id=367,„Unipay, ნავიგატორი ელექტრონული საფულე ქართულო ნლაინსამყაროში“, 11 ივნისი, 2011წ. უკანასკნელადიქნაგადამოწმებული - 20.03.2015.

31. http ://ru.wikipedia.org/wiki/%D0, უკანასკნელადიქნაგადამოწმებული -

32. Бабаев А. Б. Банки в сети Интернет ,Банковские технологии, 2001,№11,

33. Система электронного банкинга, М.- Изд-во “ВИФИТ”,2007,с.1.

34. Банки и банковские операции: Учебник / Под ред. проф. Е.Ф. Жукова. Банки и биржи, издательское объединение “ЮНИТИ”,2004,с.234, Ст.26.

35. White L. H. The Technology Revolution and Monetary Evolution, In: The Future of Money in the Information Age. , 2001 Cato Institute's 14th Annual MonetaryConference.

36. Смородинов О.В. Банки и рынок электронной коммерции, Банковские технологии, 2001, №11,с.13.

37.Колесников И. М. Математическое моделирование Экономическихпроцессов: учебное пособие / И.М. Колесников.Ставрополь: АГРУС, 2005, с.108 ,ст.99.