საქართველოს ტექნიკური უნივერსიტეტი

ლუკა შონია

კორპორაციული ქსელის მრავალდონიანი უსაფრთხოების უზრუნველყოფის მეთოდების და საშუალებების კვლევა

წარდგენილია დოქტორის აკდემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა: ინფორმატიკა

შიფრი - 0401

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0175, საქართველო

2020 წელი

საქართველოს ტექნიკური უნივერსიტეტი

ინფორმატიკის და მართვის სისტემების ფაკულტეტი

ჩვენ, ხელისმომწერნი ვადასტურებთ, რომ გავეცანით **ლუკა შონიას** მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: **„კორპორაციული ქსელის მრავალდონიანი უსაფრთხოების უზრუნველყოფის მეთოდების და საშუალებების კვლევა“** და ვაძლევთ რეკომენდაციას საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკის და მართვის სისტემების ფაკულტეტის საუნივერსიტეტო სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

„----“ „----------“, 2020 წელი

ხელმძღვანელი: პროფესორი ო. შონია

რეცენზენტი: _____

რეცენზენტი: _____

საქართველოს ტექნიკური უნივერსიტეტი

2020 წ

ავტორი: ლუკა შონია

დასახელება: „კორპორაციული ქსელის მრავალდონიანი უსაფრთხოების უზრუნველყოფის მეთოდების და საშუალებების კვლევა“

ფაკულტეტი: ინფორმატიკა და მართვის სისტემები

სადოქტორო პროგრამა: ინფორმატიკა

ხარისხი: საძიებო დოქტორის აკადემიური ხარისხი

სხდომა ჩატარდა: _____

_____

ავტორის ხელმოწერა

რეზიუმე

ინფორმაციული ტექნოლოგიების საყოველთაოდ გავრცელება-დანერგვამ, საწარმოების, ბიზნეს პროცესების, სახელმწიფო მართვის პროცესების ავტომატიზებამ, ელექტრონული ურთიერთობათა მოდელების საყოველთაო აღიარება-გამოყენებამ წინა პლანზე წამოწია ინფორმაციის, როგორც საკუთრების უფლების ობიექტის სამართლებრივი დაცვის აუცილებლობა. თავის მხრივ მოყვანილია მაგალითები, რაც აშკარად მიგვანიშნებს ამ ამოცანის პრობლემატურობაზე. ამის უმთავრესი მიზეზი კი, მდგომარეობს, პირველ რიგში, ინფორმაციის როგორც საკუთრების უფლების ობიექტის თავისებურებაში - ის საკუთრების უფლების ტრადიციული მატერიალური ობიექტისგან განსხვავებით ადვილად კოპირებადია, ადვილად გადაეცემა სხვა საკუთრების უფლების მქონე პირს საკუთრების უფლების რაიმე აშკარა (შესამჩნევი) დარღვევის გარეშე. გარდა ამისა ინფორმაციის კოპირებისა და გადაცემის საფრთხეს ამწვავებს ის გარემოება, რომ ის ინახება და მუშავდება დიდი ოდენობის სუბიექტების მისაწვდომ გარემოში, რომლებიც არ არიან ამ ინფორმაციის საკუთრების უფლების მატარებლები. ესაა, მაგალითად, ფართო სპექტრი საყოველთაოდ გავრცელებული ავტომატიზებული სისტემებისა, დაწყებული ცალკეული ადამიანების კომპიუტერული სამუშაო ადგილებით, დამთავრებული კორპორატიული ავტომატიზებული სისტემებით, ელექტრონული ხელისუფლებით და ინტერნეტით.

სადისერტაციო ნაშრომში წარმოდგენილია კორპორაციული საინფორმაციო სისტემების დაცვის უზრუნველყოფის თანამედროვე პრობლემები და მათი გადაწყვეტის მეთოდები და საშუალებები. დახასიათებულია კორპორაციული საინფორმაციო სისტემების ინფორმაციული უსაფრთხოების (იუ) უზრუნველყოფათან დაკავშირებული რისკები, კომპიუტერულ დანაშაულებათა მაშტაბები და კორპორაციული საინფორმაციო სისტემების (კსს) იუ-ის უზრუნველყოფიდან მომდინარე საფრთხეები. მოყვანილია კორპორაციულ საინფორმაციო სისტემებში ინფორმაციის დაცვის უახლესი სერვისები, მათთან დაკავშირებული რისკები და განხილულია კორპორაციული საინფორმაციო სისტემების უზრუნველყოფის ძირითადი რეკომენდაციები.

ამასთან დაკავშირებით, წინამდებარე ნაშრომში მოყვანილია უსაფრთხოების ფუნდამენტური პრინციპები, ისევე, როგორც ღია პრობლემები. განხილულია კორპორაციული ქსელების უსაფრთხოების საკითხები. უნდა აღინიშნოს, რომ კორპორაციული ქსელების მარშრუტიზაციის პროტოკოლები სპეციფიკაციებში არ განსაზღვრავს რაიმე სახის პრევენციულ ღონისძიებებს ან უსაფრთხოების მექანიზმებს. ამდენად, კორპორაციული ქსელების მარშრუტიზაციის პროტოკოლების უსაფრთხოება გადაუდებელ აუცილებლობად იქცა ქსელის გაშვების სტიმულირებისა და გამოყენების სფეროს გაფართოებისთვის. შესაბამისად, წინამდებარე ნაშრომში შემოთავაზებულია და განსაზღვრული განსხვავებული გადაწყვეტილებები და კონცეფციები უსაფრთხოების

მიმართულებით. ძირითადი ყურადღება თავდაპირველად გამახვილებულია საწყის ნაბიჯზე – მარშრუტიზაციის პროტოკოლების ხარვეზების შესწავლასა და ანალიზზე.

ზემოთ აღნიშნულიდან გამომდინარე, ნაშრომში ყურადღება ექცევა შემდეგი ამოცანების გადაჭრას, როგორიცაა კორპორაციულ ქსელებში ინფორმაციული პაკეტების მარშრუტიზაციის უსაფრთხოების ამაღლება; დაშიფვრისა და აუტენტიფიკაციის მექანიზმების გამკაცრება; კორპორაციულ ქსელებში სხვადასხვა კავშირგაბმულობის არხის ანალიზი და უსაფრთხოების ამაღლების მიზნით ახალი მეთოდების დამუშავება; მოცილებული სამუშაო ადგილების (ადგილობრივი თუ რეგიონული ოფისები) ადმინისტრირება და მართვა კორპორაციული ქსელების გამოყენებით; სისტემაში გამოყენებული აპარატურული მოწყობილობების პარამეტრების დისტანციური მართვა და ადმინისტრირება; სხვადასხვა ადგილობრივ თუ მოცილებულ ობიექტებზე წვდომის გრაფიკების დამუშავება და ანალიზი (ერთიან სისტემაში მონაწილე მხარეების დონეზე); დოკუმენტბრუნვის სისტემის აგება; თითოეული პერსონალის დონეზე ისტორიების შექმნა და მათი ანალიზი; ერთიანი ინფორმაციული არქივის შექმნა და მის საფუძველზე სტატისტიკური ანალიზის ჩატარება ცხრილებისა და დიაგრამების სახით; ავტომატიზებული სისტემის აგება და რეალიზაცია.

VPN ქსელში უსაფრთხოების უზრუნველსაყოფად განხილულია არსებული კრიპტოგრაფიული მეთოდები, მოყვანილია მათი დადებითი და უარყოფითი მხარეები და, არსებული პრობლემებიდან გამომდინარე, შემუშავებულია სიმბოლოების დაშიფვრის კომბინირებული მეთოდი.

ნაშრომში აგრეთვე დეტალურადაა განხილული კორპორაციული ქსელის კომპონენტები და სისტემები, გააანალიზებულია ასეთი ქსელის გამოყენებასთან დაკავშირებული საფრთხეების სხვადასხვა ფორმა და აღნიშნული საფრთხეების აღმოსაფხვრელად შემოთავაზებულია ახალი მეთოდები.

Abstract

The widespread use of information technology, the automation of enterprises, business processes, and public administration processes, and the widespread use of electronic communications models have brought to the fore the need for legal protection of information as an object of property rights. In turn, examples are given, which clearly indicate the problematic nature of this task. The main reason for this is, first of all, the peculiarity of the information as an object of property right - it is easily copied unlike the traditional material object of property right, easily transferred to another person with the right of ownership without any obvious (noticeable) violation of property rights. In addition, the danger of copying and transmitting information is exacerbated by the fact that it is stored and processed in an environment accessible to a large number of entities who are not holders of the right to own this information. This is, for example, a wide range of commonly automated systems, ranging from individual people to computer workplaces, to corporate automated systems, to e-government and the Internet.

The dissertation presents the current problems of ensuring the protection of corporate information systems and the methods and means of solving them. It is characterized by the risks associated with the provision of information security (UC) of corporate information systems, the scale of cybercrime, and the threats posed by the provision of corporate information systems (UCS). The latest information protection services in corporate information systems, the risks associated with them are discussed and the main recommendations for providing corporate information systems are discussed.

In this regard, the present paper discusses the fundamental principles of security, as well as open problems. The security issues of corporate networks are discussed. It should be noted that corporate network routing protocols do not specify any kind of preventive measures or security mechanisms in the specifications. Thus, the security of corporate network routing protocols has become an urgent need to stimulate network launch and expand the scope of use. Accordingly, the present paper presents and defines different solutions and concepts in terms of security. The main focus is initially on the initial step - the study and analysis of the shortcomings of the routing protocols.

Based on the above, the paper focuses on solving the following tasks, such as increasing the security of routing information packages in corporate networks; Tightening encryption and authentication mechanisms; Analyze different communication channels in corporate networks and develop new methods to increase security; Administration and management of vacancies (local or regional offices) using corporate networks; Remote control and administration of the equipment used in the system; Development and analysis of access schedules for various local or remote facilities (at the level of the parties involved in the unified system); Construction of a document circulation system; Create stories at each staff level and analyze them; Create a unified information archive and conduct statistical analysis based on it in the form of tables and diagrams; Construction and sale of an automated system.

The existing cryptographic methods are discussed to ensure security in the VPN network, their pros and cons are listed, and, based on the existing problems, a combined method of encrypting symbols is developed.

The paper also discusses in detail the components and systems of a corporate network, analyzes the various forms of threats associated with the use of such a network, and proposes new methods to eliminate these threats.

შინაარსი

ცხრილების ნუსხა

ნახაზების ნუსხა

შესავალი

კომპიუტერისა და პროგრამირების მეთოდების განვითარებასთან არის დაკავშირებული, აგრეთვე, კორპორაციული ქსელების უსაფრთხოების ამოცანა, რომელიც მოითხოვს უსაფრთხოების მხარდამჭერი ავტომატიზებული სისტემის შექმნას. აღნიშნული პრობლემა წარმოადგენს გამოკვლევის აქტუალურ სფეროს და დღესდღეობითაც აქტიურად მიმდინარეობს მუშაობა ამ პრობლემის გადასაჭრელად.

კორპორაციული ქსელები სწრაფად იქცა ჩვენი ცხოვრების აუცილებელ ნაწილად. ამის ნათელი დადასტურებაა მსგავსი ქსელების ფართოდ გამოყენება სხვადასხვა სფეროში, იქნება ეს ოფისი, კომპანია, საგანმანათლებლო დაწესებულებები,, აეროპორტები, სასტუმროები თუ სხვა. თუმცა კორპორაციული ქსელების უსაფრთხოების საკითხები სერიოზულ ბარიერს წარმოადგენს მათი ფართოდ დანერგვისათვის. ადეკვატური უსაფრთხოების გარეშე სხვადასხვა ორგანიზაციის უმრავლესობა უარს იტყვის კორპორაციული ქსელების გამოყენებაზე, სამთავრობო უწყებები აკრძალავენ კორპორაციული ქსელების გამოყენებას, შესაბამისად, მსგავსი ქსელების უსაფრთხოება მნიშვნელოვანი საკითხია, რაზეც უნდა გამახვილდეს ყურადღება, თუკი ასეთი ქსელების გამოყენება ფართოდ დაინერგება.

წინამდებარე ნაშრომში ყურადღება გამახვილებულია კორპორაციული ქსელების ინფორმაციულ უსაფრთხოების უზრუნველყოფის მეთოდების და საშუალებების კვლევაზე. კორპორაციული ქსელების უსაფრთხოების თემა საკმაოდ ფართოა და მოიცავს ისეთ სფეროებს, როგორიცაა ქსელის პროტოკოლების, უსადენო მოწყობილობების, ოპერაციული სისტემებისა და ა.შ. უსაფრთხოებას.

სადისერტაციო ნაშრომის ძირითად მიზანს წარმოადგენს ის, რომ შემუშავდეს მთელი რიგი ღონისძიებები, რომლებიც აამაღლებს კორპორაციული ქსელების უსაფრთხოებას და მისი საშუალებით მოხდება მოცილებული სამუშაო ადგილების მართვა, აგრეთვე უსაფრთხოების

სისტემის თვისებების გამოკვლევისათვის ფორმალური მეთოდების დამუშავება და ამის საფუძველზე სისტემის პრაქტიკული რეალიზაცია.

ზემოთ აღნიშნული მიზნიდან გამომდინარე, ნაშრომში ყურადღება ექცევა ისეთი ამოცანების გადაჭრას, როგორიცაა კორპორაციულ ქსელებში ინფორმაციული პაკეტების მარშრუტიზაციის უსაფრთხოების ამაღლება; დაშიფვრისა და აუტენტიფიკაციის მექანიზმების გამკაცრება; კორპორაციულ ქსელებში სხვადასხვა კავშირგაბმულობის არხის ანალიზი და უსაფრთხოების ამაღლების მიზნით ახალი მეთოდების დამუშავება; მოცილებული სამუშაო ადგილების (ადგილობრივი თუ რეგიონული ოფისები) ადმინისტრირება და მართვა კორპორაციული ქსელების გამოყენებით; სისტემაში გამოყენებული აპარატურული მოწყობილობების პარამეტრების დისტანციური მართვა და ადმინისტრირება; სხვადასხვა ადგილობრივ თუ მოცილებულ ობიექტებზე წვდომის გრაფიკების დამუშავება და ანალიზი (ერთიან სისტემაში მონაწილე მხარეების დონეზე); დოკუმენტბრუნვის სისტემის აგება; თითოეული პერსონალის დონეზე ისტორიების შექმნა და მათი ანალიზი; ერთიანი ინფორმაციული არქივის შექმნა და მის საფუძველზე სტატისტიკური ანალიზის ჩატარება ცხრილებისა და დიაგრამების სახით; ავტომატიზებული სისტემის აგება და რეალიზაცია.

ჩატარებული კვლევების საფუძველზე შემუშავდა მეთოდები, რომლების საფუძველზეც ხდება: კორპორაციული ქსელებში ინფორმაციული პაკეტების მარშრუტიზაციის უსაფრთხოების ამაღლება; დაშიფვრისა და აუტენტიფიკაციის მექანიზმების გამკაცრება; მოცილებული სამუშაო ადგილების (ადგილობრივი თუ რეგიონული ოფისები) ადმინისტრირება და მართვა კორპორაციული ქსელების გამოყენებით.

წარმოდგენილი მეთოდების საფუძველზე დამუშავდა კორპორაციული ქსელების უსაფრთხოების მხარდამჭერი ავტომატიზებული სისტემა.

სადისერტაციო ნაშრომი შედგება 3 თავისაგან. პირველ თავში წარმოდგენილია ძირითადი ცნობები კორპორაციული კომპიუტერული

ქსელების ტექნოლოგიებისა და კომპონენტების შესახებ, კორპორაციული საინფორმაციო სისტემების ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებულ რისკებზე. მოკლედ განხილულია კორპორაციული ქსელის ერთ-ერთი მთავარი კომპონენტის - უსადენო ქსელების ყველა ნაირსახეობა, აღწერილია მათი სტრუქტურის თავისებურებები და გამოყენების მეთოდები. მოყვანილია უსადენო ქსელებთან დაკავშირებული უსაფრთხოების საკითხები და ჩატარებულია მათი ანალიზი. განხილულია უსადენო ქსელების უსაფრთხოების პრობლემის აქტუალურობა და მათი თავისებურებანი. აღწერილია შესაძლო საფრთხეები და ამავე თავში დახასიათებულია ის თავდასხმები, რომლებსაც შეიძლება ადგილი ჰქონდეს უსადენო ქსელებში. წამოდგენილია კორპორაციული საინფორმაციო სისტემების ინფორმაციული უსაფრთხოების უზრუნველყოფიდან მომდინარე საფრთხეები. ჩამოყალიბებულია კორპორაციული ქსელების უსაფრთხოების ავტომატიზებული სისტემის ძირითადი ამოცანები. მოყვანილია კორპორაციული ქსელების გამოყენების სხვადასხვა სფერო.

მეორე თავში დამუშავებულია კორპორაციული საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფის მეთოდები თავიანთი ფუნქციონალური დანიშნულებებით. VPN ქსელში უსაფრთხოების არსებული მთოდების შესწავლითა და პრობლემის ანალიზით შემუშავებულია მონაცემთა დაშიფვრის ახალი მეთოდები. ისინი უზრუნველყოფს ინფორმაციული პაკეტების მარშრუტიზაციის უსაფრთხოების ამაღლებას.

მესამე თავში აღწერილია კორპორაციული საინფორმაციო სისტემებში ინფორმაციული ნაკადების შეფასების მოდელი და საბოლოო ეტაპზე გააანალიზებულია სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ექსპერიმენტული შემოწმების შედეგები.

თავი 1. კორპორაციული საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფის თანამედროვე პრობლემები და მათი გადაწყვეტის მეთოდები და საშუალებები

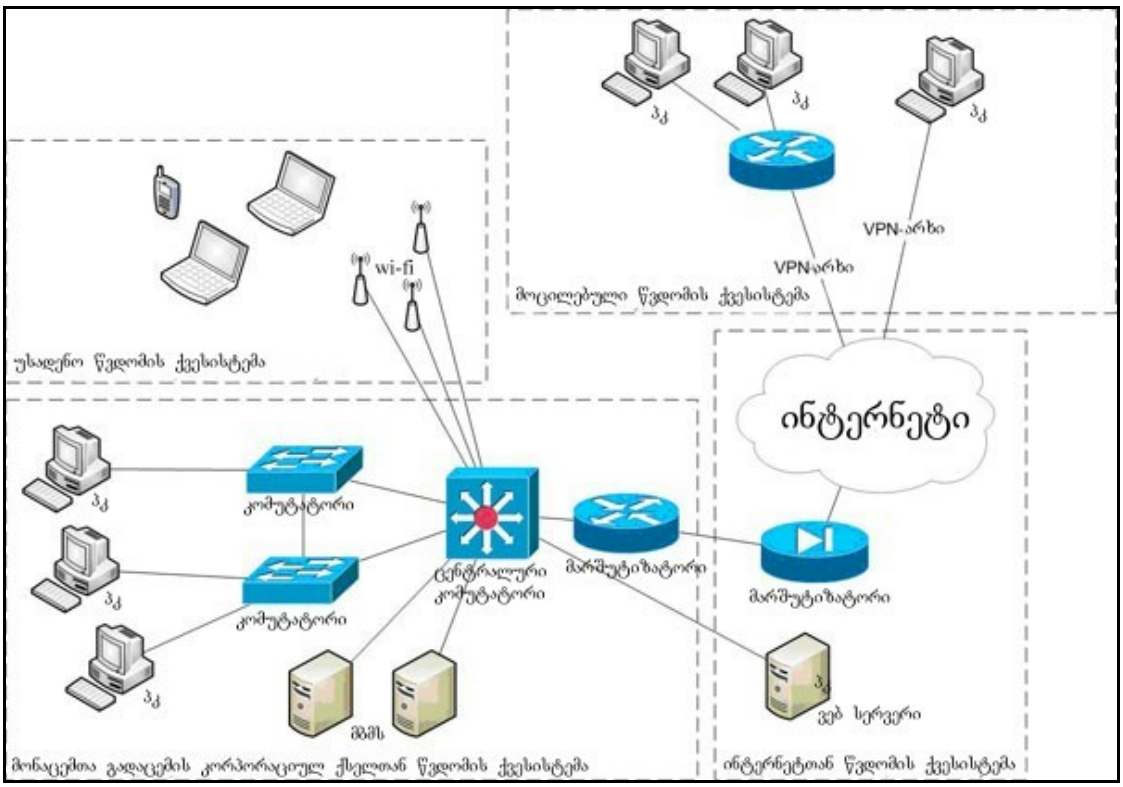
1.1. კორპორაციული საინფორმაციო სისტემების ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებული რისკების ზოგადი დახასიათება

ინფორმაციული ტექნოლოგიების სწრაფმა განვითარებამ შესაძლებელი გახადა გლობალური ქსელის – ინტერნეტის და ისეთი ინფორმაციული გარემოს შექმნა რომელიც ადამიანის მოღვაწეობის ყველა სფეროზე ახდენს გავლენას. იმ სფეროებს, რომელშიც გამოიყენებოდა, გამოიყენება ან შეიძლება გამოყენებული იქნეს მონაცემთა ოპერატიული გაცვლა მიეკუთვნება: საბანკო საქმე, ანგარიშების განაღდება, ელექტრონული კომერცია, საბირჟო ვაჭრობა, აუქციონები, აზარტული თამაშები, ელექტრონული იდენტიფიკაცია, სამედიცინო სერვისებთან დისტანციური წვდომა, კორპორაციული ქსელები, საიდუმლო მონაცემების შენახვა და დამუშავება, საბუთების სერტიფიცირებული მიწოდება, კონტრაქტების დადება, საბუთების ნამდვილობის დადასტურება, არჩევნებზე ხმის მიცემა, გართობა, ლიცენზირება, ბილეთების შეკვეთა და გაყიდვა, იტერაქტიული თამაშები და სხვ.

თანამედროვე ინფორმაციული ტექნოლოგიების გამოყენების ყველაზე უფრო პერსპექტიულ მიმართულებას წარმოადგენს ბიზნესი, რადგან ასეთი ტექნოლოგიების შესაძლებლობები აადვილებს ინფორმაციის გავრცელებას, ზრდის საწარმოო პროცესის ეფექტურობას, ხელს უწყობს ბიზნესის სფეროში საქმიანი ოპერაციების გაფართოებას. კომპანიის ბიზნესის ეფექტურობა პირდაპირ არის დამოკიდებული ბიზნეს-პროცესების ოპერატიულ მართვასა და ხარისხზე.

ბიზნესის მართვის ერთ-ერთ მთავარ ინსტრუმენტებს წარმოადგენენ კორპორაციული ინფორმაციული სისტემები. ახალი ტიპის საწარმო წარმო-

ადგენს ერთმანეთთან ურთიერთმოქმედ განაწილებული ქვესისტემების, ფილიალების და ჯგუფების განშტოებულ ქსელს. განაწილებული კორპორაციული ინფორმაციული სისტემები დღევანდელ პირობებში წარმოადგენენ თანამედროვე კომპანიების საწარმოების უმნიშვნელოვანეს საშუალებას, რადგან ისინი ბიზნესის ტრადიციული ფორმების ელექტრონულ ბიზნესში გარდაქმნის საშუალებას იძლევიან (ნახ.1).



ნახ.1. კორპორაციული ქსელის სხვადასხვა ქვესისტემები

ელექტრონული ბიზნესი წარმოადგენს საქმიანი პარტნიორების, თანამშრომლების და კლიენტების ურთიერთობის ახალ, გამორჩეულად პერსპექტიულ ფორმას და მას შეუძლია დიდი შემოსავლების მოტანა. ელექტრონული ბიზნესი გამოიყენებს ინტერნეტ ქსელს და თანამედროვე ინფორმაციული ტექნოლოგიების ყველა მიმართულებას საქმიანი ეფექტურობის გასაზრდელად, კერძოდ გაყიდვების, მარკეტინგის, გადახდების, ფინანსური ანალიზის, თანამშრომლების მოძებნის, კლიენტებისა და პარტნიორების მხარდაჭერის და სხვ.

ელექტრონული ბიზნესის განხორციელებისას აუცილებელ პირობას წარმოადგენს ინფორმაციული უსაფრთხოება. ამ უკანასკნელში იგულისხმება ინფორმაციისა და ინფრასტრუქტურების დაცვა შემთხვევითი ან შეგნებული ზემოქმედებებისაგან, რადგან დაუცველობამ შეიძლება გამოიწვიოს ინფორმაციის მფლობელებისთვის ან მომხმარებლებისთვის მნიშვნელოვანი ზარალის მოტანა.

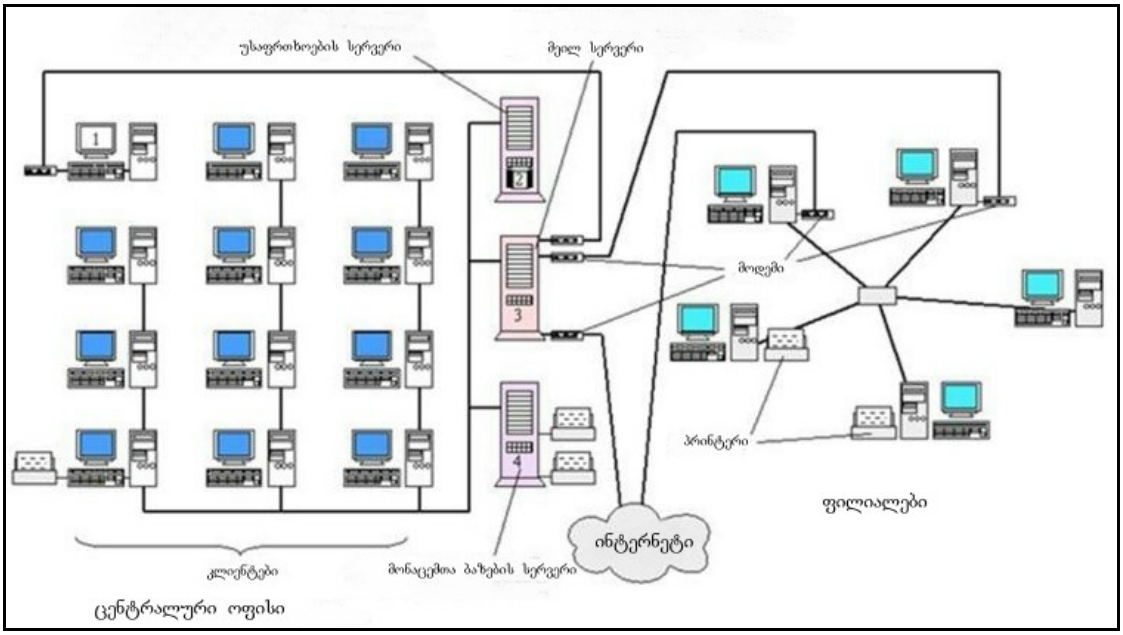
კორპორაციული ინფორმაციული სისტემების უსაფრთხოების უზრუნველყოფა წარმოადგენს კომპანიის ხელმძღვანელობის პრიორიტეტულ ამოცანას, რადგან კონფიდენციალურობის შენახვაზე, კორპორაციული ინფორმაციული რესურსების მთლიანობასა და მისაწვდომობაზე მნიშვნელოვნადაა დამოკიდებული როგორც კომპანიის ეფექტური მუშაობა, ისე ოპერატიული გადაწყვეტილებების მიღება.

კომპიუტერული საშუალებების და ინფორმაციული ტექნოლოგიების ინტენსიური განვითარების მიუხედავად თანამედროვე ინფორმაციული სისტემების და კომპიუტერული ქსელების დაცულობა სამწუხაროდ არ იზრდება. ამიტომ ინფორმაციული უსაფრთხოების უზრუნველყოფის პრობლემების გადასაწყვეტად მონაწილეობას იღებენ როგორც კომპიუტერული სისტემების და ქსელების სპეციალისტები, ისე ელექტრონულ ბიზნესში მომუშავე მრავალრიცხოვანი მომხმარებლები და კომპანიები.

ამ ეტაპზე და უახლოეს მომავალში კორპორაციული სისტემების რესურსების საიმედო დაცვის უზრუნველსაყოფად საჭიროა ინფორმაციული უსაფრთხოების ქვესისტემების იზოლირება ინფორმაციის დაცვის ყველაზე პროგრესული და პერსპექტიული ტექნოლოგიების გამოყენებით.

საერთო მოხმარების ქსელის ბაზაზე ორგანიზებული კორპორაციული ქსელის გადაქცევას კერძო ქსელად უზრუნველყოფს შემდეგი სამი ფუნდამენტალური თვისება: დაშიფვრა, აუტენტიფიკაცია (ნამდვილობის შემოწმება) და შეღწევის კონტროლი. მხოლოდ ამ სამი თვისების ერთდროულად რეალიზაცია უზრუნველყოფს სამომხმარებლო კომპიუტერების, საწარმოების სერვერების და კავშირის დაუცველი ფიზიკური არხებით გადასა-

ცემი ინფორმაციის დაცვას არასასურველი გარეშე შეღწევებისგან, ინფორმაციის გაჟონვისაგან და არასანქციონირებული მოქმედებებისგან (ნახ.2).



ნახ.2. კორპორაციული ქსელის მაგალითი

დღეისათვის აღსანიშნავნია, რომ ინტერნეტი დიდი სისწრაფით ვითარდება როგორც სერიოზული პროფესიული გარემო, ასევე ფაქტია ისიც, რომ ე.წ. კომპიუტერული დამნაშავეები, მათ შორის ჰაკერები, სხვადასხვა სახის ვირუსების შემქმნელები უფრო ხშირად ცდილობენ თავიანთი ჩვევებიდან მიიღონ მატერიალური სარგებელი. ისინი სხვადასხვა მეთოდებით, მავნე პროგრამების გამოყენებით, ცდილობენ კომპიუტერებიდან მოიპარონ ღირებული კონფიდენციალური ინფორმაცია, როგორიცაა მაგალითად, ინტერნეტში შეღწევის პირადი პაროლები, საკრედიტო ბარათების ნომრები, საბანკო და კომერციულ დოკუმენტებთან შეღწევის კოდები და სხვა. აქვე შეიძლება დავასახელოთ პოტენციური ბოროტმზრახველობის ძირითადი კატეგორიები: ოფისში მომუშავე პერსონალი; პროვაიდერების და შუალედური საკომუნიკაციო კვანძების ტექნიკური პერსონალი; სპეციალური სახელმწიფო სამსახურები.

კერძო დაცვის ფირმები. ზოგიერთი ასეთი ფირმა აწარმოებს ინფორმაციის არაკანონიერ შეგროვებას და გაყიდვას. მაგალითად, ასეთ

ფირმებს შეუძლიათ არამარტო სატელეფონო საუბრების ჩაწერა, არამედ ელექტრონული საფოსტო წერილების ხელში ჩაგდება;

ჰაკერები. ექსპერტთა აზრით ჰაკერების შესაძლებლობები აშკარად გაზვიადებულია, მაგრამ მათი შესაძლებლობების იგნორირება არ შეიძლება.

ამრიგად ინფორმაციული ტექნოლოგიების საყოველთაოდ გავრცელება-დანერგვამ, საწარმოების, ბიზნეს-პროცესების, სახელმწიფო მართვის პროცესების ავტომატიზებამ, ელექტრონული ურთიერთობათა მოდელების საყოველთაო აღიარება-გამოყენებამ წინა პლანზე წამოწია ინფორმაციის, როგორც საკუთრების უფლების ობიექტის სამართლებრივი დაცვის აუცილებლობა. დღეისათვის ნებისმიერი მიზანდასახული სუბიექტი იძულებულია მოახდინოს თავისი საქმიანობის ავტომატიზება და იქონიოს ელექტრონული კავშირები, როგორც სახელმწიფო ხელისუფლების ორგანოებთან, ასევე პარტნიორებთან. საჭიროებისას კი ნებისმიერ სუბიექტთან

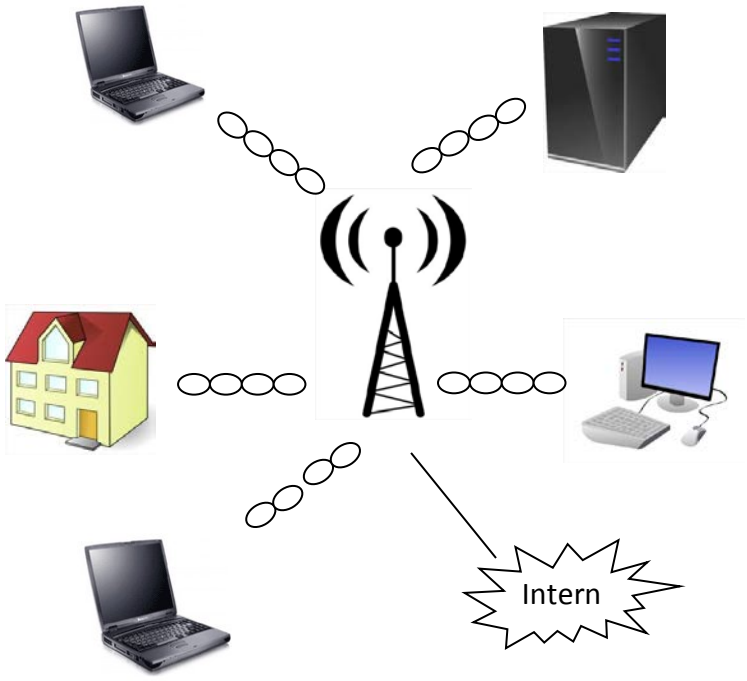
Compliance ბაზის ინფრასტრუქტურა - ესაა ერთობლიობა ხარჯებისა და აპარატურულ პროგრამულ უზრუნველყოფაზე, აგრეთვე ინფორმაციული ტექნოლოგიების (იტ) მომსახურებებზე, რომლებიც განკუთვნილია ინფორმაციული ტექნოლოგიების რისკების კონტროლის, ეფექტური მართვის და კანონმდებლობის მოთხოვნების უზრუნველყოფისათვის აუცილებელი ზომების მისაღებად. აშშ-ში მომქმედი სულ ცოტა რვა ნორმატიული დოკუმენტი მოიცავს ყველა დონის რისკებისა.

1.2. უსადენო ქსელები, მასთან დაკავშირებული უსაფრთხოების საკითხები და მათი ანალიზი

კორპორაციული საინფორმაციო სისტემების (კსს) ერთ-ერთ მთავარ კომპონენტს წარმოადგენს უსადენო ქსელები. ისინი ადამიანების ცხოვრებაში, სადაც არ უნდა იმყოფებოდნენ ისინი - სამსახურში,

სახლში ან საზოგადოებრივი თავშეყრის ადგილებში, დიდ როლს თამაშობს. თუნდაც მაშინ, როცა უსადენო ქსელი იქმნება მარტივი მიზნით - უზრუნველყოს კავშირი ადამიანსა და ინფორმაციის წყაროს შორის სადენების გამოყენების გარეშე, საჭიროა გავერკვეთ უსადენო ქსელების ძირითად კონცეფციაში, განვიხილოთ მასთან დაკავშირებული უსაფრთხოების საკითხები, შემდეგ კი ვნახოთ, თუ როგორ მუშაობს ისინი და რა სარგებლობა შეუძლია მოიტანოს ამა თუ იმ შემთხვევაში.

უსადენო ქსელები ადამიანებს საშუალებას აძლევს დაუკავშირდნენ და მიიღონ კავშირის ნებართვა სხვადასხვა სისტემასთან და ინფორმაციასთან, შეამოწმონ ელექტრონული ფოსტა და დაათვალიერონ WEB-გვერდები, ყოველგვარი სადენების გამოყენების გარეშე, მიუხედავად იმისა, თუ სად იმყოფება ადამიანი - შენობის გარეთ, ქალაქგარეთ ან მსოფლიოს ნებისმიერ წერტილში (ნახ. 3).



ნახ. 3. უსადენო ქსელის მაგალითი

უსადენო ქსელები მრავალი წელია არსებობს ჩვენ გარშემო. უსადენო კავშირის პრიმიტიულ ფორმას შეიძლება მივაკუთვნოთ გემებს

შორის მორზეს ანბანით ინფორმაციის გადაცემა სპეციალური შუქურების საშუალებით (ასეთი მეთოდი იყო და რჩება ზღვაში ინფორმაციის გადაცემის ძირითად ფორმად) და, რა თქმა უნდა, პოპულარული მობილური ტელეფონები, რომლებიც ადამიანებს საშუალებას აძლევს დიდ მანძილზე დაამყარონ ერთმანეთთან კავშირი, აგრეთვე, ისინი შეიძლება მივაკუთვნოთ უსადენო კავშირების ჯგუფს.

არსებობს უსადენო კავშირების სხვადასხვა ნაირსახეობა, მაგრამ უსადენო ქსელების ძირითად თავისებურებად ითვლება ის, რომ კავშირი მყარდება კომპიუტერულ მოწყობილობებს შორის. ასეთებს მიეკუთვნება: პერსონალური ციფრული დამხმარეები (Personal digital assistance, PDA), ნოუთბუქები, პერსონალური კომპიუტერები, სერვერები, პრინტერები და სხვა. კომპიუტერულ მოწყობილობებში იგულისხმება ისეთი მექანიზმები, რომელთაც გააჩნიათ პროცესორები, მეხსიერება და რომელიმე ქსელთან რეაგირების საშუალება. საერთოდ, მობილური ტელეფონები არ მიეკუთვნება კომპიუტერული მოწყობილობების რიცხვს, მაგრამ უახლეს ტელეფონებს გააჩნია განსაზღვრული გამოთვლითი საშუალებები და ქსელური ადაპტერები. აქედან გამომდინარე, ყველაფერი მიდის იმისკენ, რომ უახლოეს მომა ვალში ელექტრონული მოწყობილობების უმრავლესობა აღიჭურვება უსადენო ქსელებში ჩართვის შესაძლებლობებით.

როგორც ჩვეულებრივი ქსელები, რომლებიც დაფუძნებულია სადენების გამოყენებაზე, ასევე უსადენო ქსელებიც, ინფორმაციას გადასცემს კომპიუტერულ მოწყობილობებს შორის. ეს ინფორმაცია შეიძლება წარმოდგენილი იქნას სხვადასხვა სახით: ელექტრონული ფოსტა, WEB-გვერდი, მონაცემთა ბაზების ჩანაწერები, ვიდეოს ნაკადი ან ხმოვანი შეტყობინება. უმრავლეს შემთხვევაში უსადენო ქსელები მონაცემებს (დატა) გადასცემს ელექტრონული ფოსტის საშუალებით და ფაილების სახით. უსადენო ქსელების მახასიათებლების

გაუმჯობესებასთან დაკავშირებით შესაძლებელია ვიდეოსიგნალების გადაცემა, აგრეთვე სატელეფონო კავშირების უზრუნველყოფა.

მომხმარებლების, სერვერებისა და მონაცემთა ბაზების ურთიერთქმედების უზრუნველსაყოფად უსადენო ქსელები, როგორც გადამცემი საშუალება, იყენებს რადიოტალღებს ან ინფრაწითელ დიაპაზონს. ინფორმაციის გადაცემის ეს არეალი უხილავია ადამიანისათვის. დღეისათვის მწარმოებლების უმრავლესობა ქსელური ინტერფეისის პლატებს (network interface card, NIC), რომლებიც ქსელური ადაპტერების სახითაა ცნობილი და ანტენებს კომპიუტერულ მოწყობილობებში ინტეგრირებას უკეთებს ისეთი სახით, რომ ისინი შეუმჩნეველია მომხმარებლებისათვის. ყოველივე ეს უსადენო მოწყობილობას უფრო მობილურს და მოხერხებულს ხდის პრაქტიკაში.

უსადენო ქსელებს, რომლებიც უზრუნველყოფს კავშირს სხვადასხვა ზომის ფიზიკურ ზონაში, ყოფენ სხვადასხვა კატეგორიებად:

- უსადენო ლოკალური ქსელი (wireless local-area network, WLAN);
- უსადენო პერსონალური ქსელი (wireless personal-area network, PAN);
- უსადენო რეგიონული ქსელი (wireless metropolitan-area network, MAN);
- უსადენო გლობალური ქსელი (wireless wide-area network, WAN);

(ცხრილი 1)-ში მოცემულია უსადენო ქსელების ნაირსახეობების მოკლე აღწერა. უსადენო ქსელების ყველა სახეობას გააჩნია თავისებურებები, რისი წყალობითაც დაკმაყოფილებულია თითოეულისადმი წაყენებული სხვადასხვა მოთხოვნა.

ცხრილი 1. უსადენო ქსელების ნაირსახეობები

სახეობა	მოქმედების სფერო	თვისებები	სტანდარტი
უსადენო პერსონალური ქსელი	მომხმარებელთან უშუალო სიახლოვე	საშუალო	Bluetooth, IEEE 802.15, IRDA
უსადენო	შენობის	უმაღლესი	IEEE 802.11

ლოკალური ქსელი	ფარგლებში		Wi-Fi
უსადენო რეგიონული ქსელი	ქალაქის ფარგლებში	უმაღლესი	IEEE 802.16
უსადენო გლობალური ქსელი	მთელ მსოფლიოში	დაბალი	ფიჭური სისტემები

უსადენო პერსონალური ქსელები გამოირჩევა ინფორ მაციის მცირე მანძილზე გადაცემით (17 მეტრამდე), რაც მათ იდეალურს ხდის შენობის პატარა ტერი ტორიაზე ან „პერსონალურ ზონაში“ გამოსაყენებლად. უსადენო პერსო ნალური ქსელების თვისებები არის საშუალო, ინფორმაციის გადაცემის სიჩქარე არ სცილდება 2 მბ/წ-ს. ბევრ სიტუაციაში უსადენო პერსონალური ქსელები წარმატებით ცვლის სადენიან ქსელებს (ნახ. 4).

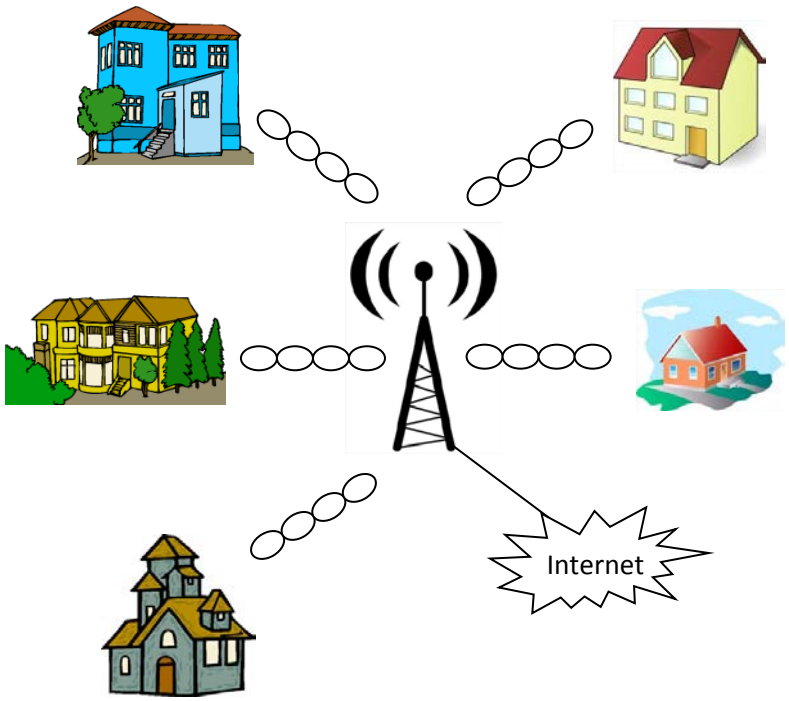
ნახ. 4. უსადენო პერსონალური ქსელი უზრუნველყოფს კომპიუტერულ მოწყობილობებს შორის ინფორმაციის გადაცემას მცირე მანძილზე

ასეთი სახის ქსელს შეუძლია უზრუნველყოს, მაგალითად, მონაცემთა უსადენო სინქრონიზაცია PDA მომხმარებელზე და მის

პერონალურ კომპიუტერზე ან ნოუთბუქზე. ანალოგიურად, შესაძლებელია უსადენო კავშირი პრინტერთან.

უსადენო პერსონალური ქსელების მიმღებ-გადამცემების უმეტესობა გამოირჩევა კომპაქტური ზომით და სჭირდება მცირე სიმძლავრე, რაც მათ ეფექტურს ხდის პატარა სამომხმარებლო მოწყობილობებთან მიმართებაში, აგრეთვე, საშუალებას აძლევს კომპიუტერულ მოწყობილობებს დიდი ხანი იმუშაოს ერთ ბატარეაზე. ყოველივე ეს მომხმარებელს იცავს აკუმულატორის ხშირად დატენვისაგან. გარდა ამისა, მცირე გამოყენებადმა სიმძლავრემ განაპირობა უსადენო პერსონალური ქსელების წარმატებით დანერგვა მობილურ ტელეფონებში და PDA-ში. ტელეფონს შეუძლია უწყვეტად ურთიერთქმედებდეს PDA-ს სატელეფონო წიგნთან. ასევე, ტელეფონზე საუბრის ან მუსიკის მოსმენისას, რომელიც ციფრული სახითაა ჩაწერილი PDA-ზე, შესაძლებელია გამოყენებულ იქნეს ყურსასმენები. ყოველივე ეს შესაძლებელია სადენების გამოყენების გარეშე.

უსადენო პერსონალური ქსელებისთვის სტანდარტად ითვლება 802.15. აშშ-ს ცნობილმა საინჟინრო ინსტიტუტებმა ელექტროტექნიკისა და ელექტრონიკის დარგში (Institute of Electrical and Electronics Engineers, IEEE) თავიანთ სტანდარტ 802.15-ში უსადენო პერსონალური ქსელებისთვის ჩართეს სპეციფიკაცია Bluetooth. ასეთი ტექნოლოგია უზრუნველყოფს საიმედო და ხანგრძლივ გადაწყვეტას ისეთი კომპიუტერული მოწყობილო ბებისთვის, რომლებიც შეერთებულია პატარა ზონაში, მცირე მანძილზე. (ნახ.5).



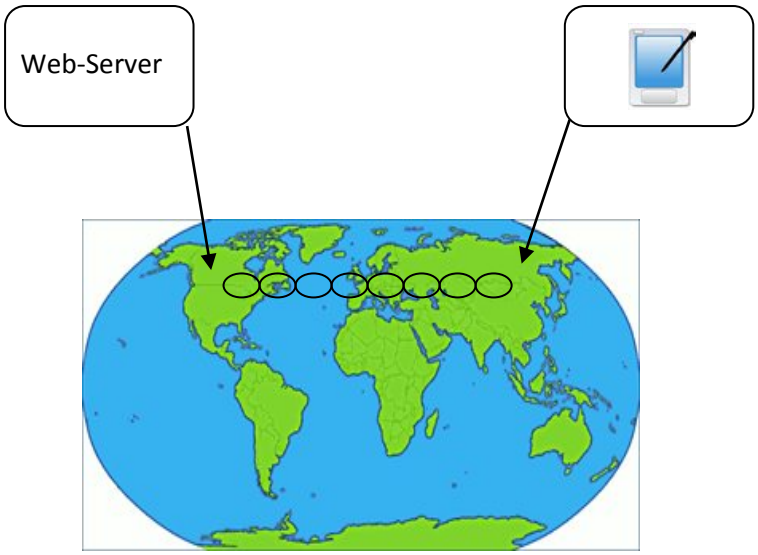
ნახ. 5. უსადენო რეგიონული ქსელები ქალაქის მასშტაბით უზრუნველყოფს მოცილებული შენობების კავშირს ინტერნეტთან

უსადენო ინტერნეტის მომსახურების მომწოდებლები (Wireless Internet Service Provider, WISP) მომხმარებლებს ქალაქის მასშტაბით წარმოუდგენენ უსადენო რეგიონალურ ქსელებს, რომლებიც უზრუნველყოფს მუდმივ უსადენო კავშირს მოცილებულ შენობებს შორის. მსგავს ქსელებს გააჩნია არსებითი უპირატესობა ჩვეულებრივ სადენიან ქსელებთან შედარებით, როგორიცაა, მაგალითად, ციფრული სააბონენტო ხაზები (Digital Subscriber Line, DSL), ვინაიდან ხშირ შემთხვევაში მისი დამონტაჟება დიდ ეკონომიურ ხარჯებთანაა დაკავშირებული.

სამომხმარებლო ბაზარი გვთავაზობს სხვადასხვა დაპატენტებულ გადაწყვეტილებას უსადენო რეგიონული ქსელებისთვის, მაგრამ მწარმოებლები ყოველთვის ეყრდნობიან სტანდარტებს. ზოგიერთები მომწოდებელი იყენებს სტანდარტ 802.11 უსადენო რეგიონული ქსელების შექმნისთვის, მაგრამ ასეთი სტანდარტის სისტემები ოპტიმალურია და

აკმაყოფილებს მოთხოვნებს შენობის შიგნით. მათ შეუძლია შენობის გარეთ კავშირის დამყარება მიმართული ანტენების დახმარებით.

უსადენო გლობალური ქსელები უზრუნველყოფს ინფორმაციასთან წვდომას ქვეყნისა და კონტინენტის მასშტაბით. უსადენო გლობალურ ქსელებს გააჩნია მოქმედების შეუზღუდავი არეალი, რომელიც უზრუნველყოფილია სატელეკომუნიკაციო კომპანიების მიერ (ნახ. 6).



ნახ. 6. უსადენო გლობალური ქსელები უზრუნველყოფს კავშირს მთელს მსოფლიოში

სატელეკომუნიკაციო ოპერატორების მიერ მიღწეული შეთანხმებები როუმინგთან დაკავშირებით შესაძლებელს ხდის კავშირების დიდ მანძილზე დამყარებას და უზრუნველყოფს მონაცემების სწრაფ გადაცემას მობილურ მომხმარებლებს შორის. მხოლოდ ერთ სატელეკომუნიკაციო კომპანიასთან ანგარიშ სწორების შემდგომ მომხმარებელს უსადენო გლობალური ქსელების მეშვეობით მსოფლიოს ნებისმიერი წერტილიდან შეუძლია კავშირის დამყარება ინტერნეტის სხვადასხვა მომსახურებასთან. მონაცემების გადაცემის სიჩქარე ერთ მომხმარებელზე გადაანგარიშებისას უსადენო გლობალურ ქსელებში მაღალი არ არის, მაგრამ მისაღებია პატარა მოწყობილობებისთვის (PDA),

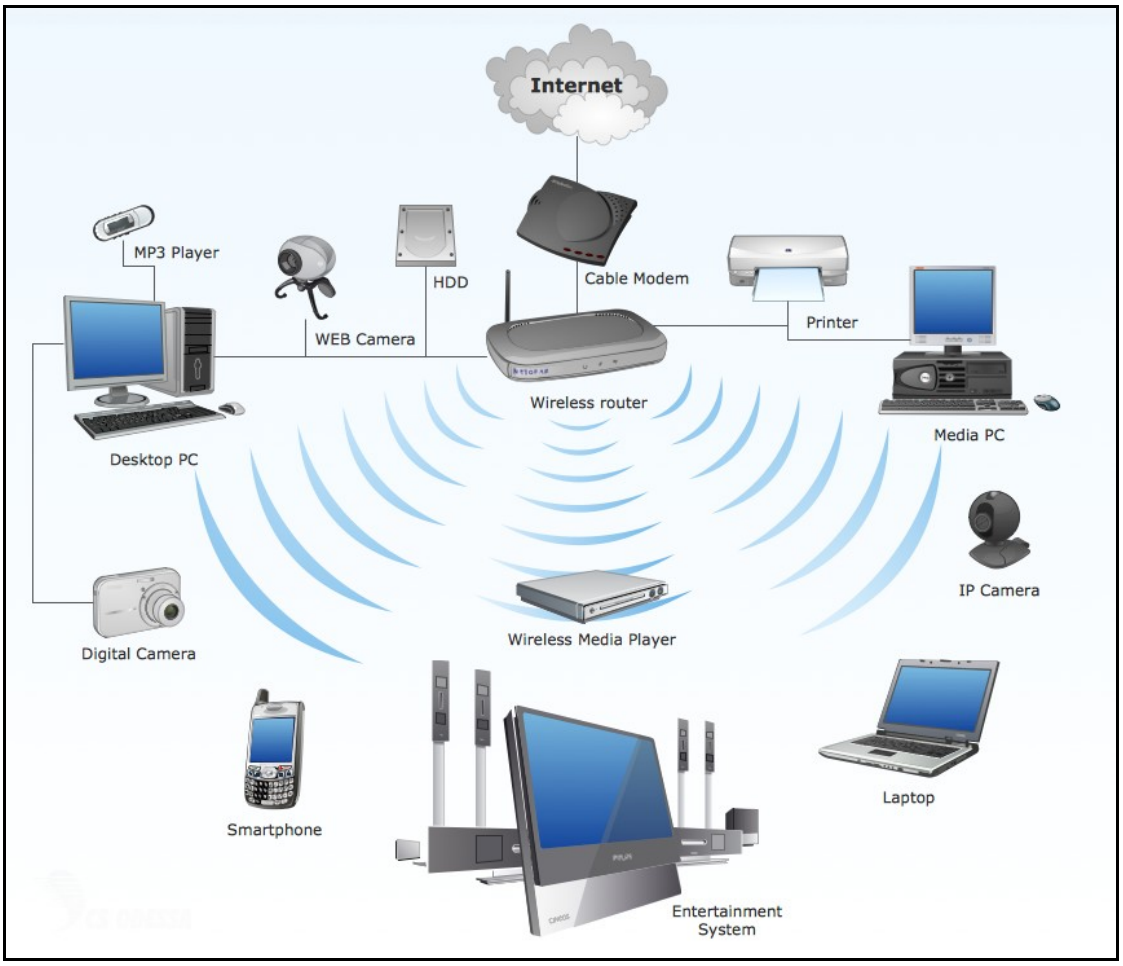
რომლებიც ეკუთვნით მომხმარებლებს და საჭიროებს ასეთი ქსელით კავშირს. მობილური ტელეფონების პატარა ეკრანი და შეზღუდული გამოთვლითი საშუალებები არ საჭიროებს ქსელის მაღალ თვისებებს. ვიდეოგამოსახულების გადაცემა მობილური ტელეფონის პატარა ეკრანზე შესაძლებელია ინფორმაციის გადაცემის მცირე სიჩქარის დროსაც.

სპეციალური სისტემები, რომლებიც ახასიათებს უსადენო გლობალურ ქსელებს, უზრუნველყოფს მომხმარებლის წვდომას ინტერნეტთან, კორპორაციულ სისტემებთან და ელექტრონული ფოსტის მიღება-გადაცემას, მიუხედავად იმისა, თუ სად იმყოფება მომხმარებელი - ოფისში, სახლში თუ შენობის გარეთ. მაგალითად, ქსელის აბონენტებს თავისუფლად შეუძლიათ დაამყარონ კავშირი ტაქსით მგზავრობის ან ქალაქში გასეირნების დროსაც. უსადენო გლობალურ ქსელებს შეუძლიათ ფუნქციონირება ისეთი ადგილებიდან, საიდანაც სხვა ტიპის ქსელებისთვის წვდომა შეუძლებელია, რის გამოც მომხმარებელი ტერიტორიულად შეზღუდული არ არის.

უსადენო გლობალური ქსელების დანერგვასთან დაკავშირებული ერთ-ერთი პრობლემათაგანი არის ის, რომ მას არ შეუძლია უნაკლო კავშირით უზრუნველყოს რომელიმე შენობაში მყოფი მომხმარებლები, ვინაიდან ამ ქსელის ინფრასტრუქტურის ელემენტები მდებარეობს შენობის გარეთ და რადიოსიგნალები შენობაში შესამჩნევად სუსტდება. შედეგად, უსადენო გლობალური ქსელების მომხმარებლებს, რომლებიც იმყოფებიან შენობაში, შეუძლიათ საერთოდ დაკარგონ კავშირი ან, უკეთეს შემთხვევაში, კავშირის თვისებები შესამჩნევად გაუა რესდება. ზოგიერთი სატელეკომუნიკაციო კომპანია უსადენო გლობალური ქსელების სისტემებს შენობაში ამონტაჟებს, მაგრამ ყოველივე ეს დიდ ხარჯებთანაა დაკავშირებული და ტექნიკურად ყოველთვის გამართლებული არ არის.

ერთ-ერთ ფართოდ გავრცელებულ უსადენო ტექნოლოგიას წარმოადგენს IEEE 802.11–ზე დაფუძნებული უსადენო ადგილობრივი ქსელი (WLAN). იგი უმეტესწილად გამოიყენება პერსონალურ კომპიუტერებსა და ლეპტოპებს შორის მონაცემთა უსადენოდ გადაცემისთვის შენობებს შიგნით. ფიჭურ ქსელთან შედარებით მოცემული ტექნოლოგია მოწყობილობებს საშუალებას აძლევს კავშირი პოტენციურად ძალიან მაღალი სიჩქარით დაამყარონ (მაგრამ შედარებით მოკლე მანძილებზე). ფაქტიურად ამ ქსელებს WLAN (Wireless Local Area Network) უსადენო ლოკალურ ქსელებს უწოდებენ, რადგან ისინი LAN - კავშირის ეკვივალენტს უზრუნველყოფენ შენობებს შიგნით.

უსადენო ლოკალური ქსელები გამოირჩევა მაღალი თვისებებით. ის უზრუნველყოფს ინფორმაციის გადაცემას ოფისში და ოფისს გარეთ, რომელიც განლაგებულია ერთ დიდ შენობაში. ასეთი ქსელების მომხმარებლები ჩვეულებრივ იყენებენ PDA-ებს, ნოუთბუქებსა და პერსონალურ კომპიუტერებს დიდი ეკრანებითა და პროცესორებით, რომლებსაც გააჩნიათ დიდ სისტემებთან მუშაობის უნარი. ასეთი ქსელები სრულიად აკმაყოფილებს მოთხოვნებს, რომლებიც წაყენებულია ასეთი ტიპის კომპიუტერული მოწყობილობების შეერთების პარამეტრებისადმი (ნახ. 7).



ნახ. 7. უსადენო ლოკალური ქსელები უზრუნველყოფს კავშირს შენობებს შიგნით

უსადენო ლოკალური ქსელები მარტივად უზრუნველყოფს იმ თვისებებს, რომლებიც აუცილებელია მაღალი დონის სისტემების უწყვეტად შესრულებისათვის. ასეთი ქსელის მომხმარებლებს სერვერიდან შეუძლიათ მიიღონ დიდი მოცულობის ელექტრონული ფოსტა ან ვიდეოს ნაკადი. უსადენო ლოკალური ქსელები სრულიად აკმაყოფილებს ყველა საოფისე სისტემის მოთხოვნებს.

უსადენო ლოკალური ქსელებისთვის სტანდარტი არის IEEE 802.11. არსებობს ამ სტანდარტის სხვადასხვა ვერსია, რომელიც ინფორმაციის გადაცემას უზრუნველყოფს 2,4 და 5 გჰ დიაპაზონში. ასეთი სტანდარტის ძირითადი პრობლემა არის ის, რომ იგი ვერ უზრუნველყოფს სხვადასხვა ვერსიის მქონე კომპიუტერული მოწყობილობების ურთიერთქმედებას. მაგალითად, კომპიუტერული

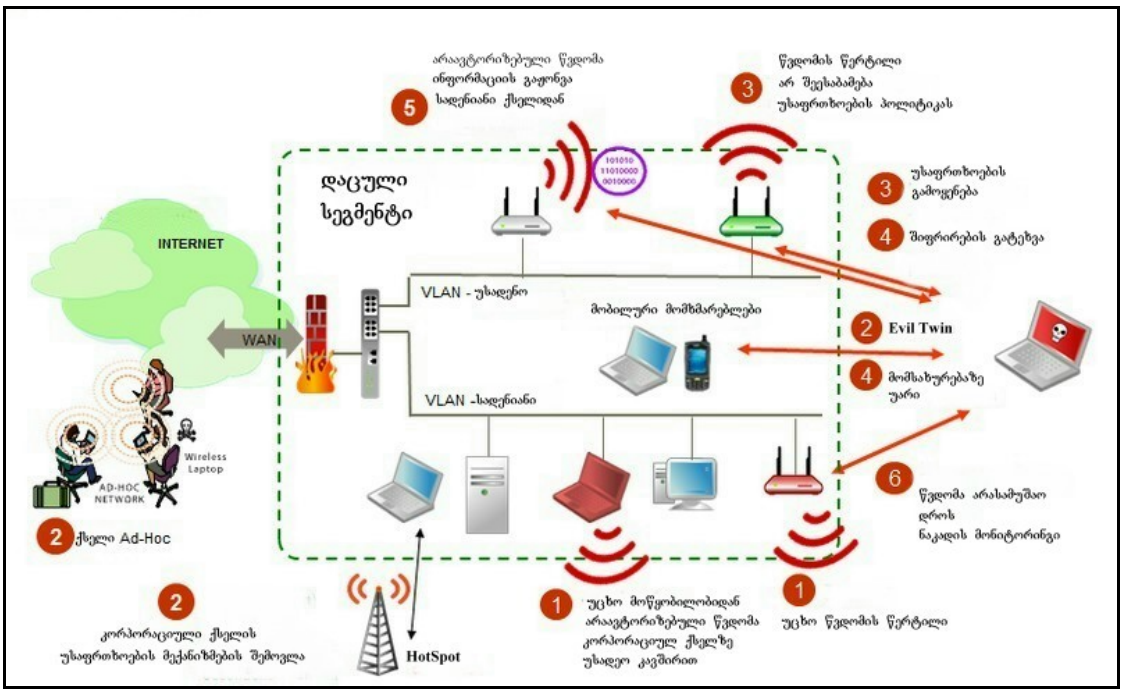
მოწყობილობის ადაპტერები, რომლებიც შეესაბამება 802.11ა სტანდარტის უსადენო ლოკალურ ქსელებს, ვერ უკავშირდება კომპიუტერულ მოწყობილობებს, რომლებიც შეესაბამება 802.11ბ სტანდარტს. არსებობს კიდევ სხვა პრობლემები ამ სტანდარტთან დაკავშირებით, როგორიცაა, მაგალითად, უსაფრთხოების არასა-კმარისი ზომები.

უსადენო პერსონალური, ლოკალური, რეგიონული და გლობალური ქსელები ურთიერთშემავსებელია და აკმაყოფილებს სხვადასხვა მოთხოვნას, მაგრამ ზოგჯერ ძნელია განასხვავო ერთი ქსელი მეორისგან. მაგალითად, უსადენო ლოკალურ ქსელს შენობის შიგნით შეუძლია უზრუნველყოს ურთიერთკავშირი PDA-სა და პერსონალურ კომპიუტერს შორის, ანალოგიურად იმისა, როგორც ამას ასრულებს უსადენო პერსონალური ქსელი.

მომხმარებლის თვალსაზრისით რომ ვიმსჯელოთ მომავალ პერსპექტივებზე, მაშინ უსადენო ქსელების სახეობებს შორის არსებული საზღვრები უნდა წაიშალოს. უკვე შექმნილია კომპიუტერული მოწყობილობების სპეციალური ქსელური ადაპტერები, რომელთაც გააჩნია უსადენო ქსელების სხვადასხვა სახეობის მუშაობისადმი მხარდაჭერა. მაგალითად, ტურისტებს ან ბიზნესმენებს შეიძლება ჰქონდეთ თანამედროვე მობილური ტელეფონი, რომელიც ურთიერთქმედებს როგორც უსადენო ლოკალურ ქსელთან, ასევე უსადენო გლობალურ ქსელთან. ყოველივე ეს უზრუნველყოფს უსადენო კავშირს, აქედან გამომდინარე, მაგალითად, მომხმარებელი, რომელიც იმყოფება აეროპორტის შენობაში, მუშაობს თავის ელექტრონულ ფოსტასთან, რომელიც იყენებს საერთო კავშირის მქონე უსადენო ლოკალურ ქსელს შემდეგ, მგზავრობის დროს, ურთიერთქმედებს სხვა სახის მომსახურებასთან, რომელიც დაფუძნებულია მობი ლური ქსელით მონაცემების გადაცემასთან.

უკანასკნელ ხანებში უსადენო ქსელებში უსაფრთხოება და მომსახურების ხარისხი უაღრესად მნიშვნელოვანი და აქტიური კვლევის

საგანი გახდა, რის მიზეზსაც მონაცემთა პაკეტების გადაცემის მხარდაჭერის მზარდი მოთხოვნა წარმოადგენს. ადეკვატური უსაფრთხოების გარეშე ორგანიზაციები თავს აარიდებენ უსადენო ქსელების გამოყენებას. წინამდებარე კვლევის მიზანს წარმოადგენს ის, რომ შემუშავდეს მთელი რიგი ღონისძიებისა, რომლებიც აამაღლებს უსადენო ქსელების უსაფრთხოებას და მისი საშუალებით მოხდება მოცილებული სამუშაო ადგილების მართვა. (ნახ. 8).



ნახ. 8. უსადენო ქსელების გამოყენებასთან დაკავშირებული საფრთხეების სხვადასხვა ფორმა

უსადენო ტექნოლოგიები, რომლებიც მუშაობენ ფიზიკური და ლოგიკური შეზღუდვების გარეშე მათი სადენიანი ქსელებისაგან განსხვავებით, მნიშვნელოვნად ზრდის სამუშაოს მოქნილობას, მომხმარებლის შრომის ეფექტურობას და ქსელის განლაგების ხარჯების შემცირებას. დეტალურად განვიხილოთ უსადენო ქსელების გამოყენებასთან არსებული რისკები.

რისკი პირველი - უცხო მოწყობილობები. უცხოები არიან ისეთი მოწყობილობები, რომლებიც კორპორაციულ ქსელზე არასანქცირებული

წვდომის საშუალებას იძლევიან, კორპორაციული ქსელის უსაფრთხოების პოლიტიკით განსაზღვრული დაცვის მექანიზმების გვერდის ავლის გზით. ყველაზე ხშირად ეს მოწყობილობები არიან თვითნებურად დაყენებული წვდომის წერტილები. მსოფლიო სტატისტიკის მიხედვით სწორედ ეს მეთოდი წარმოადგენს კორპორაციული ქსელის გატეხვის ყველაზე ხშირ მიზეზს მაშინაც კი, როდესაც ორგანიზაცია არ იყენებს უსადენო კავშირს.

რისკი მეორე - არაფიქსირებული კავშირი. როგორც ზემოთ აღინიშნა, უკაბელო მოწყობილობები არ არის "მიბმული" ერთ რომელიმე ფიქსირებულ სადენზე და მუშაობის პროცესში შეუძლია შეცვალოს მიეთების წერტილი. მაგალითად, არასწორად კონფიგურირებული უსადენო კლიენტი ავტომატურად ასოცირდება და მომხმარებელს აერთებს უახლოეს უსადენო ქსელთან. ასეთი მექანიზმი საშუალებას აძლევს თავდამსხმელებს მიუერთდნენ უსადენო ქსელს.

აგრეთვე, მომხმარებელთა უმრავლესობას, რომლებიც აღჭურვილნი არიან უსადენო მოწყობილობებით და არ არიან კმაყოფილი არსებული სადენიანი ქსელის ხარისხით, უყვართ გადაერთონ უახლოეს უსადენო წერტილებზე (HotSpot), რაც უსაფრთხოს ხდის მოქმედ კორპორაციულ ქსელს.

არსებობს Ad-Hoc ქსელები - ეს არის უკაბელო მოწყობილობებს შორის ერთრანგიანი მიერთება წვდომის წერტილების გამოყენების გარეშე, რომელიც არის მოსახერხებელი სწრაფად მოხდეს ინფორმაციის გაცვლა მოწყობილობებს შორის ან ამოიბეჭდოს სასურველი დოკუმენტი Wi-Fi პრინტერის საშუალებით. ყოველუვე ეს ასევე უსაფრთხოს ხდის მოქმედ კორპორაციულ ქსელს და საშუალებას აძლევს თავდამსხმელებს მარტივად მიუერთდნენ კორპორაციულ ქსელს. ასევე არსებობს ტექნოლოგია - Evil Twin, რომლითაც ბოროტგანმზრახველი ქმნის წვდომის წერტილის ასლს, რომელიც მდებარეობს ქსელის მოქმედების იმავე რადიუსში და თვითონვე ცვლის ორიგინალ წვდომის წერტილს ასლით, რომელზეც უერთდებიან

მომხმარებლები და საშუალებას იძლევა თავდამსხმელმა წვდომა მოიპოვოს კონფიდენციალურ ინფორმაციასთან.

რისკი მესამე - ქსელებისა და მოწყობილობების ნაკლოვანებები. კორპორაციულ ქსელში ზოგიერთი ქსელური მოწყობილობა შეიძლება იყოს უფრო დაუცველი, ვიდრე სხვები, ისინი შეიძლება არასწორად იყვნენ კონფიგურირებული. ამ შემთხვევაში გასაკვირი არ არის ის, რომ თავდამსხმელები თავდაპირველად თავს დაესხმევიან სწორედ ასეთ მოწყობილობებს. მაგალითად, ერთმა არასწორად კონფიგურირებულმა წვდომის წერტილმა, რომელსაც არა აქვს ჩართული აუტენტიფიკაციისა და შიფრირების მექანიზმები, შეიძლება გამოიწვიოს კორპორატიული ქსელის გატეხვა.

რისკი მეოთხე - "მომსახურებაზე უარი" და შიფრირების გატეხვა. "მომსახურებაზე უარი" სახეობის შეტევა (Denial of service, DoS) - ეს არის თავდასხმა, რის შედეგადაც კორპორაციული ქსელი ხდება გამოუსადეგარი ან მისი მუშაობა იბლოკება. ასეთი შეტევის შესაძლებლობა უნდა გაითვალისწინოს ყველამ, ვინც კი გამართავს უსადენო ქსელს. აუცილებელია დაფიქრება იმაზე, თუ რა მოხდება, როდესაც ქსელი გახდება მიუწვდომელი განუსაზღვრელი დროით.

DoS შეტევის სერიოზულობა დამოკიდებულია იმაზე, თუ რა შედეგს გამოიწვევს უსადენო ქსელის მწყობრიდან გამოსვლა. მაგალითად, ჰაკერს შეუძლია გახადოს მიუწვდომელი უსადენო ლოკალური ქსელი, რომელიც გამართულია სახლში, ხოლო ამის შედეგი იქნება მხოლოდ სახლის მეპატრონის შეწუხება, მაგრამ საწარმოს ინვენტარიზაციის უსადენო სისტემის მწყობრიდან გამოსვლა მნიშვნელოვან ფინანსურ დანაკარგებს გამოიწვევს.

DoS შეტევის სახესხვაობიდან ერთ-ერთს წარმოადგენს მეთოდი ”უხეში ძალა” (brute-force attack) ინფორმაციული პაკეტების მასიური გაგზავნის დროს ამოქმედებულია ქსელის ყველა რესურსი და, შედეგად, ქსელი წყვეტს მუშაობას - ეს არის DoS შეტევის ვარიანტი, რომლის შესრულება ხდება

მეთოდით ”უხეში ძალა”. ინტერნეტში შეიძლება მოიძებნოს ისეთი პროგრამული საშუალებები, რომლებიც შეაძლებინებს ჰაკერს უსადენო ქსელში გამოიწვიოს ინფორმაციული პაკეტების ინტენსიური გადაცემა. ჰაკერს შეუძლია განახორციელოს DoS შეტევა მეთოდით ”უხეში ძალა” სერვერზე ქსელის სხვა კომპიუტერებიდან გამოუსადეგარი პაკეტების გაგზავნის გზით. ყოველივე ეს იწვევს ქსელში არამწარმოებლურ დანახარჯებს და ლეგიტიმურ მომხმარებლებს არ აძლევს საშუალებას გამოიყენოს ქსელში შესასვლელი შესაძლებლობა.

უსადენო ქსელების მუშაობის გაჩერების სხვა ხერხს წარმოადგენს მეთოდი ”შეგრძნების აღმოჩენა” (carrier sense access), რომლის დროსაც გამოიყენება მძლავრი რადიოსიგნალი. იგი ახშობს სხვებს ისე, რომ წვდომის წერტილები და ქსელის ინტერფეისის რადიოპლატები გამოუსადეგარი ხდება. თუმცა, ქსელზე შეტევის განხორციელების მცდელობა მძლავრი რადიოსიგნალის გამოყენებით შეიძლება ჰაკერისთვის აღმოჩნდეს მეტად სარისკო, ვინაიდან ასეთი შეტევის განხორციელებისას მძლავრი გადამცემი უნდა განთავსდეს იმ შენობის უშუალო სიახლოვეს, სადაც ფუნქციონირებს უსადენო ქსელი. აქედან გამომდინარე, უსადენო ქსელის მფლობელს შეუძლია აღმოაჩინოს ჰაკერი აღმომჩენი საშუალებების გამოყენებით, რომლებიც მიეკუთვნება ქსელური ანალიზატორების ჯგუფს. მას შემდეგ, რაც აღმოჩნდება წინასწარგანსაზღვრული ხარვეზების წყარო, მისი მფლობელი იძულებული გახდება შეწყვიტოს შეტევა, ან სულაც განსასჯელის სკამზე აღმოჩნდეს.

გარდა ამისა, Dos შეტევას ხელს უწყობს დაცვის ზოგიერთი მექანიზმი. მაგალითად, WPA (დაცული წვდომა Wi-Fi-სადმი, Wi-Fi Protected Access) მექანიზმმა შეიძლება გამოიწვიოს ”მომსახურებაზე უარი” სახეობის შეტევა. WPA ქსელის მომხმარებლები აუტენტიფიკაციისათვის იყენებენ მათემატიკურ ალგორითმებს. თუ რომელიმე მომხმარებელი შეეცდება მიიღოს მისადმი წვდომა და ერთი წამის განმავლობაში გააგზავნის

არაავტორიზებული მონაცემების ორ პაკეტს, WPA ჩათვლის, რომ გახდა შეტევის ობიექტი და ქსელის მუშაობას შეწყვეტს.

შედარებით მოქმედ დაცვას Dos შეტევის წინააღმდეგ წარმოადგენს უსაფრთხოების მკაცრი წესების შემუშავება და შესრულება, მაგალითად, როგორიც არის ბრანდმაუერების სისტემების დაყენება და განახლება, ანტივირუსული სისტემების მუდმივად განახლება, სიმბოლოების დიდი რაოდენობით პაროლების გამოყენება, არაგამოყენებადი ქსელური მოწყობილობების ქსელიდან გათიშვა და სხვა ყველა ის ქმედება, რომლებიც მკაცრად უნდა დაიცვას კორპორაციული ქსელის ყველა მომხმარებელმა.

რისკი მეხუთე - არაავტორიზებული წვდომა. უსადენო ქსელების უსაფრთხოება საგრძნობლად განსხვავდება მათი სადენიანი ანალოგის უსაფრთხოებისგან, რის მიზეზსაც ფიზიკური გარემოს ბუნება წარმოადგენს. უსადენო გარემოში კავშირისას გადაცემული და მიღებული სიგნალები ჰაერში მოგზაურობს. შესაბამისად, ნებისმიერ კვანძს, რომელიც გამგზავნი კვანძის გადაცემის დიაპაზონში მდებარეობს და იცის საოპერაციო სიხშირე და სხვა ფიზიკური დონის ატრიბუტები (მოდულაცია, კოდირება და ა.შ.), პოტენციურად შეუძლია სიგნალის გაშიფრვა იმგვარად, რომ გამგზავნს ან სავარაუდო მიმღებს არაფერი ეცოდინება აღნიშნული შეჭრის შესახებ. საპირისპიროდ ამისა, საკაბელო ქსელებში მსგავსი შეჭრა შესაძლებელია მხოლოდ იმ შემთხვევისას, თუ თავდამსხმელისთვის მისაწვდომი გახდება გადაცემის ფიზიკური საშუალება (სადენი, ბოჭკო და ა.შ.), რისთვისაც, როგორც წესი, აუცილებელია ასეთ საშუალებასთან მიერთება. ვინაიდან უსადენო ქსელები არ არის დამოკიდებული ინფრასტრუქტურაზე დაფუძნებულ რესურსებზე, როგორიცაა დენის სტაბილური წყარო, მაღალი სიხშირე, უწყვეტი კავშირი ან უცვლელი მარშრუტირება, მათ მიმართ თავდასხმების განხორციელება საკმაოდ ადვილია.

ამ პრობლემის გადაწყვეტის გზა ისაა, რომ მინიმუმ დაიშიფროს ის ინფორმაცა, რომელიც გადაეცემა უსადენო მოწყობილობებსა და საბაზისო

სადგურებს. დაშიფრვის პროცესის დროს მონაცემთა ბიტები იცვლება საიდუმლო გასაღების დახმარებით. რადგანაც გასაღები საიდუმლოა, ჰაკერს არ შეუძლია მონაცემების ამოშიფვრა. აქედან გამომდინარე, ეფექტური მექანიზმების გამოყენების ხარჯზე დაშიფვრას შეუძლია აამაღლოს მონაცემთა დაცულობა.

რისკი მეექვსე - ნაკადის მონიტორინგი.

არაავტორიზებული შეღწევის საწინააღმდეგოდ უსადენო ქსელში გამოიყენება ურთიერთქმედებითი აუტენტიფიკაცია, რომელიც ხორციელდება ქსელის მოწყობილობებსა და წვდომის წერტილებს შორის. აუტენტიფიკაცია - მოწმდება მომხმარებლის ან მოწყობილობის იდენტურობა. უსადენო ქსელში უნდა გამოიყენებოდეს მეთოდები, რომლის საშუალებითაც ხდება საბაზისო სადგურის დარწმუნება ქსელის მოწყობილობის იდენტურობაში და პირიქით. ეს აუცილებელია იმისთვის, რომ შეერთდნენ ლეგიტიმური საბაზისო სადგურები და მოწყობილობები. გარდა ამისა, წვდომის წერტილები უნდა გადიოდნენ აუტენტიფიკაციის პროცედურებს კომუტატორზე, რაც ქსელში გამორიცხავს მიდგმული წვდომის წერტილების გამოჩენას.

უსადენო ქსელის დაცვა შესაძლებელია გარედან რადიოსიგნალების შეღწევისაგან შენობის წინააღმდეგობის გაწევის უნარის უზრუნველყოფის გზით. არსებობს ზოგიერთი რეკომენდაცია, რომლის საშუალებითაც შესაძლებელია შენობაში რადიოსიგნალების ნაკადის შემცირება:

- თუ შენობის შიდა კედლებს გაჩნია ლითონის გამძლე ზედაპირი, სასურველია მისი დამიწება;

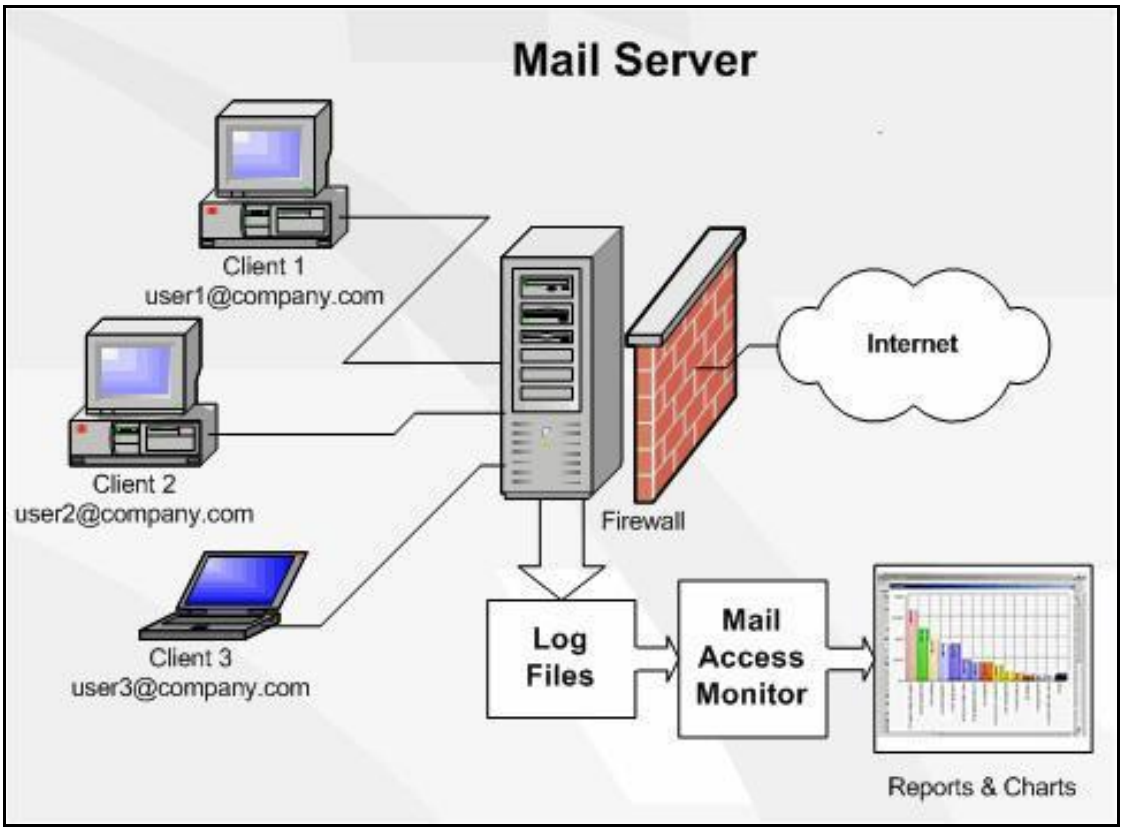
- სასურველია დაყენდეს თერმოიზოლაციის მქონე ფანჯრები და მოხდეს მისი მოლითონება;

_ შენობის შიდა და გარე კედლებზე გამოყენებული იქნას ლითონის მინარევის საღებავი;

- მოხდეს გადამცემის სიმძლავრის დარეგულირება ისეთი სახით, რომ მთლიანად გამოირიცხოს სიგნალის გაჟონვა ან მისი დონე დაიწიოს ისეთ მნიშვნელობამდე, რომ შესაძლებელი იქნეს ჰაკერის ადვილად გამოვლინება.

1.3. კორპორაციული საინფორმაციო სისტემების ინფორმაციული უსაფრთხოების უზრუნველყოფიდან მომდინარე საფრთხეები

კომპიუტერულ დამნაშავეებს გააჩნიათ მთელი „არსენალი მეთოდებისა“, რათა შეტევები განახორციელონ ინტერნეტის ერთ-ერთ უმნიშვნელოვანეს მომსახურების სფეროზე, როგორიცაა ელექტრონული ფოსტა (ნახ. 9).



ნახ. 9. საფოსტო სერვერის მუშაობის მაგალითი

ამ შემთხვევაში, უმეტეს წილად, გადასაცემი ინფორმაციის კოდირება არ ხდება და მისი გადაცემა ხორციელდება ჩვეულებრივი ტექსტით. საფოსტო სერვერი აანალიზებს წერილის მისამართის იმ ნაწილს, რომელიც

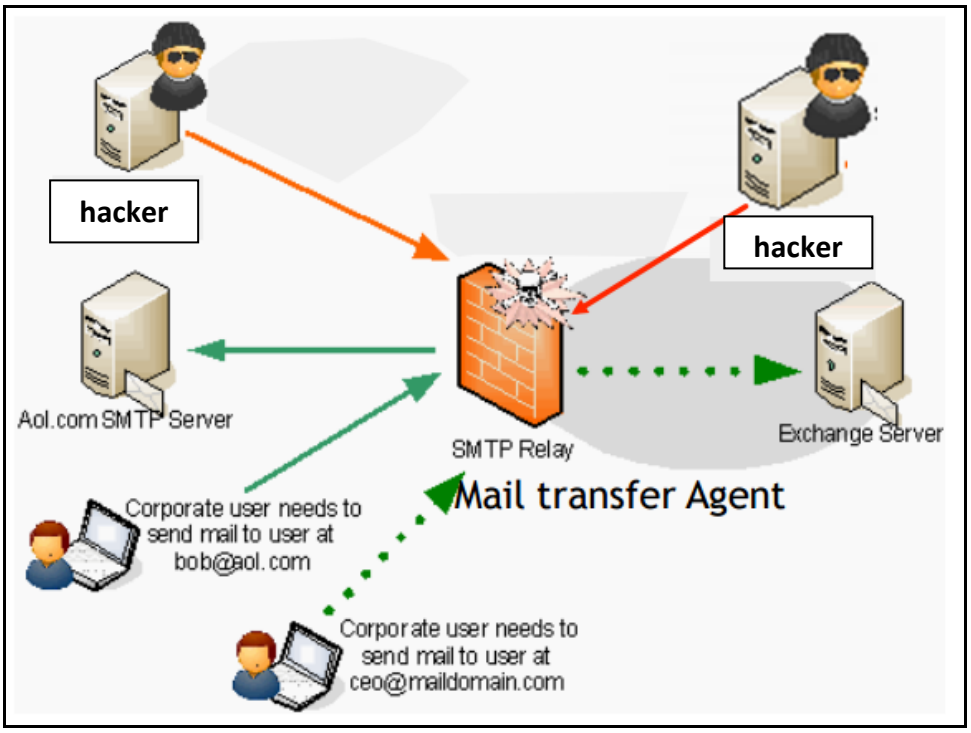
მოყვება ნიშანს - @. ამ ნაწილის საფუძველზე განისაზღვრება IP მისამართი იმ საფოსტო სერვერისა, რომელიც ემსახურება ადრესატს, მეორე ეტაპზე მყარდება კავშირი ამ სერვერთან და ხდება წერილის გადაცემა. ამ შემთხვევაში, იგულისხმება, რომ არ გამოიყენება წერილის ხელში ჩაგდების სპეციალური ტექნიკა. წერილი შეიძლება ხელში იქნას ჩაგდებული მხოლოდ გამგზავნისა და ადრესატის სერვერებზე. წერილის ხელში ჩაგდება შესაძლებელია გამგზავნსა და ადრესატს შორის ნებისმიერ წერტილში თუ გამოიყენება სპეციალური ტექნიკა და შუალედურ სერვერებზე დამატებითი პროგრამული უზრუნველყოფა.

თუ გადაცემის მომენტში ადრესატის (მიმღების) საფოსტო სერვერი მიუწვდომელია, მაშინ წერილის გადაგზავნა ხდება მიმღების რეზერვულ საფოსტო სერვერზე (თუ ასეთი სერვერის არსებობაზე ინფორმაცია ცნობილია), ან ელ. ფოსტის სერვერზე, რომელიც გამგზავნის სერვერზე ცნობილია, როგორც შუალედური სერვერი საფოსტო გზავნილებისა, შემდეგში გაგზავნის ფუნქცია გადადის ასეთ სერვერზე.

გავრცელებულია გამგზავნის ან მიმღების კომპიუტერში შეღწევის გამოყენება კონკრეტული შეტყობინების ხელში ჩასაგდებად. ამ შემთხვევაში, ლოკალურ კომპიუტერში ყენდება ფარული პროგრამა (მაგალითად პროგრამა „ტროას ცხენი“) ბოროტმზრახველის საფოსტო მისამართზე შემავალი და გამომავალი პირის ელ. ფოსტის ხელში ჩასაგდებად, მაგრამ გამოუსადეგარია პირთა ჯგუფის წინააღმდეგ სამოქმედოდ, ვინაიდან იზრდება მსხვერპლის კომპიუტერებზე გარეშე პირის ყოფნის აღმოჩენის რისკი.

კომპანიის საფოსტო ტრაფიკის ხელში ჩაგდებისას შეტევის ობიექტი, როგორც წესი ხდება კორპორაციის საფოსტო სერვერი. ამ შემთხვევაში შეტევათა განხორციელების ვარიანტები ძალზე დიდია, თუმცა შეიძლება აღმოჩნდეს, რომ საფოსტო სერვერის გატეხვა რაღაც მიზეზით შეუძლებელია. მაშინ ბოროტმზრახველს უნდა ჰქონდეს შეღწევის შესაძლებლობა კავშირგაბმულობის ხაზების შუალედურ კვანძებში,

რომლის მეშვეობითაც საფოსტო ტრაფიკი ვრცელდება კომპანიის დაცულ ქსელსა და ინტერნეტს შორის. აქ აუცილებელია გამოყენებულ იქნას სპეციალური პროგრამა, რომელიც გაანალიზებს მთელ ტრაფიკს ინტერნეტსა და კომპანიის ქსელს შორის და გამოყოფს შემავალ და გამავალ შეტყობინებებს (ნახ. 10).



ნახ. 10. საფოსტო სერვერზე შეტევის მაგალითი

ელ. ფოსტაზე ყურადღებას იმიტომ ვამახვილებთ, რომ ამ სერვისს გააჩნია მთელი რიგი უპირატესობანი, რაც განაპირობებს მის ფართოდ გავრცელებას. ეს უპირატესობებია:

ა) შეტყობინებათა მიწოდების მაღალი სიჩქარე;

ბ) ადრესატისათვის შეტყობინების გარანტირებული მიწოდება;

გ) კონფიდენციალობა.

როგორც პრაქტიკამ გვიჩვენა ძალზე მწვავედ დგას ინტერნეტ მომსახურების ინფორმაციის კონფიდენციალობის უზრუნველყოფა. დიდ საფრთხეს წარმოადგენს ელ.ფოსტის მისამართების „გაჟონვა“. გარდა ამისა პრობლემას წარმოადგენს ის, რომ სტანდარტული ფოსტის ოქმებით

გადაცემული ინფორმაცია ღიაა, თანაც არცერთი სტანდარტული ოქმი ელ. ფოსტისა (SMTP, POP3, IM, P4) არ შეიცავს დაშიფვრის მექანიზმს, რომელიც უზრუნველყოფდა მიმოწერის კონფიდენციალობას. ფაილები შეიძლება წაკითხული იქნას ბოროტმზრახველის მიერ. უფრო მეტიც, ადამიანთა უმეტესობას ავიწყდება, რომ ინტერნეტი ესაა საზოგადოებრივი ადგილი და რომ ელ.ფოსტა, სანამ ის მიაღწევს დანიშნულ ადგილს გაივლის რამოდენიმე კომპიუტერს და „მოგზაურობისას“ შეიძლება მოხდეს მისი პერლუსტრაცია. სამწუხაროდ მოყვანილი მაგალითებით არ ამოიწურება ქსელური შეტევების სახეები, ისინი ისევე მრავალფეროვანია, როგორც სისტემები, რომელთა წინააღმდეგაც ეს შეტევები ხორციელდება.

როგორც ზემოთ აღვნიშნეთ, ბოროტმზრახველი ცდილობს რა იპოვოს თავისი ქმედებებით თავისი ქმედებებით ქსელში სარგებელი, ხშირად მიმართავს პაროლებზე შეტევას, რომლისათვისაც იყენებს მთელ რიგ მეთოდებს: უბრალო გადარჩევა (brute force attak), „ტროას ცხენი“, IP - სპუფინგი და პაკეტების სნიფინგი. მიუხედავად იმისა, რომ მომხმარებლის სახელი და პაროლო შეიძლება მოპოვებულ იქნას IP-სპუფინგისა და პაკეტების სნიფინგით, ბოროტმზრახველები ცდილობენ ფართოდ გამოიყენონ სხვის ქსელში შეღწევის სხვადასხვა მეთოდები.

IP-სპუფინგი გაყალბებასთანაა დაკავშირებული. ბოროტმზრახველი, რომელიც იმყოფება კორპორაციის შიგნით, ან მის გარეთ, თავს ასაღებს ნებადართულ მომხმარებლად. ჩვეულებრივ IP-სპუფინგი შემოიფარგლება ყალბი ინფორმაციისა ან მავნე ბრძანებების ჩართვით ქსელში ცირკულირებად ინფორმაციის ნაკადში. ორმხრივი კავშირისათვის ბოროტმზრახველმა უნდა შეცვალოს მარშუტიზაციის მთელი ცხრილი, რათა მთელი ტრაფიკი მიმართოს ყალბ IP-მისამართზე. თუ ბოროტმზრახველი მოახერხებს შეცვალოს მარშუტიზაციის ცხრილი, მაშინ მას საშუალება ეძლევა მიიღოს ყველა პაკეტი და უპასუხოს მათ, როგორც სანქცირებულმა მომხმარებელმა.

აღნიშნული სახის შეტევის შესუსტება (და არა თავიდან აცილება) შესაძლებელია შემდეგი მეთოდების გამოყენებით: დაშვების კონტროლი- ექსპერტთა აზრით, უმარტივეს მეთოდად IP-სპუფინგის ასაცილებლად ითვლება დაშვების კონტროლის სისტემის სწორად ორგანიზება.

დამატებითი აუტენტიფიკაციის საუკეთეო საშუალებად ითვლება კრიპტოგრაფია, მაგრამ თუ ეს შეუძლებელია, მაშინ კარგი შედეგის მიღება შესაძლებელია ე.წ. ორფაქტორიანი აუტენტიფიკაციით ერთჯერადი პაროლების გამოყენებით.

რაც შეეხება პაკეტების სნიფერს - ესაა გამოყენებითი პროგრამა, რომელიც იყენებს ქსელურ რუკას და მუშაობს promiscuous mode რეჟიმში (ამ რეჟიმში ყველა პაკეტს, რომლებიც მიიღება ფიზიკური არხებით, ქსელური ადაპტერი აგზავნის გამოყენებით პროგრამასთან). ამ დროს სნიფერი მოიტაცებს ყველა ქსელურ პაკეტს, რომელიც გადაიცემა გარკვეული დომენის გავლით. დღეისათვის სნიფერები ქსელში მუშაობენ სავსებით კანონიერად. ისინი გამოიყენებიან ქსელის დიაგნოსტიკისა და ტრაფიკის ანალიზისათვის. მაგრამ იმის გამო, რომ ზოგიერთი გამოყენებითი პროგრამები გადასცემენ მონაცემებს ტექსტური ფორმით (telnet, FTP, SMTP, POP3 და ა.შ.), სნიფის მეშვეობით შეიძლება გავიგოთ სასარგებლო ინფორმაცია, ზოგჯერ კონფიდენციალურიც (მაგ: მომხმარებელთა სახელები და პაროლები). ექსპერტები პაკეტების სნიფინგისგან მომდინარე საფრთხის შესამცირებლად გვთავაზობენ შემდეგ საშუალებებს:

აუტენტიფიკაცია - აუტენტიფიკაციის საშუალებები პაკეტების სნიფინგისგან დაცვის ერთ-ერთ ძლიერ საშუალებადაა აღიარებული;

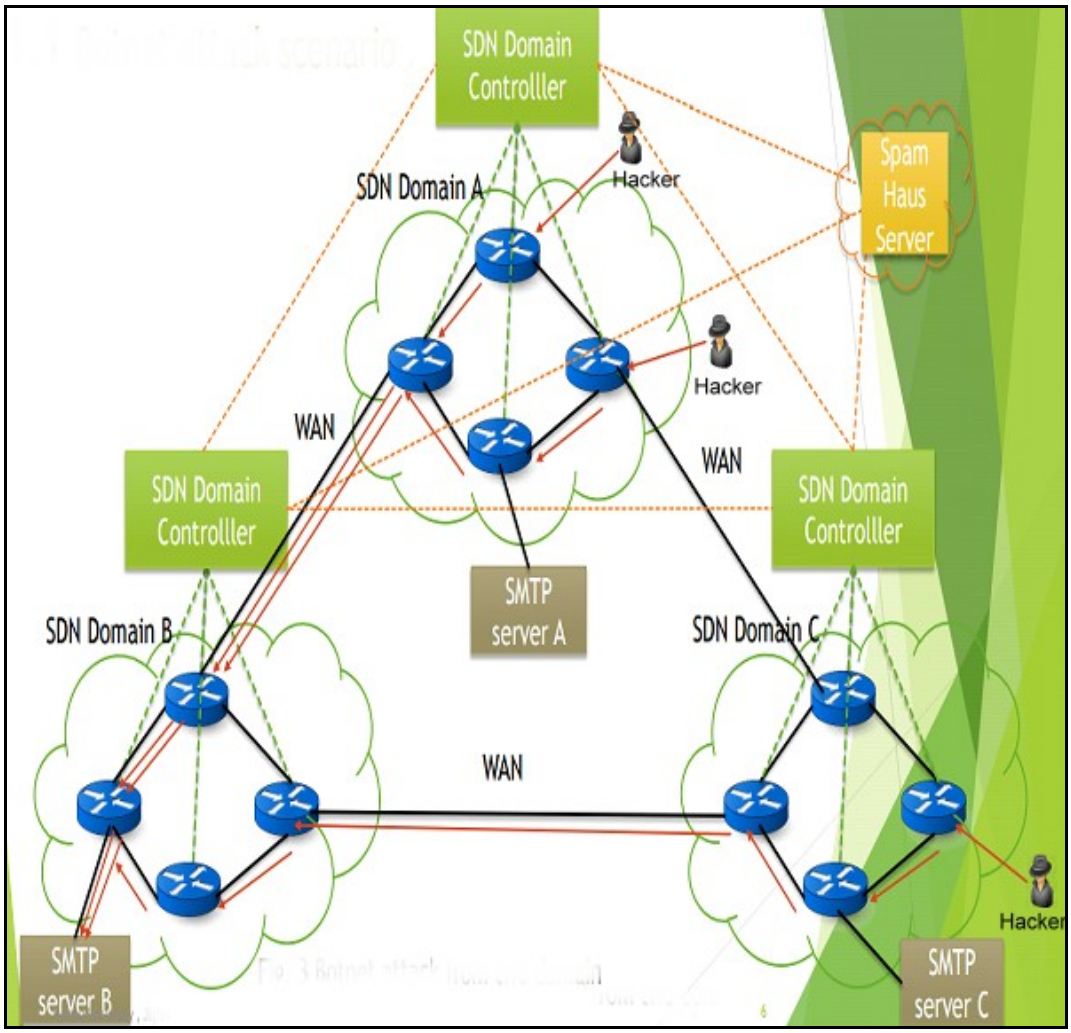
კომუტირებადი ინფრასტრუქტურა - იგულისხმება ქსელში კომუტირებადი ინფრასტრუქტურის შექმნა;

ანტი-სნიფერები - ესაა სპეციალური პროგრამები ან აპარატურული საშუალებები, რომელთაც შეუძლიათ ქსელში მომუშავე სნიფების ამოცნობა;

კრიპტოგრაფია - ამ შემთხვევაში ინფორმაცია სრულადაა დაცული გამჟღავნებისაგან.

ე.წ. ”ადამიანი შუაში” (Man-in-the-Middle) ტიპის შეტევის განხორციელებისათვის ბოროტმზრახველს სჭირდება დაშვება ჰქონდეს ქსელით გადაცემულ პაკეტებთან. ასეთი დაშვება ყველა პაკეტთან, რომელიც გადაიცემა პროვაიდერთან ნებისმიერ სხვა ქსელში, შეიძლება მიიღოს, მაგალითად, ამ პროვაიდერის თანამშრომელმა. ამ ტიპის შეტევის განსახორციელებლად ხშირად გამოიყენება პაკეტების სნიფერები, სატრანსპორტო და მარშუტიზაციის ოქმები.

გამოყენებითი პროცესების დონეზე შეტევებიც მრავალნაირია. ყველაზე უფრო გავრცელებულია პროგრამული უზრუნველყოფების (sendmail, HTTP, FTP) სუსტი მხარეების გამოყენება, რომელთა მეშვეობითაც ბოროტმზრახველებს შეუძლიათ შეაღწიონ კომპიუტერებში, იმ მომხმარებლების სახელით, რომლებიც უშუალოდ მუშაობენ ამ გამოყენებით პროგრამებთან (ჩვეულებრივ ეს არის არა უბრალო მომხმარებელი, არამედ პრივილეგირებული, სისტემური დაშვების მქონე ადმინისტრატორი). გამოყენებით დონეზე განხორციელებული შეტევებისას პრობლემას წარმოადგენს, ის რომ ბოროტმზრახველები ხშირად იყენებენ იმ პორტებს, რომელთაც ქსელთშორისი ეკრანის გავლის ნება აქვთ. ამ დონეზე შეტევების სრულად აცილება შეუძლებელია. ჰაკერები ძალზე ხშირად აქვეყნებენ ინტერნეტში მონაცემებს სხვადასხვა პროგრამების სუსტი მხარეების შესახებ. ამ შემთხვევაში მთავარია სისტემური ადმინისტრირების სწორად წარმართვა (ნახ. 11).



ნახ. 11. კორპორაციულ ქსელზე შეტევის მაგალითი

ქსელური შეტევის სახეებს განეკუთვნება ქსელური დაზვერვა, რომელიც გულისხმობს ქსელზე საყოველთაოდ ხელმისაწვდომი მონაცემების და გამოყენებითი პროცესების მეშვეობით, რომელიმე ქსელის წინააღმდეგ შეტევის განხორციელებისას ბოროტმზრახველი, როგორც წესი, ცდილობს მასზე მიიღოს რაც შეიძლება მეტი ინფორმაცია. ქსელური დაზვერვა ხორციელდება DNS შეკითხვათა ფორმით, ექო-ტესტირებით (ping sweep) და პორტების სკანირებით. DNS შეკითხვები საშუალებას იძლევიან გაგებული იქნას თუ ვინ ფლობს ამა თუ იმ დომენს და ამ დომენებს რა მისამართები აქვთ მიკუთვნებული. ექო-ტესტირება DNS-ის მეშვეობით გაგებული მისამართებისა საშუალებას იძლევა დავინახოთ თუ მოცემულ მომენტში რელურად რომელი ჰოსტები მუშაობენ. ჰოსტების სიის მიღების

შემდეგ ბოროტმზრახველი მიმართავს პორტების სკანირებას, რათა დადგინდეს იმ მომსახურებათა სრული სია, რომლებსაც ეს ჰოსტები ახორციელებენ და ბოლოს ბოროტგამზრახველი აანალიზებს ჰოსტებზე რეალიზებულ გამოყენებით პროცესებს, რის შედეგადაც მოიპოვება ინფორმაცია, რომელზე დაყრდნობითაც ხდება გატეხვა.

ხშირ შემთხვევებში ადგილი აქვს ქსელში არსებული ნდობის ბოროტად გამოყენებას. ასეთი ნდობის ბოროტად გამოყენების კლასიკურ მაგალითს წარმოადგენს სიტუაციები კორპორაციული ქსელების პერიფერიულ ნაწილში. ქსელების ამ ნაწილში ხშირად განთავსებულია DNS, SMTP და HTTP სერვერები. ვინაიდან ისინი ეკუთვნიან ერთსა და იმავე სეგმენტს და ენდობიან ერთმანეთს, ამიტომ ერთ-ერთი მათგანის გატეხვა იწვევს სხვების გატეხვასაც. სხვა მაგალითს წარმოადგენს სისტემა, ქსელთაშორისი ეკრანის გარე მხარეს და აქვს ნდობა ეკრანის შიდა მხარეს არსებული სისტემისა. ამ შემთხვევაშიც გარე სისტემის გატეხვით, ბოროტმზრახველს, არსებული ნდობის გამოყენებით ეძლევა საშუალება შეაღწიოს სისტემაში, რომელიც დაცულია ქსელთაშორისი ეკრანით.

ასეთი ნდობისას არსებული გატეხვის რისკი შეიძლება შემცირდეს თუ გამკაცრდება ნდობის დონის კონტროლი საკუთარი ქსელის ფარგლებში.

ნდობის ბოროტად გამოყენების სახესხვაობას წარმოადგენს პოსტების გადამისამართება, როცა გატეხილი პოსტი გამოიყენება ქსელთაშირისი ეკრანის გავლით იმ ტრაფიკის გადასაცემად, რომელიც სხვა შემთხვევაში აუცილებლად დაწუნებული და ბლოკირებული იქნებოდა.

არ შეიძლება არ შევეხოთ ისეთ მავნე პროგრამებს, რომლებიც ავრცელებენ კომპიუტერულ ვირუსებს და უდიდეს ზიანს აყენებენ, როგორც ცალკეულ მომხმარებლებს, აგრეთვე მთლიანად იმ საქმიან სამყაროს, რომელიც ინტენიურად სარგებლობს ინტერნეტით. აგრეთვე გარკვეულწილად გაიზარდა „ტროას ცხენის“ მსგავსი პროგრამების გავრცელება, ასევე იმ ვირუსებისა, რომელთა მეშვეობითაც ხდება ფულის მოპარვა ინტერნეტ-ანგარიშებიდან (საგადამხდელო სისტემაში - მაგ: Web

Money) ამასთან ვირუსები იწერება ახალი ოპერაციული სისტემისათვისაც (მაგ: Linux). ფაილების უფასო გაცვლის სისტემისათვის და ა.შ. არ შეიძლება არ დავეთანხმოთ ექსპერტებს, რომ ყოველთვის მოიძებნება ვირუსის დაწერისა და გავრცელების მსურველი და მიუხედავად აღნიშნული ტენდენციისა დაუშვებელია ყურადღების შესუსტება ამ სახის კომპიუტერული დანაშაულებების მიმართ.

1.4. კორპორაციული საინფორმაციო სისტემების უსაფრთხოების უზრუნველყოფის ავტომატიზებული სისტემის ძირითადი ამოცანები

კორპორაციულ საინფორმაციო სისტემებში უსაფრთხოების უზრუნველყოფის პრობლემისადმი კომპლექსური მიდგომა ეფუძნება კონკრეტულ კსს-სთვის შემუშავებულ უსაფრთხოების პოლიტიკას, კერძოდ მეტი უსაფრთხოებისათვის საურველია შეიქმნას ავტომატიზებული სისტემა, რომელიც მოახდენს კსს-ის დაცვის საშუალებების მუშაობის ეფექტურობის რეგლამენტირებას. იგი მოიცავს ინფორმაციის დამუშავების ყველა თავისებურებას, განსაზღვრავს რა მთელი სისტემის ქცევას განსხვავებულ სიტუაციებში. კორპორაციული ქსელის უსაფრთხოების საიმედო სისტემის შექმნისთვის აუცილებელია განისაზღვროს ის ძირითადი ამოცანები, რომლის განხორციელების შედეგადაც მოხდება კსს-ში ინფორმაციული უსაფრთხოების გაძლიერება.

ავტომატიზებული სისტემის ძირითადი ამოცანების შემუშავება იწყება მონაცემების ხელით დამუშავების პროცედურების გამოკვლევით, რათა შესწავლილი და განზოგადებული იქნას ის სირთულეები, რომელსაც აწყდება მომხმარებელი. ასეთი გამოკვლევა ზოგადი ხასიათისაა და მდგომარეობს სიძნელეების გამოვლენაში და არა მათი მიზეზის დადგენაში. თავდაპირველად ხდება მართვის არსებული პროცედურების ზოგადი

გამოკვლევა, ხოლო შემდგომში მოხდება მართვის იმ თითოეული ამოცანის ცალ-ცალკე შესწავლა, რომლის ავტომატიზაციაც არის გათვალისწინებული.

კორპორაციულ საინფორმაციო სისტემებში უსაფრთხოება და მომსახურების ხარისხი უკანასკნელ ხანებში უაღრესად მნიშვნელოვანი და აქტიური კვლევის საგანი გახდა, რის მიზეზსაც მონაცემთა პაკეტების გადაცემის მხარდაჭერის მზარდი მოთხოვნა წარმოადგენს. ადეკვატური უსაფრთხოების გარეშე ორგანიზაციები თავს აარიდებენ კორპორაციული ქსელების გამოყენებას. უსაფრთხოების საკითხები ქსელებში მნიშვნელოვან დაბრკოლებას წარმოადგენს მათივე ადაპტირებისთვის. შესაბამისად, მსგავსი ქსელების უსაფრთხოება მნიშვნელოვანი სფეროა, რაც რეაგირებას მოითხოვს, თუკი ასეთი ქსელები ფართოდ იქნება გამოყენებული. აუცილებელია, რომ აღნიშნული სფეროს მკვლევარებმა მოახდინონ ღია პრობლემების იდენტიფიცირება და უზრუნველყონ შესაბამისი გადაწყვეტილებები ამ პრობლემებისთვის. თითოეული ასეთი მცდელობა კორპორაციულ ქსელს ოდნავ უფრო უსაფრთხოს ხდის. წინამდებარე ნაშრომის მიზანს წარმოადგენს ის, რომ შემუშავდეს მთელი რიგი ღონისძიება, რომლებიც აამაღლებს კორპორაციული ქსელების უსაფრთხოებას და მისი საშუალებით მოხდება მოცილებული სამუშაო ადგილების მართვა.

ზემოთ აღნიშნული მიზნიდან გამომდინარე, ნაშრომში ყურადღება ექცევა ისეთი ამოცანების გადაჭრას, როგორიცაა:

- კორპორაციულ ქსელებში ინფორმაციული პაკეტების მარშრუტი-ზაციის უსაფრთხოების ამაღლება;

- დაშიფვრისა და აუტენტიფიკაციის მექანიზმების გამკაცრება;

- კორპორაციულ საინფორმაციო სისტემებში მთლიანი ქსელის სკანირება, ანალიზის ჩატარება, მავნე პროგრამების (Netcut, HackRF, WifiKill და სხვა) გამოვლენა და უსაფრთხოების ამაღლების მიზნით ახალი მეთოდების დამუშავება;

- მოცილებული სამუშაო ადგილების (ადგილობრივი თუ რეგიონული ოფისები) ადმინისტრირება და მართვა კორპორაციული ქსელების გამოყენებით;

- სისტემაში გამოყენებული აპარატურული მოწყობილობების პარამეტრების დისტანციური მართვა და ადმინისტრირება;

- სხვადასხვა ადგილობრივ თუ მოცილებულ ობიექტზე წვდომის გრაფიკების დამუშავება და ანალიზი (ერთიან სისტემაში მონაწილე მხარეების დონეზე);

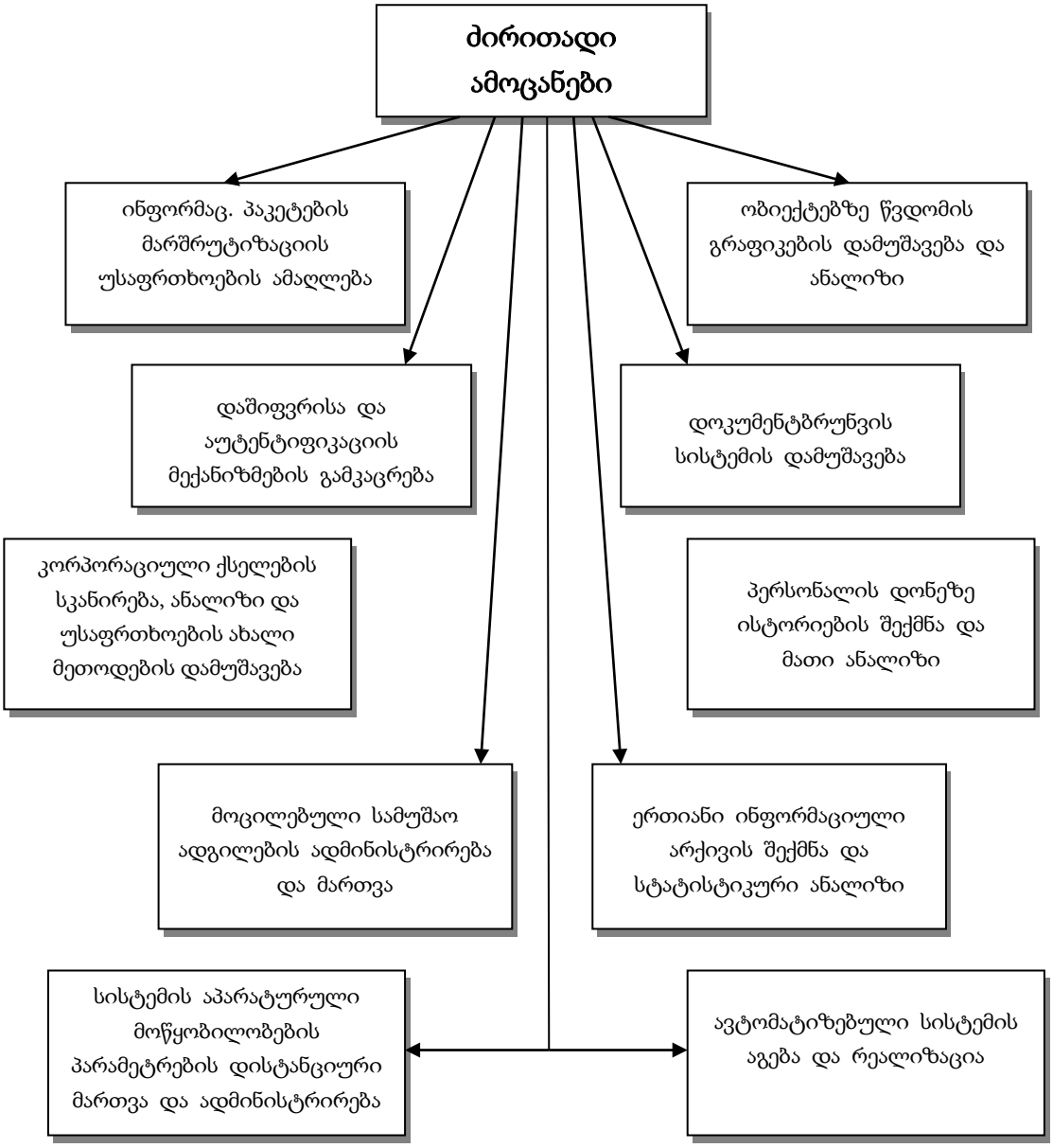
- დოკუმენტბრუნვის სისტემის აგება (პერსონალის სამუშაო დროის აღრიცხვა, მათთვის აპარატურულ მოწყობილობებთან წვდომის გრაფიკების დამუშავება, ორგანიზაციის შემოსული და გასული კორესპონდენციების აღრიცხვა და სხვა);

- თითოეული პერსონალის დონეზე ისტორიების შექმნა და ანალიზი;

- ერთიანი ინფორმაციული არქივის შექმნა და მის საფუძველზე სტატისტიკური ანალიზის ჩატარება ცხრილებისა და დიაგრამების სახით;

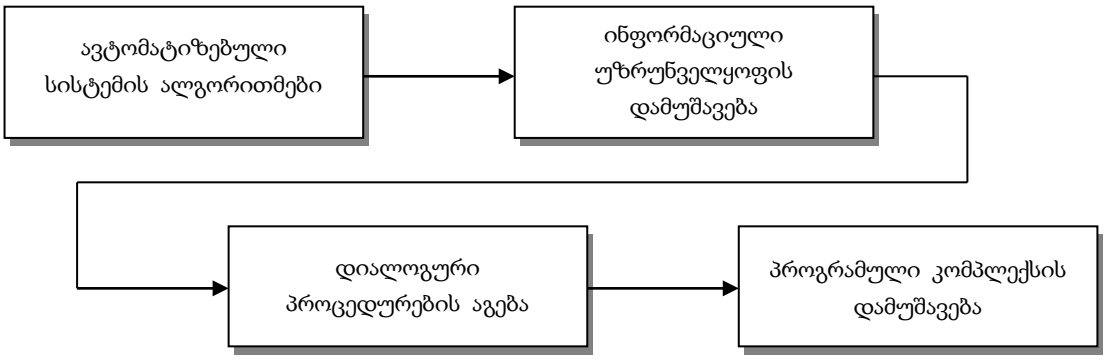
- ავტომატიზებული სისტემის აგება და რეალიზაცია.

უსაფრთხოების სისტემის ძირითადი ამოცანების სტრუქტურა მოცემულია (ნახ.12)-ზე.



ნახ. 12. უსაფრთხოების სისტემის ძირითადი ამოცანები

პროცესები (ნახ.13).



ნახ. 13. ავტომატიზებული სისტემის დაპროექტების მთავარი ეტაპები

აღნიშნული პროცედურების ჩატარების შემდეგ დამუშავდება ავტომატიზებული სისტემის პროგრამული კომპლექსი და მისი სტრუქტურა. შეიქმნება პროგრამული კომპლექსის კლასები, კონსტრუქტორები, პროცედურები, ფუნქციები და მეთოდები.

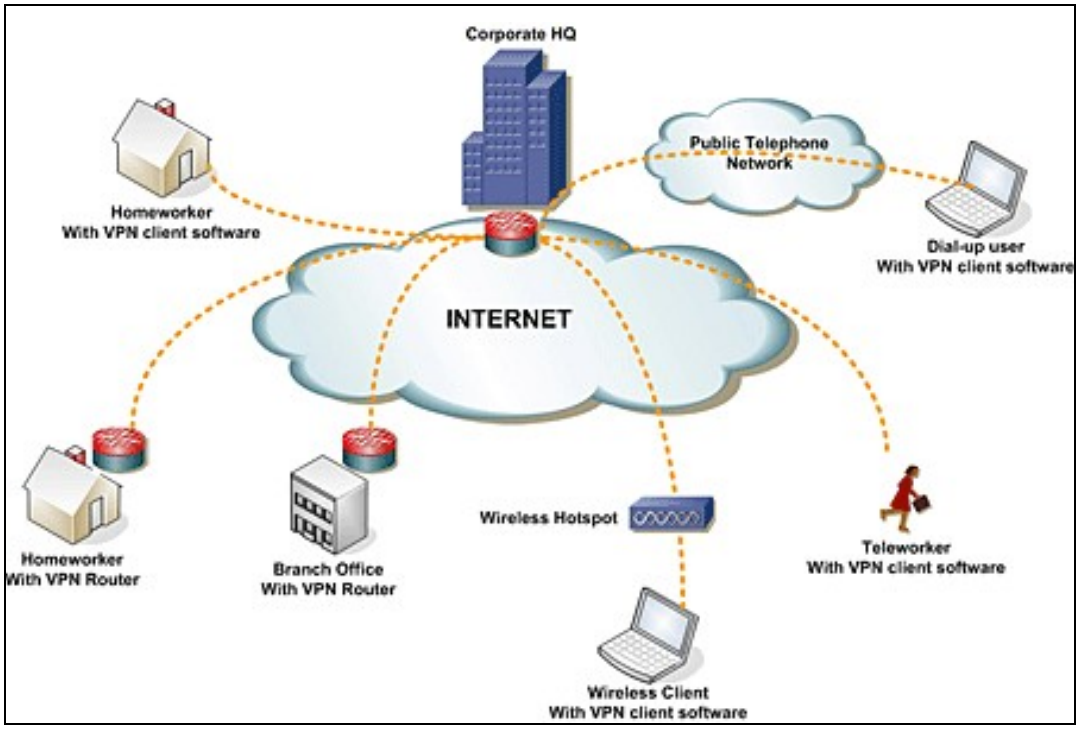
თავი 2. კორპორაციული საინფორმაციო სისტემის უსაფრთხოების უზრუნველყოფის მეთოდების და ალგორითმების დამუშავება

2.1. VPN აგების კონცეფცია, ქსელის ფუნქციები და მათი კლასიფიკაცია

ინტერნეტის განვითარებასთან ერთად გვაქვს საჭიროება დავიცვათ მონაცემები, რომელსაც გადავცემთ ღია ქსელში, როგორიცაა ინტერნეტი. არავინაა დაცული იმისგან, რომ მის ტრაფიკს ბოროტმოქმედი სხვადასხვა ტექნიკის საშუალებით ხელში ჩაიგდებს და გამოიყენებს ცუდი მიზნებისთვის. ამ საფრთხისგან თავის დასაცავად საჭიროა ვიზრუნოთ გადაცემული მონაცემების დაცულობაზე. დაუცველ ქსელში მონაცემების გადაცემისთვის გამოიყენება სხვადასხვა დაცული პროტოკოლი როგორებიცაა HTTPS,SSH,TLS,IPSEC და სხვა.

ერთ-ერთი ასეთი დაცული ტექნოლოგიაა VPN, რომელიც თავის მხრივ იყენებს სხვადასხვა პროტოკოლებს. თავდაპირველად VPN არ უზრუნველყოფდა მონაცემების ავთენტურობასა და შიფრაციას. მაგალითისთვის GRE (Generic Routing Encapsulation) ტუნელირების პროტოკოლი, რომელიც შეიმუშავა კომპანია Cisco_მ და წარმოადგინა 1994 წელს, გვაძლევს საშუალებას ორ დაშორებულ ქსელს ჰქონდეს წვდომა ერთმანეთის შიდა რესურსებზე, მაგრამ არ უზრუნველოფს არანაირი სახის უსაფრთხოებას. იმ შემთხვევაში თუ ბოროტმოქმედი მოახერხებს GRE ტუნელში გადაცემული ტრაფიკის შეგროვებას მარტივად ნახავს გადაცემულ მონაცემებს. დაუშიფრავი VPN-ის სხვა მაგალითებია: ATM(Asynchronous Transfer Mode), PVC (permanent virtual circuits) და MPLS(Multiprotocol Label Switching) ტექნოლოგიები. დღეს დღეობით როდესაც ვსაუბრობთ VPN_ზე თავისთავად მოიაზრება, რომ ვგულისხმობთ

ისეთი სახის VPN-ს, სადაც მონაცემები უსაფრთხოება უზრუნველყოფილია გადაცემის დროს (ნახ.14).



ნახ. 14. ვირტუალური კერძო (დაცული) ქსელი

ძირითადად არსებობს VPN-ის ორი ტიპი დაშორებული წვდომის (remote access) და ოფისი ოფისთან (site to site).

დაშორებული VPN-ის შემთხვევაში კავშირი არ არის სტატიკური, შესაძლებელია კავშირის პარამეტრები შეიცვალოს დინამიურად. მაგალითად თანამშრომელს რომელიც არის მივლინებაში და დრო და დრო ჭირდება წვდომა კორპორატიულ სერვისებთან ვერ ექნება მუდმივად მომართული VPN კავშირი. მას შეიძლება შეეცვალოს IP მისამართი. ამიტომ კავშირის წამოწყება უნდა შეეძლოს თანამშრომელს საჭიროების დროს, რომელსაც წინასწარ ეცოდინება VPN სერვერის მონაცემები, რომელიც იქნება უცვლელი.

ოფისი ოფისთან (site to site) VPN კავშირი ძირითადად გამოიყენება ორი ოფისის ერთმანეთთან დასაკავშირებლად. ამ დროს კონფიგურაცია სტატიკურია და ორივე მხარემ იცის ერთმანეთის მონაცემები.

არსებობს VPN-ის სხვადასხვა პროტოკოლი რომელიც დღეს გამოიყენება. ეს არის მათი არასრული ჩამონათვალი:

PPTP

L2TP/ipsec

OpenVPN

SSTP

SofthEther

WireGuard

PPTP VPN შექმნა კორპორაცია მაიკროსოფტმა 1996 წელს, მისი RFC გამოქვეყნდა 1999 წელს. ის იყენებს GRE ტუნელს. ის ვეღარ უზრუნველყოფს დაცვის იმ დონეს, რაც მისაღებია დღეს. მისი კონფიგურაციის სიმარტივიდან გამომდინარე ზოგიერთი მას დღესაც იყენებს. აგენტი ჩაშენებულია Windows სისტემაში რაც ხსნის აგენტის დაყენების საჭიროებას ჰოსტზე. იყენებს 1723/tcp პორტს. დღეისთვის არსებობს ცნობილი მოწყვლადობები PPTP_სთვის.

L2TP/IPSEC არის ტუნელირების პროტოკოლი, რომელსაც თავის მხრივ არ გვთავაზობს შიფრაციას და კონფიდენციალურობას. მაგრამ შესაძლებელია IPSEC-თან ერთად გამოყენება, რომელიც გვთავაზობს მაღალი დონის უსაფრთხოებას. იყენებს 500/udp, 1701/udp, 4500/udp პორტებს. არ არსებობს ცნობილი მოწყვლადობა, რომელიც ეჭვქვეშ დააყენებდა ამ პროტოკოლის უსაფრთხოებას.

OpenVPN არის ღია კოდის მქონე პროტოკოლი. ის მუშაობს როგორც UDP ასევე TCP პროტოკოლებზე. იყენებს SSL/TLS პროტოკოლს, ჩუმათობით მუშაობს 1194/UDP-ზე მაგრამ შეგვიძლია მივუთითოთ ნებისმიერი სხვა პორტი. აღნიშნული თვისება გამოსადეგია ისეთ შემთხვევებში, როდესაც შეზღუდულია გამავალი პორტების გამოყენების შესაძლებლობა. სხვა პროტოკოლებისგან გამოირჩევა გადაცემის სისწრაფით. ამ ეტაპისთვის პროტოკოლისთვის არ არსებობს ცნობილი მოწყვლადობა.

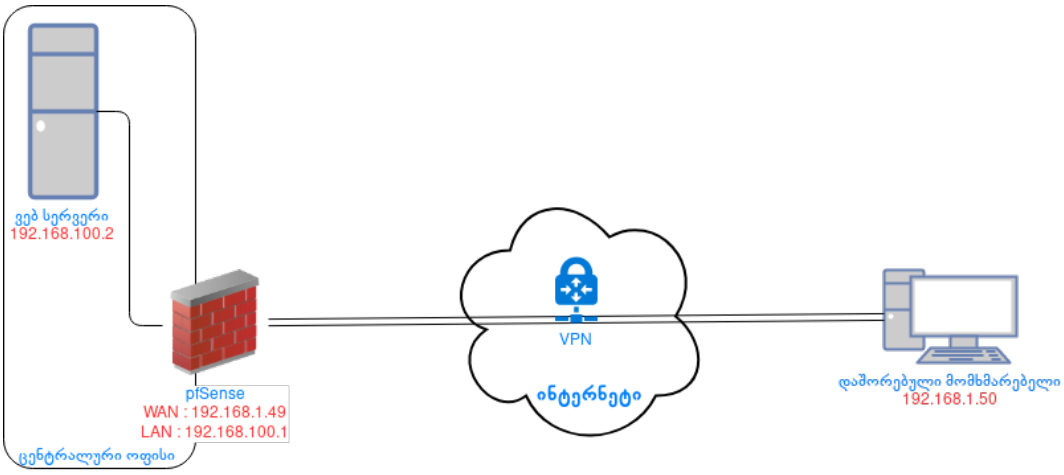
SSTP არის კომპანია მაიკროსოფტის მიერ დაპატენტებული VPN ტექნოლოგია. იყენებს SSL/TLS ტექნოლოგიას. SSTP პროტოკოლი ინტეგრირებულია მაიკროსოფტის ოპერაციულ სისტემებში, რაც ამარტივებს მის კონფიგურაციას კლიენტებზე. სხვა ოპერაციულ სისტემებზე არ არსებობს ჩაშენებული აგენტი. საჭიროა სხვა მწარმოებლების/დეველოპერების მიერ შექმნილი კლიენტის დაყენება. ამ დროისთვის არ არსებობს ცნობილი მოწყვლადობა SSTP პროტოკოლისთვის.

SoftEther არის ღია კოდის მქონე VPN სერვერი, რომელსაც აქვს სხვადასხვა პროტოკოლების მხარდაჭერა: OpenVPN,SSTP,L2TP/ipsec და SofthEther VPN პროტოკოლი. ის შექმნა დაიიუ ნობორიმ (Daiyuu Nobori) 2014 წელს. მისი "ასაკის" გამო დიდი პოპულარობით არ სარგებლობს სხვა VPN-ებთან შედარებით. ამ ეტაპისთვის არ არსებობს მისი ცნობილი მოწყვლადობა.

WireGuard არის ღია კოდის მქონე პროტოკოლი. რომელიც საშუალებას გვაძლევს შევქმნათ point to point კავშირები. ის ეშვება როგორც ლინუქსის კერნელის მოდული და შესაბამისად გვთავაზობს უკეთეს წარმადობას ვიდრე IPSEC და OpenVPN პროტოკოლები. ჩამოთვლილიდან ის ყველაზე "ახალგაზრდა" პროტოკოლია, რის გამოც არ არის ფართოდ გამოყენებული. ამ დროისთვის ის არ არის ხელმისაწვდომი Windows პლატფორმაზე.

როგორც ვხედავთ VPN პროტოკოლების ფართო სპექტრი არსებობს. ცალსახა "გამარჯვებული" პროტოკოლებს შორის არ გვაქვს. ყველაზე ხშირად გამოიყენება L2TP/IPSEC. OpenVPN პროტოკოლი არ არის ფართოდ დანერგილი ენტერპრაიზ დონის უსაფრთხოების სისტემებში. მაგრამ გვაქვს ღია კოდის მქონე სისტემები სადაც ის ხშირად გამოიყენება. ერთ-ერთი ასეთი სისტემაა pfSense რომელსაც აქვს OpenVPN პროტოკოლის მხარდაჭერა. ქვემოთ განვიხილავ VPN სერვერის კონფიგურაციას pfSense პლატფორმაზე.

არსებობს VPN ტოპოლოგიის განზოგადებული დიაგრამა. მსგავსი ტოპოლოგია ხშირად გამოიყენება ყოველდღიურობაში. ვინაიდან ტოპოლოგია აწყობილია ლაბორატორიაში, გამოყენებულია შიდა დამისამართება. თუმცა ეს არ ცვლის VPN_ის კონფიგურაციის არსს (ნახ.15).



ნახ. 15. VPN ტოპოლოგიის განზოგადებული დიაგრამა

როგორც ტოპოლოგიიდან ჩანს გვყავს დაშორებული მოხმარებელი, რომელსაც ჭირდება ჰქონდეს კავშირი სათაო ოფისში არსებულ რესურსთან. ვებ სერვერი თავის მხრივ არ არის წვდომადი გარედან(ინტერნეტიდან) და მისი გამოყენება შეიძლება მხოლოდ ოფისიდან. ამ პრობლემების მოსაგვარებლად სხვადასხვა ხერხი არსებობს, ერთ-ერთია VPN. ოფისის მხარეს პერიმეტრზე დგას pfSense ფაერვოლი რომელზეც დავაკონფიგურირებთ OpenVPN სერვერს მომხმარებელი/პაროლი+ სერთიფიკატის აუთენთიფიკაციით. აღნიშნული ხერხი არის ყველაზე მეტად დაცული. მოხმარებელს ჭირდება გამოიყენოს სერთიფიკატი და ამასთან ერთად იცოდეს მომხმარებელი/პაროლის კომბინაცია.

აქ მოცემულია იმ ნაბიჯების ჩამონათვალი, რომელიც საჭიროა ჩვენი მიზნის წარმატებულად განხორციელებისათვის.

- სერთიფიკატის ავტორიტეტის შექმნა.

- სერთიფიკატის შექმნა OpenVPN სერვერისთვის.

- მომხმარებლის შექმნა (რომლითაც კლიენტი გაივლის ავტორიზაციას).

- OpenVPN სერვერის შექმნა (remote access certificate+user/pass access).

- OpenVPN აგენტის საინსტალაციო პაკეტის/კონფიგურაციის ექსპორტი.

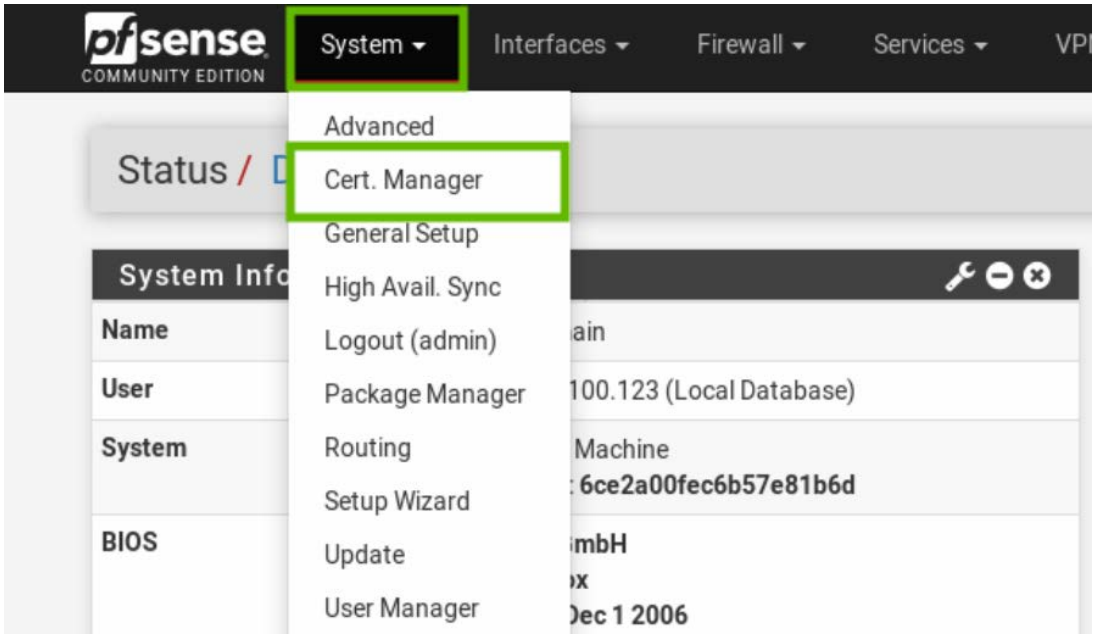
- VPN სერვერის დაშვების წესის შექმნა ფაერვოლში.

- ტესტირება.

ავაწყოთ კონფიგურაცია და მივყვეთ შემდეგ მიმდევრობას:

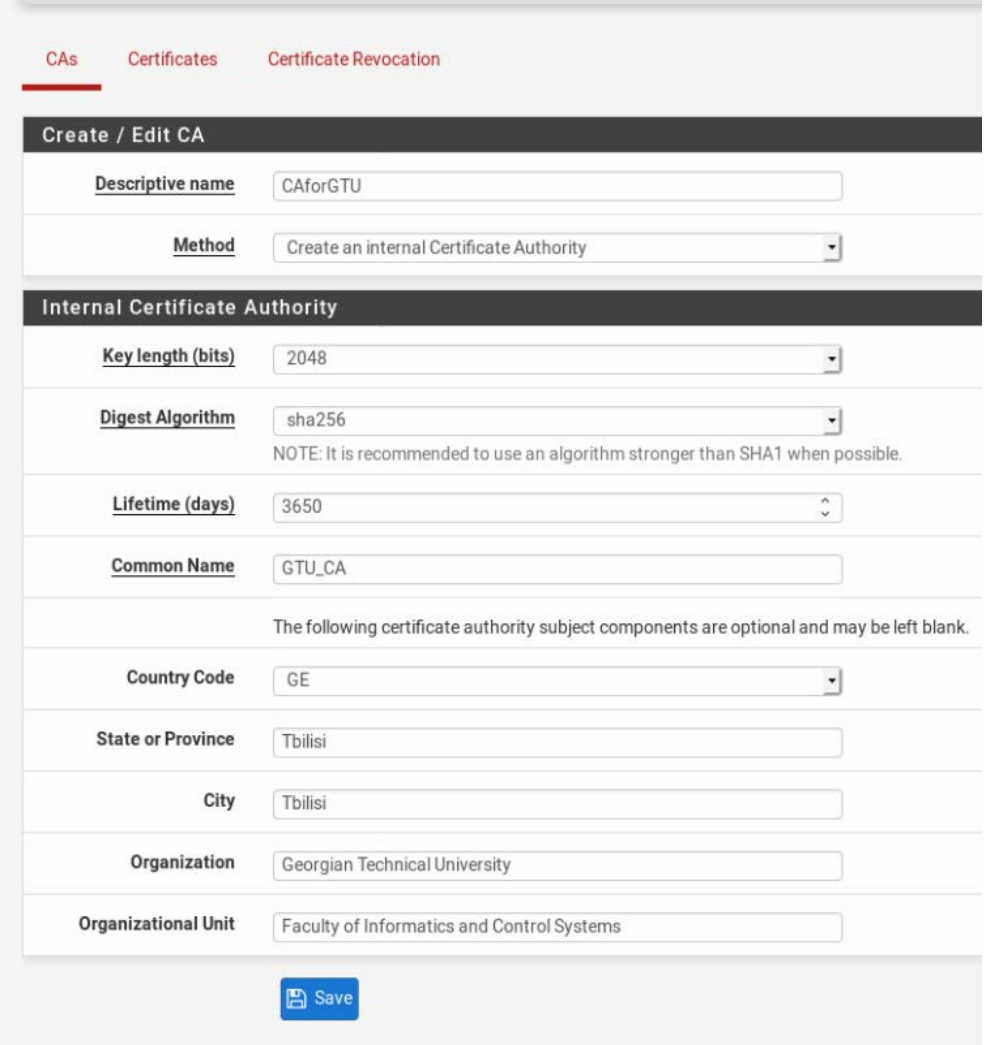
1. სერთიფიკატის ავტორიტეტის შექმნა

პირველ რიგში დავუკავშირდეთ სერტიფიკატების მენეჯერს (ნახ.16).



ნახ. 16. სერტიფიკატების მენეჯერი

შევქმნათ ეგრედ წოდებული რუთ სერთიფიკატის ავტორიტეტი (Root Certificate Authority) (ნახ.17).

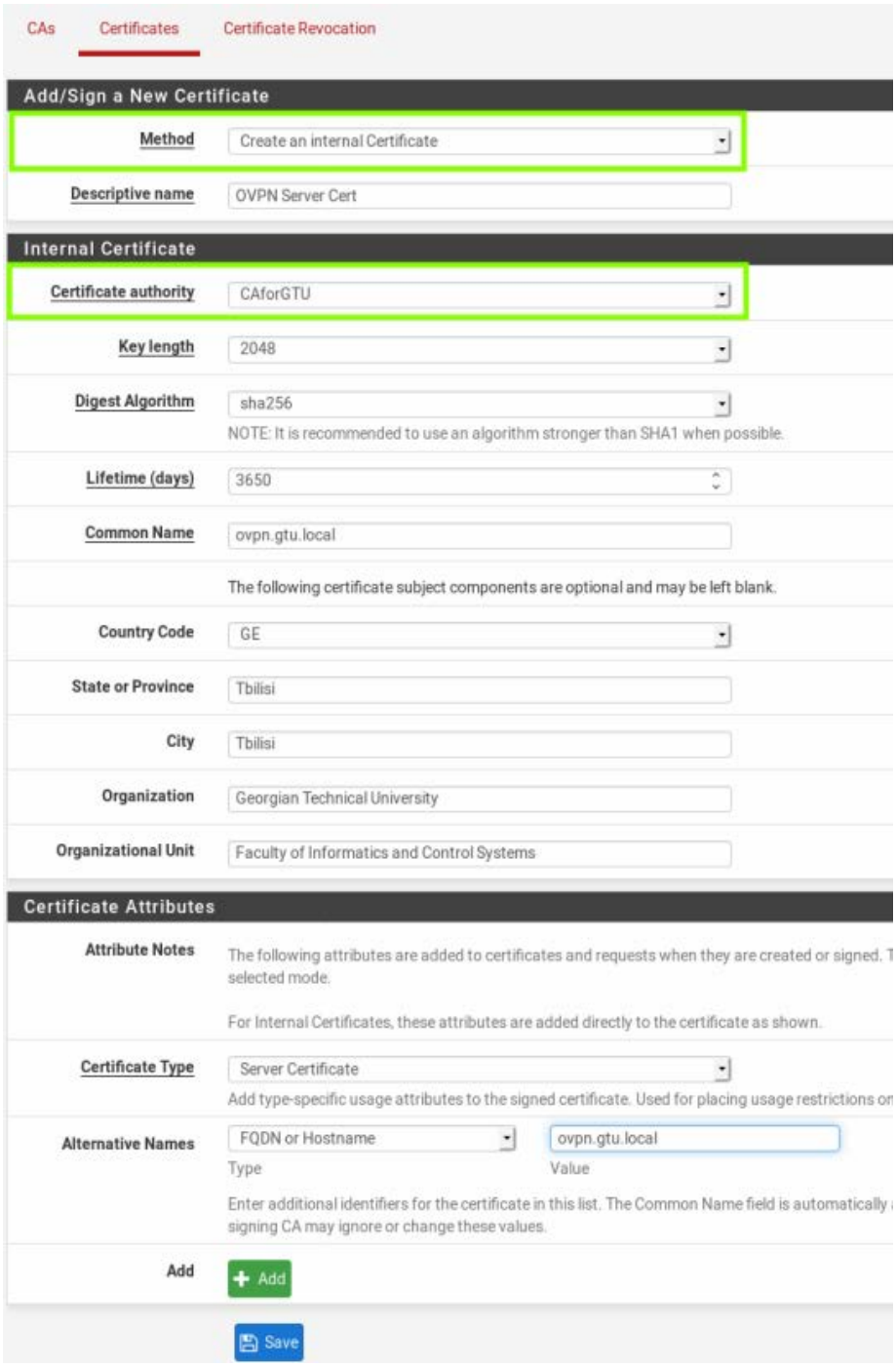


ნახ. 17. სერთიფიკატის ავტორიტეტი

2. სერთიფიკატის შექმნა OpenVPN სერვერისთვის.

სერთიფიკატის ავტორიტეტის ველში უნდა მივუთითოთ ის ROOT CA რომელიც შევქმენით წინა ნაბიჯში (ნახ.18).

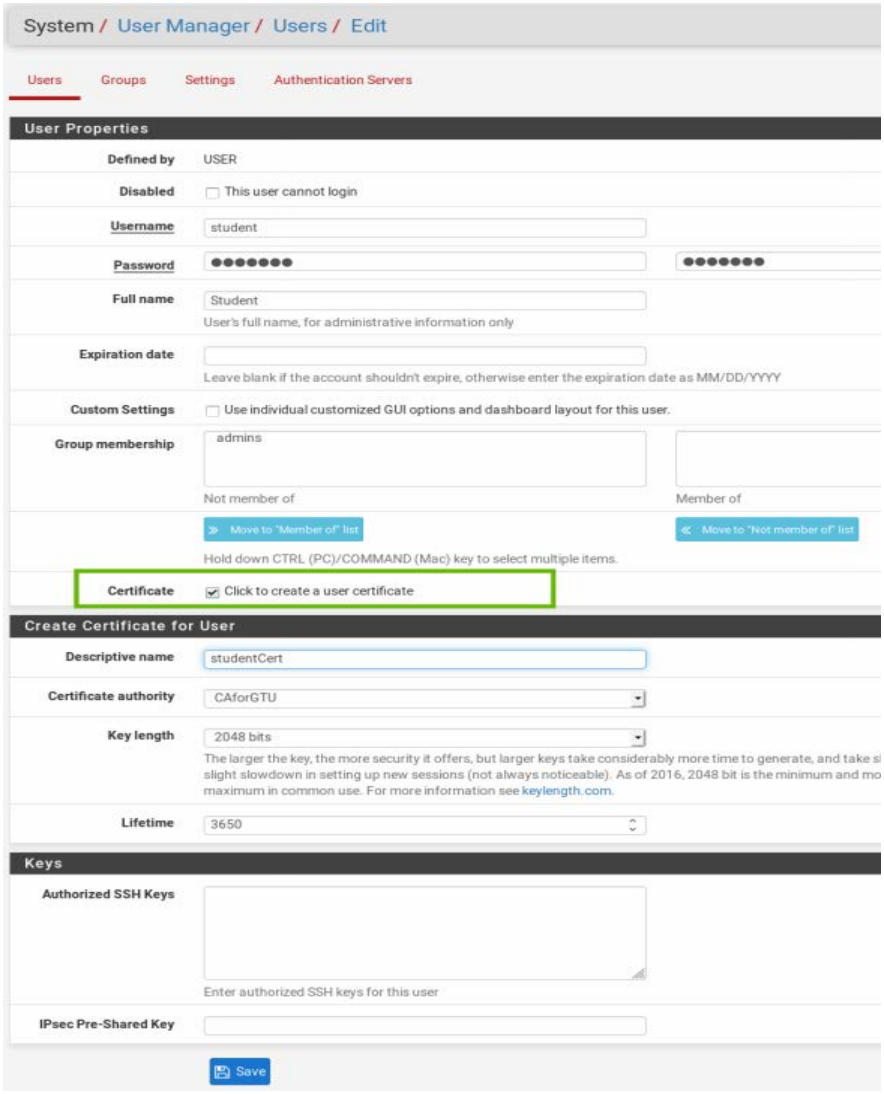
.



ნახ. 18. სერთიფიკატის შექმნა

3. მომხმარებლის შექმნა (რომლითაც კლიენტი გაივლის ავტორიზაციას)

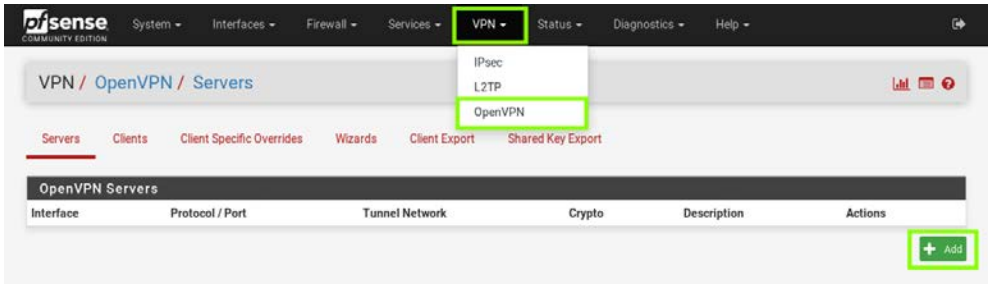
აუცილებელია მოვნიშნოთ სერთიფიკატის შექმნის ჩექბოქსი. ვინაიდან ვაპირებთ Certificate+user/pass ავტორიზაციის გამოყენებას (ნახ.19).



ნახ. 19. მომხმარებლის შექმნა

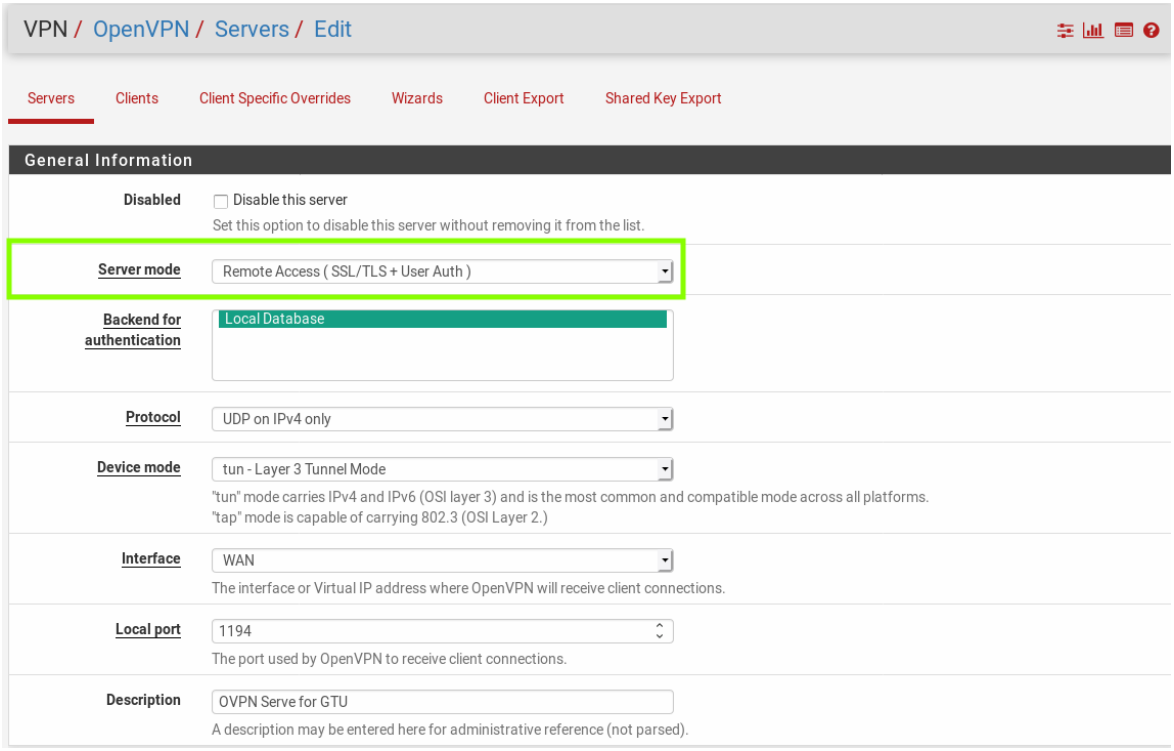
4. OpenVPN სერვერის შექმნა

პირველ რიგში დავამატოთ OVPN სერვერი (ნახ.20).



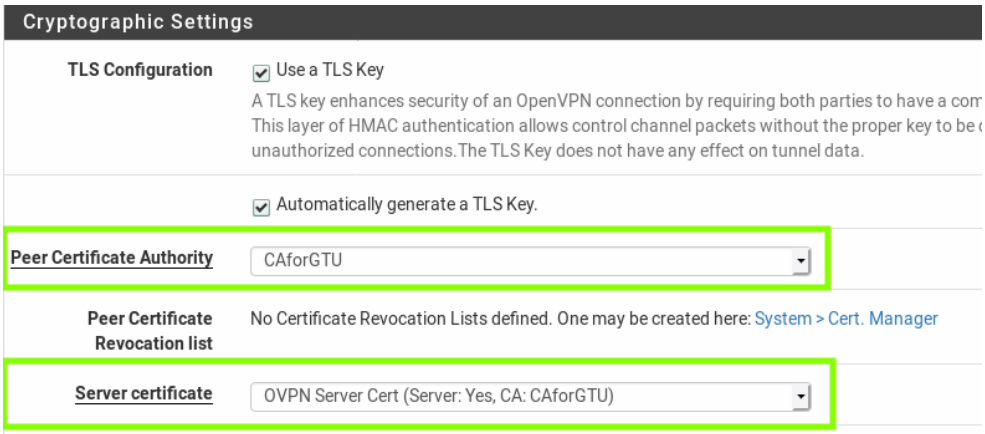
ნახ. 20. სერვერის შექმნა

სერვერის რეჟიმი ავირჩიოთ Remote Access (SSL/TLS + User Auth) (ნახ.21).



ნახ. 21. სერვერის რეჟიმის არჩევა

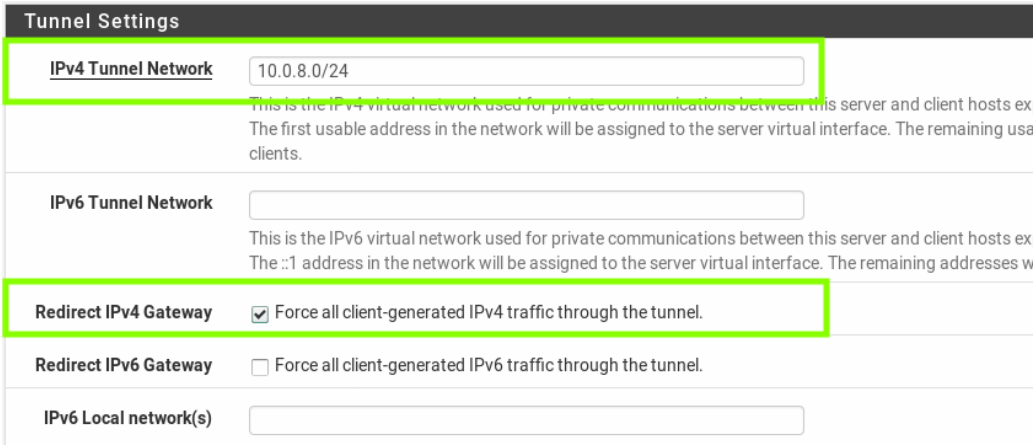
კრიპტოგრაფიულ მომართვებში მივუთითოთ ის სერთიფიკატის ავტორიტეტი, რომელიც შევქმენით პირველ ნაბიჯში. სერვერის სერთიფიკატის ველში მივუთითოთ მე-2 ნაბიჯში შექმნილი სერთიფიკატი (ნახ.22).



ნახ. 22. კრიპტოგრაფიული მომართვები

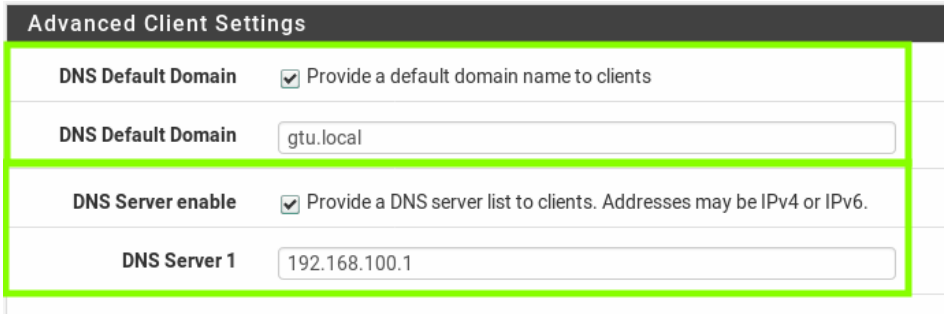
ტუნელის მომართვებში მივუთითოთ ჩვენთვის სასურველი ქსელი, რომლის დამისამართებაც გვინდა, რომ ჰქონდეთ სერვერს/კლიენტებს. ჩვენს შემთხვევაში ეს არის 10.0.8.0/24 ქსელი. მოვნიშნოთ, რომ გვსურს

გადავამისამართოთ IPv4 ტრაფიკი მთლიანად. ეს გამოიწვევს, რომ კლიენტის როუტინგ ცხრილში დაემატება როუტი, რომელიც გადაამისამართებს მთელს IPv4 ტრაფიკს OVPN გეითვეისკენ (ნახ.23).



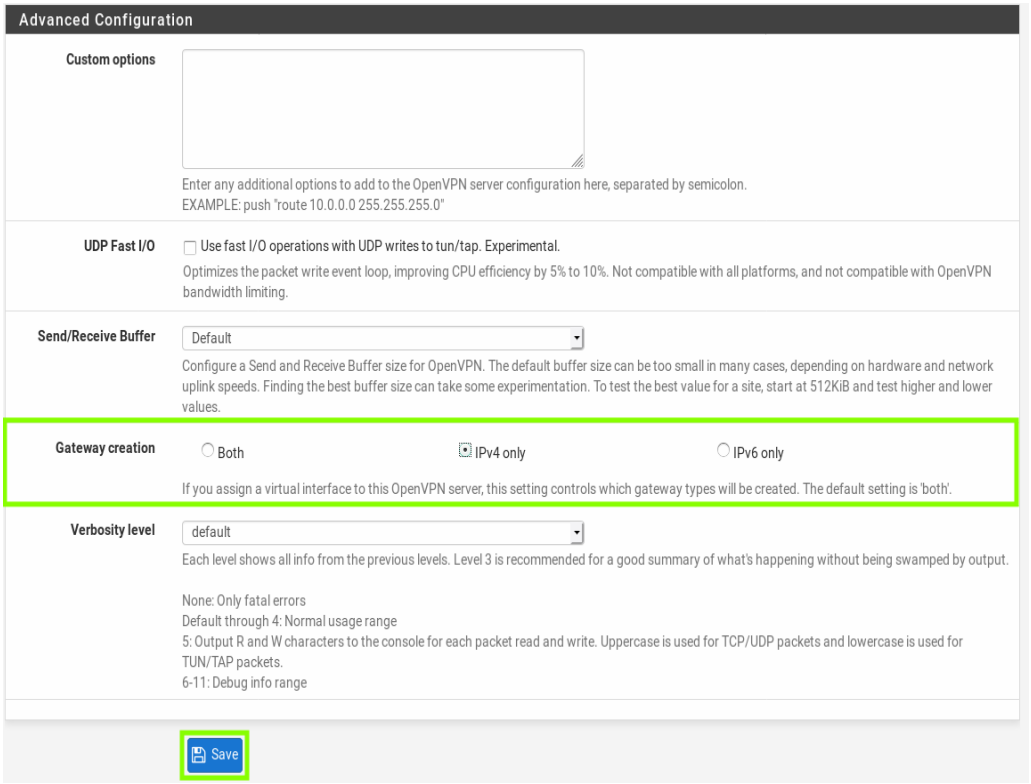
ნახ. 23. ტუნელის მომართვები

კლიენტის დამატებით მომართვებში შეგვიძლია მივუთითოთ დომეინი რომელსაც Ovpn სერვერი მიანიჭებს კლიენტს. ასევე მივუთითოთ შიდა DNS სერვერი, რომელსაც გამოიყენებს კლიენტი შიდა სერვისებისთვის დომეინური სახელების "გადასათარგმნად" (ნახ.24).



ნახ. 24. კლიენტის დამატებითი მომართვები

დამატებით კონფიგურაციაში გეითვეის შექმნისთვის მივუთითოთ IPv4 Only. ვინაიდან ჩვენ ვიყენებთ მხოლოდ IPv4 პროტოკოლს არ გვჭირდება IPv6 ინტერფეისის შექმნა (ნახ.25).

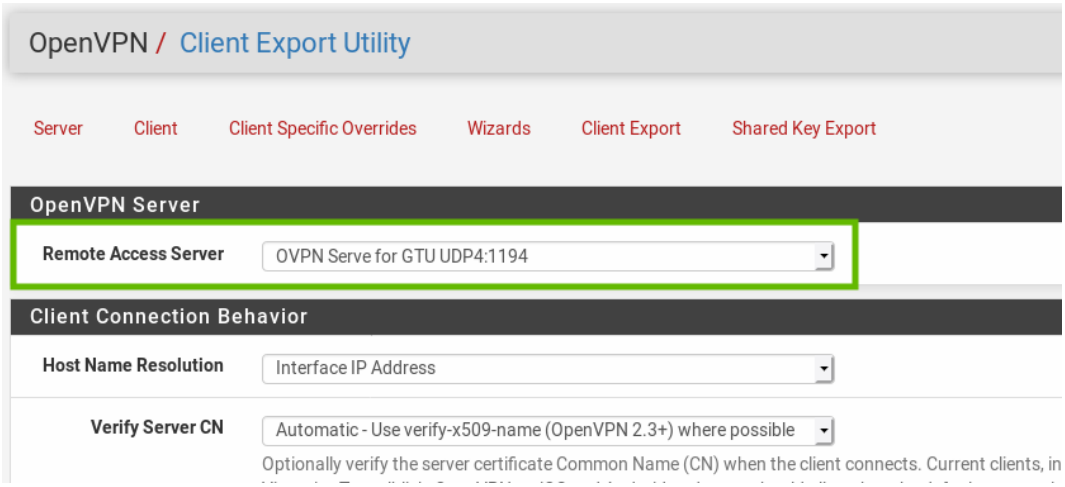


ნახ. 25. დამატებითი კონფიგურირება

5. OpenVPN აგენტის საინსტალაციო პაკეტის/კონფიგურაციის ექსპორტი.

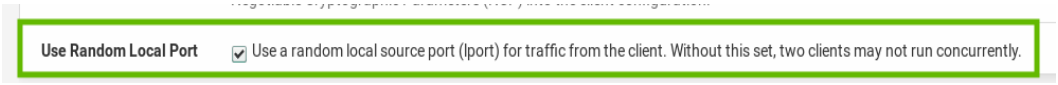
ეხლა უკვე შეგვიძლია დავაექსპორტოთ კლიენტის საინსტალაციო პაკეტი საკონფიგურაციო ფაილებთან ერთად.

პირველ რიგში ავირჩიოთ ჩვენს მიერ შექმნილი OVPN სერვერი (ნახ.26).



ნახ. 26. სერვერის არჩევა

ასევე აღვნიშნოთ ალამი (ჩექბოქსი) რომლის საშუალებითაც კლიენტს ექნება შესაძლებლობა გამოიყენოს ნებისმიერი ლოკალური პორტი. თუ არ ჩავრთავთ ამ ფუნქციას ორ კლიენტს შეიძლება ჰქონდეს ერთდროულად დაკავშირების პრობლემა VPN სერვერთან (ნახ.27).

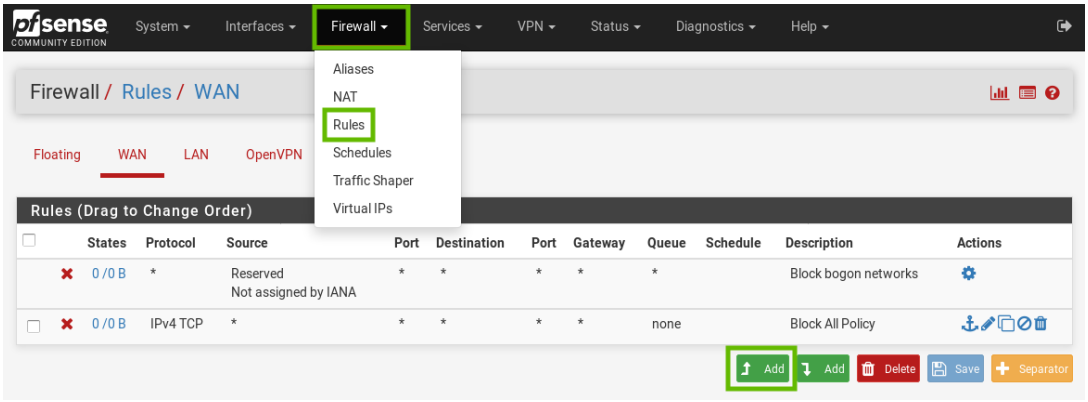


ნახ. 27. ალმის არჩევა

ამის შემდეგ შეგვიძლია ჩამოვტვირთოთ საინსტალაციო პაკეტი(მხოლოდ Windows-ისთვის), რომელიც ამავდროულად შეიცავს საკონფიგურაციო ფაილებს.

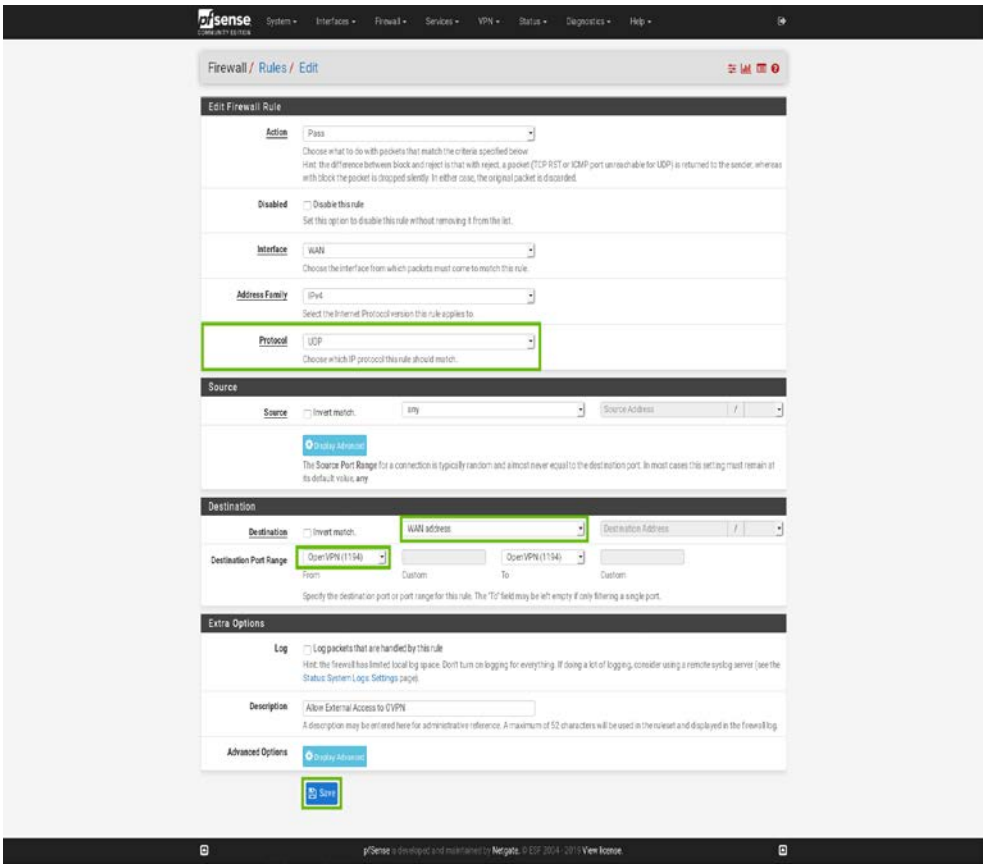
6. VPN სერვერის დაშვების წესის შექმნა ფაერვოლში.

იმისათვის, რომ pfSense-მა დაუშვას გარედან შემომავალი ტრაფიკი VPN-ისთვის საჭიროა შევქმნათ დაშვება firewall_ში. ამისთვის საჭიროა შევქმნათ წესი (ნახ.28).



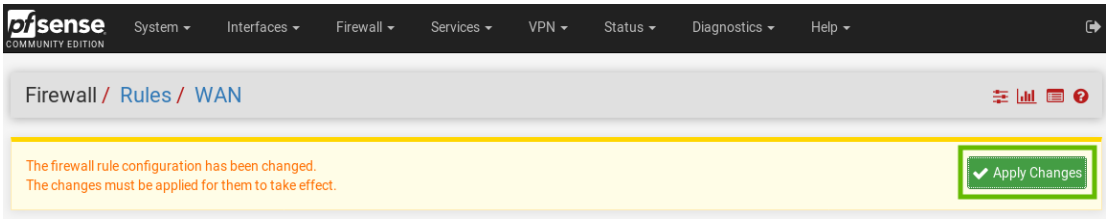
ნახ. 28. firewall დაშვების შექმნა

მივუთითოთ Action-ში მივუთითოთ დაშვება (pass). ავირჩიოთ UDP პროტოკოლი. ადრესატში (destination) მივუთითოთ WAN მისამართი. ადრესატის პორტში ავირჩიოთ OpenVPN 1194. ამის შემდეგ შევინახოთ შექმნილი წესი (ნახ.29).



ნახ. 29. დაშვების მითითება

იმისთვის, რომ წესი ამოქმედდეს საჭიროა მივიღოთ ცვლილებები (ნახ.30).

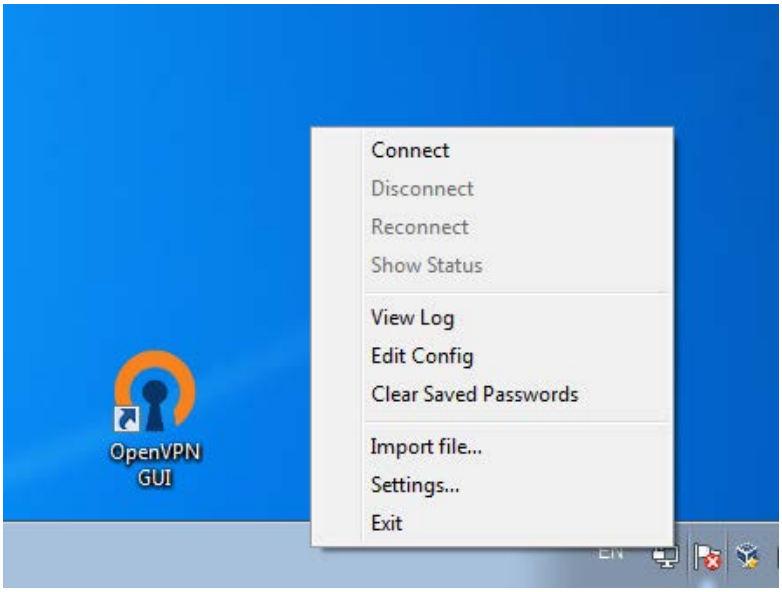


ნახ. 30. ცვლილებების მიღება

7. ტესტირება

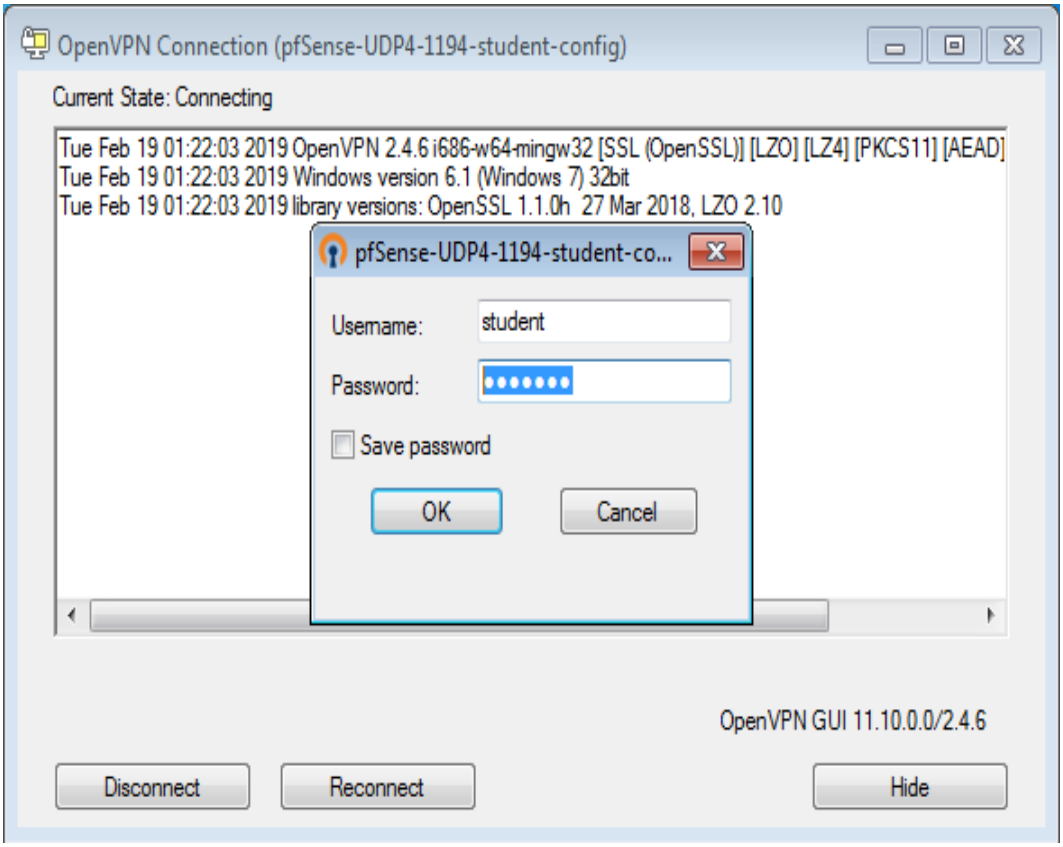
შეგვიძლია შევამოწმოთ ჩვენს მიერ შექმნილი VPN სერვერის მუშაობა. ამისთვის დაგვჭირდება კლიენტი მანქანა საიდანაც დავუკავშირდებით VPN-ს. ჩვენს შემთხვევაში გამოვიყენებთ Windows კლიენტს. კლიენტი შესაძლებელია იყოს სხვა ნებისმიერი სისტემა რომელზეც არსებობს OpenVPN კლიენტის საინსტალაციოპაკეტი. Linux, Mac OS, Android, iOS.

პაკეტის დაყენების შემდეგ, რომელიც შევქმენით მე-5 ნაბიჯში, გავუშვათ პროგრამა. ქვედა მარჯვენა კუთხეში გამოჩნდება VPN_ის სიმბოლო (ნახ.31).



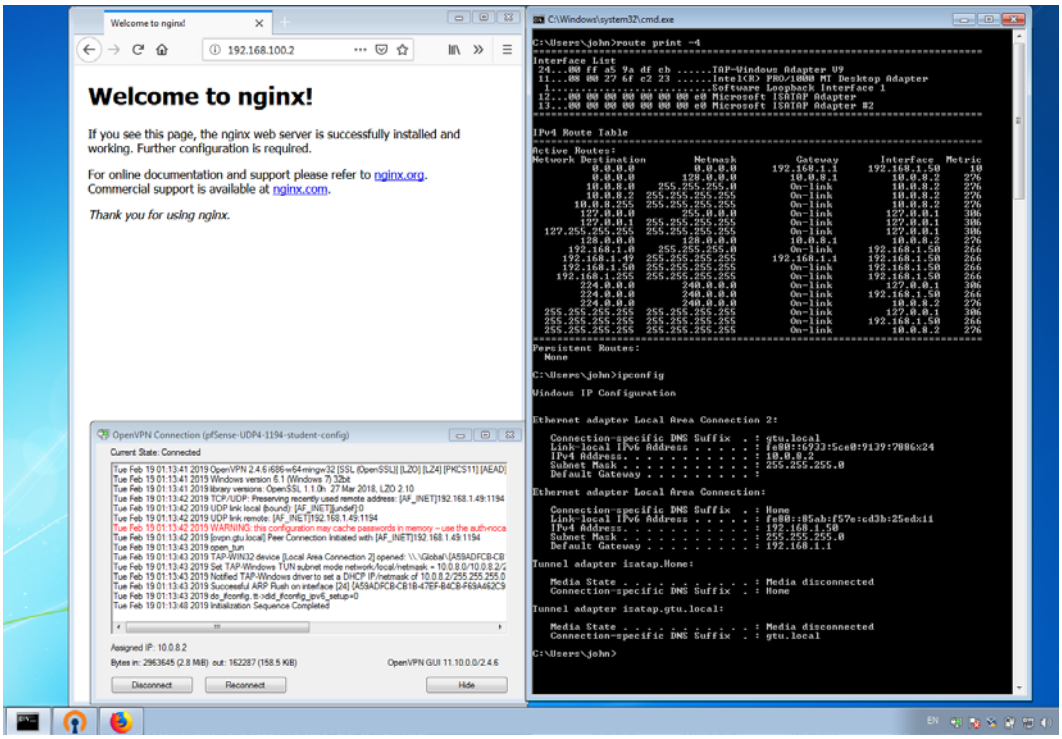
ნახ. 31. პროგრამის გაშვება

დავუკავშირდეთ სერვერს. პროგრამა მოგვთხოვს შევიყვანოთ მომხმარებელი და პაროლი. შევიყვანოთ მე-3 ნაბიჯში შექმნილი მომხმარებლის მონაცემები (ნახ.32).



ნახ. 32. მომხმარებლის აუტენტიფიკაცია

აგენტი წარმატებით დაუკავშირდა VPN სერვერს. მარჯვენა ქვედა კუთხეში არსებული OpenVPN_ის ხატულა გამწვანდა. რაც ნიშნავს რომ კავშირი დამყარებულია. გავხსნათ ცენტრალურ ოფისში არსებული ვებ სერვერი იმისათვის, რომ დავრწმუნდეთ ყველაფერის მუშაობაში. როგორც ქვემოთ მოცემულ ნახაზში ჩანს წარმატებით დავუკავშირდით ცენტრალურ ოფისში არსებულ ვებ სერვერს (ნახ.33).



ნახ. 33. დაკავშირების ფანჯარა

ტექნიკური რეალიზაციის საშუალებით განასხვავებენ შემდეგ VPN ჯგუფებს: VPN მარშრუტიზატორების ბაზაზე; VPN ქსელთაშორის ეკრანების ბაზაზე; VPN პროგრამული გადაწყვეტილებების ბაზაზე; VPN ჩაშენებული შიფრპროცესორებიანი სპეციალიზებული აპარატურული საშუალებების ბაზაზე.

VPN მარშრუტიზატორების ბაზაზე. VPN აგების მოცემული მეთოდი გვთავაზობს მარშრუტიზატორების გამოყენებას დაცული არხების შექმნისთვის. რამდენადაც, ლოკალური ქსელიდან გამოსული მთელი ინფორმაცია გადის მარშრუტიზატორებზე, სავსებით ბუნებრივია მასზე შიფრირების ამოცანის დაკისრება.

VPN ქსელთაშორის ეკრანების ბაზაზე. ქსელთაშორის ეკრანების მწარმოებელთა უმეტესობა მხარს უჭერს მონაცემთა დაგვირაბებასა და დაშიფვრას ქსელთაშორის ეკრანების ბაზაზე. ქსელთაშორის ეკრანების გამოყენებისას უნდა გვახსოვდეს, რომ მსგავსი გადაწყვეტილება მიესადაგება მხოლოდ მცირე არეალის ქსელებს, გადასაცემი ინფორმაციის შედარებით მცირე მოცულობით.

VPN პროგრამული გადაწყვეტილებების ბაზაზე. პროგრამული მეთოდებით რეალიზებული VPN-პროდუქტები, მწარმოებლურობის თვალსაზრისით, ჩამორჩება სპეციალიზებულ მოწყობილობებს, თუმცა, ფლობენ საკმარის სიმძლავრეს VPN-ქსელების რეალიზაციისთვის.

VPN სპეციალიზებული აპარატული საშუალებების ბაზაზე. მისი მთავარი უპირატესობაა მაღალი მწარმოებლურობა. სპეციალიზებული VPN-სისტემების შედარებით მაღალი სწრაფმოქმედება გამოწვეულია იმით, რომ მათში შიფრირება ხორციელდება სპეციალიზებული მიკროსქემებით. სპეციალიზებული VPN-მოწყობილობები უზრუნველყოფს უსაფრთხოების მაღალ დონეს, თუმცა, ისინი საკმაოდ ძვირადღირებულია.

2.2. ვირტუალურ კერძო ქსელებში (VPN) სიმბოლოების დაშიფვრის კომბინირებული მეთოდი

როგორც წინა პარაგრაფში აღვნიშნეთ, ორ მოცილებულ კომპიუტერს შორის, რომელიც ჩართულია გლობალურ ქსელში, ერთმანეთთან უსაფრტხოდ დასაკავშირებლად ვირტუალური კერძო ქსელები VPN (Virtual Private Network) დღეისათვის წარმოადგენს ყველაზე საუკეთესო ვარიანტს. დასმული ამოცანა ძალზე მნიშვნელოვანია, რადგან მყარი და უსაფრთხო კავშირი, სადაც ხდება სხვადასხვა სახის ინფორმაციის გადაცემა, აუცილებელია ყოველდღიური ცხოვრების ყველა სფეროში, როგორიცაა მაგალითად, საბანკო საქმე, სხვადასხვა საწარმოები და სხვა. ზემოთაღნიშნულიდან შეიძლება დავასკვნათ, რომ ვირტუალური კერძო ქსელები ყველაზე მოსახერხებელია ინფორმაციის გადასაცემად გლობალურ ქსელში ყველა კომპანია თუ ორგანიზაცია წარმმატებით მოიხმარს აღნიშნულ ტექნოლოგიას. თუმცა, საქმე მთლად ასე მარტივად არ წარმოგვიდგება. ვირტუალურ კერძო ქსელებს გააჩნიათ თავიანთი ნაკლოვანებები და სუსტი მხარეები.

ვირტუალური კერძო ქსელების ტექნოლოგია აგებულია კრიპტოგრაფიული მეთოდების გამოყენებაზე. კერძოდ, ყველა ინფორმაცია, რომელიც მიედინება დაცული კავშირის არხში, იმყოფება დაშიფრულ მდგომარეობაში. აქედან გამომდინარე, VPN-ის საფუძველს წარმოადგენს კრიპტოგრაფია და მის არეალში აგრეთვე მოქმედებს ზოგიერთი დამატებითი მექანიზმი, როგორებიცაა, მაგალითად, მომხმარებლების აუტენტიფიკაცია, მონაცემთა მთლიანობის კონტროლი და სხვა. თუმცა, კრიპტოგრაფიულ მეთოდებს გააჩნიათ თავიანთი სუსტი ადგილები.

ნებისმიერი კრიპტოგრაფიული მეთოდის გამოყენების საიმედოობა დაფუძნებულია მასში გამოყენებული დაშიფვრის ალგორითმზე. და, რა თქმა უნდა, მონაცემების სუსტი დაშიფვრა ბოროტგანმზრახველს საშუალებას აძლევს ადვილად მოიპოვოს წვდომა მისთვის სასურველ ინფორმაციაზე. ბუნებრივია, ჩნდება კითხვა, თუ რომელი კრიპტოგრაფიული მეთოდი უნდა იქნას გამოყენებული მონაცემების უსაფრთხოებისთვის (ნახ. 34).

ნახ. 34. მომხმარებელთა ავტორიზაციის ფორმა

დღეისათვის გამოიყენება ღია და დახურული კრიპტოგრაფიული ალგორითმები. ღია ალგორითმების ჯგუფს მიეკუთვნება ისეთი

ცნობილი ტექნოლოგიები, როგორებიცაა: DES (Data Encryption Standard), TripleDES (Triple Data Encryption Algorithm), RSA (Rivest, Shamir and Adleman), AES (Advanced Encryption Standard) და სხვა. ისინი გაერთიანებულნი არიან სხვადასხვა ქვეყნის ნაციონალურ სტანდარტებში. დახურული კრიპტოგრაფიული ალგორითმები მუშავდება სხვადასხვა კომპანიის მიერ და გამოიყენება თავიანთ საკუთრებაში.

ინფორმაციის დაშიფვრისთვის გამოიყენება კრიპტოგრაფიული გასაღები და დიდი მნიშვნელობა ენიჭება დაშიფვრის მექანიზმს და გასაღების სიგრძეს. ვინაიდან, რაც უფრო რთულია დაშიფვრის მექანიზმი და რაც უფრო დიდია გასაღების სიგრძე, მით უფრო გაუჭირდება ბოროტგანმზრახველს მისი ამოცნობა.

ყველა ზემოთ განხილული არსებული თუ აქამდე შემოთავაზებული კრიპტოგრაფიული ტექნოლოგია დაფუძნებულია მატრიცული მეთოდების გამოყენებაზე. რა თქმა უნდა, რაც უფრო გართულებულია მონაცემების დაშიფვრის მექანიზმი, მით უფრო გაუჭირდება ბოროტგანმზრახველს მისი გაშიფვრა. თუმცა, ამასთან ჩნდება ახალი პორბლემა, ეს არის მონაცემების გადაცემის სიჩქარე. დაშიფვრის მექანიზმის გართულებას მოსდევს მონაცემების გადაცემის სიჩქარის შემცირება, მით უმეტეს მაშინ, როდესაც მომხმარებელს უწევს მუშაობა განაწილებულ მონაცემთა ბაზების მართვის სისტემასთან. მონაცემთა ბაზაში ჩანაწერების რაოდენობის გაზრდა იწვევს მომხმარებლის მიერ მოცილებული სამუშაო ადგილიდან მონაცემთა წამოღების სიჩქარის ვარდნას. მონაცემთა ბაზების ოპტიმიზაციის პრობლემა დღეისათვის წარმოადგენს ერთ-ერთ საპრობლემო სფეროს და დღეისათვის აქტიურად მიმდინარეობს მუშაობა ამ პრობლემის აღმოსაფხვრელად. აქედან გამომდინარე, უნდა შემუშავდეს ისეთი დაშიფვრის მექანიზმი, რომელიც თავისი თვისებებით იქნება მარტივი, დიდ გამოთვლით პროცესებთან არ იქნება დაკავშირებული და, რაღა

თქმა უნდა, გარეშე უცხო პირისთვის მისი ამოცნობის ალბათობა იქნება ძალზე მცირე.

არსებულ დაშიფვრის მეთოდებს გააჩნიათ კიდევ ერთი პრობლემა. დაშიფვრის გასაღები უმეტესად არ არის ცვალებადი, ან თუ არის იშვიათად, რაც ბოროტგანმზრახველს ხელს უწყობს გარკვეული დროის განმავლობაში გაშიფროს იგი. ამიტომ, სასურველია სისტემაში შემოღებულ იქნას დამატებითი პარამეტრები (კოეფიციენტები), რომლებიც გასაღებს გახდის ცვალებადს. კერძოდ, სისტემაში მომხმარებლის ყოველი ავტორიზაციის დროს დაშიფრვისა და ამოშიფვრის გასაღები იქნება უნიკალური (ანუ არასდროს განმეორდება) და შეუძლებელი იქნება მისი გატეხვა.

ზემოთ აღნიშნული პრობლემებიდან გამომდინარე, შემუშავებულია სიმბოლოების დაშიფვრის კომბინირებული მეთოდი. სიმბოლოების დაშიფვრა და მისი ამოცნობა, თავისი თვისებებიდან გამომდინარე, შეიცავს განსაკუთრებულ პრობლემებს, რომელთა გადაწყვეტაც წარმოადგენს უსაფრთხოების ავტომატიზებული სისტემის აგების აუცილებელ პირობას. სიმბოლოების დაშიფვრის კომბინირებული მეთოდი მოიცავს შემდეგ ეტაპებს:

1) მომხმარებლის მიერ შეტანილი პაროლის დაშლა სიმბოლოებად;

2) თითოეული სიმბოლოს გადაყვანა ASCII(decimal) კოდირებაში და მათი კოდების განსაზღვრა;

3) მიღებული კოდებით სპეციალური ოპერაციის დახმარებით დამატებითი სიმბოლოების განსაზღვრა სისტემაში დაყენებული პარამეტრის მიხედვით;

4) სიმბოლოების და დამატებითი სიმბოლოების გაერთიანება და მათი სიტყვებად დაშლა (ჯგუფების შექმნა) სისტემაში დაყენებული პარამეტრის მიხედვით;

5) თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში ხდება მათი შესაბამისი კოდების განსაზღვრა;

6) სპეციალური ოპერაციის დახმარებით მიღებული კოდების რიცხობრივი მნიშვნელობა გარდაიქმნება სხვა რიცხობრივ მნიშვნელობად და მიიღება ახალი კოდების სიმრავლე;

7) მიღებული კოდების სიმრავლისაგან მიიღება სპეციალური სიმბოლოებისაგან შემდგარი ჯგუფები;

8) მიღებული ჯგუფების გაერთიანებით მიიღება სპეციალური სიმბოლოების ერთობლიობისგან შემდგარი დაშიფრული ინფორმაცია.

სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ეტაპები თავისი ფუნქციონალური დანიშნულებებით შეიძლება დახასიათდეს შემდეგნაირად:

პირველ ეტაპზე მომხმარებლის მიერ შეტანილი პაროლი იწერება სპეციალურ მასივში, სადაც განსაზღვრულია სიტყვის დასაწყისი და დასასრული. აგრეთვე, ხდება სიტყვის დაშლა სიმბოლოებად და ცალკეული სიმბოლოსთვის განსაზღვრულია მისი ინდექსი.

მე-2 ეტაპზე თითოეული სიმბოლო განიხილება ASCII(decimal) კოდირებაში და მათთთვის განისაზღვრება კოდები, რომლებიც იმახსოვრება სპეციალურ ცვლადებში;

მე-3 ეტაპზე ინფორმაციის უსაფრთხოება ბევრად არის დამოკიდებული მომხმარებლებზე. მაგალითად, მომხმარებელმა შეიძლება აირჩიოს ძალიან ადვილი პაროლი, რომელიც ამოსაცნობად მარტივი იქნება უცხო პირისთვის. აქედან გამომდინარე, აუცილებელია ავტომატიზებულად მოხდეს მისი „გართულება“. მეორე ეტაპზე მიღებული კოდებით სპეციალური ოპერაციის დახმარებით სისტემაში დაყენებული პარამეტრის მიხედვით განისაზღვრება მოდიფიცირებული კოდები, რომლებისგანაც მიიღება დამატებითი სიმბოლოები.

მე-4 ეტაპზე მიღებული სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით იქმნება „გართულებული“ პაროლი, რომელსაც ემატება მიმდინარე თარიღისა და დროის რიცხობრივი მნიშვნელობები. შემდეგ ხდება მისი სიტყვებად დაშლა (ჯგუფების

შექმნა) სისტემაში დაყენებული პარამეტრის მიხედვით. სასურველია, რომ მომხმარებლის ავტორიზაციის პროცესში ცენტრალური სერვერისთვის პაროლის გადაცემა მოხდეს ნაწილ-ნაწილ (ცალკეულ ჯგუფებად) შუალედური დასტურების ვითარებაში.

მე-5 და მე-6 ეტაპებზე თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში ხდება მათი შესაბამისი კოდების განსაზღვრა. შემდეგ სპეციალური ოპერაციის დახმარებით მიღებული კოდების რიცხობრივი მნიშვნელობა გარდაიქმნება სხვა რიცხობრივ მნიშვნელობად და მიიღება ახალი კოდების სიმრავლე;

მე-7 და მე-8 ეტაპებზე მიღებული კოდების სიმრავლისაგან იქმნება სპეციალური სიმბოლოებისაგან შემდგარი ჯგუფები და ამ ჯგუფების გაერთიანებით გვაქვს სპეციალური სიმბოლოების ერთობლიობისგან შემდგარი დაშიფრული ინფორმაცია, რომელსაც ამოშიფრავს ცენტრალური სერვერი უკუალგორითმის საშუალებით.

განვიხილოთ სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ფორმალური ნაწილი. ამისათვის შემოვიტანოთ აღნიშვნები.

$i-$ სიმბოლოს ინდექსი; $j-$ დამატებითი სიმბოლოს ინდექსი; n_1- სიმბოლოების რაოდენობა მომხმარებლის მიერ შეტანილ სიტყვაში (პაროლში), n_2- სიმბოლოების რაოდენობა დამატებით სიტყვაში.

დასაწყისისთვის:

$$i=1; \qquad j=1; \qquad n_1=0; \qquad n_2=0 \qquad (1)$$

ვადგენთ მასივს:

$$S_{\{i\}}F, L \qquad i=\overline{1,n_1} \qquad (2)$$

სადაც $S_{\{i\}}F$ არის სიმბოლოების სიტყვის დასაწყისი, $S_{\{i\}}L$ არის სიმბოლოების სიტყვის დასასრული, n_1 არის სიმბოლოების რაოდენობა სიტყვაში.

შემდეგ სიტყვაში სიმბოლოები იშლება და ცალკეული სიმბოლოსთვის ინდექსი განისაზღვრება:

$$
\begin{aligned}
&i = 1 \\
&S_{\{i\}} = S_{\{i\}}F \\
&S_{\{i\}}F = S_{\{i\}}F + 1 \\
&i = i + 1; \qquad n_1 = n_1 + 1
\end{aligned}
\tag{3}
$$

ვიდრე $i \le S_{\{i\}}L$

რის შედეგაც მიიღება სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, მასში ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$S_{\{i\}}F, L = (S_{\{1\}}, S_{\{2\}}, ..., S_{\{n_1\}}) \tag{4}$$

თითოეული სიმბოლო განიხილება ASCII(decimal) კოდირებაში და მათთთვის განისაზღვრება კოდები. ამისათვის შემოვიღოთ მასივი:

$$S_{ASCII\{i\}}F, L \qquad i = \overline{1, n_1} \tag{5}$$

სადაც $S_{ASCII\{i\}}F$ არის სიმბოლოების კოდების დასაწყისი, $S_{ASCII\{i\}}L$ არის სიმბოლოების კოდების დასასრული, n_1 არის სიმბოლოების კოდების რაოდენობა.

მომდევნო ეტაპზე ცალკეული სიმბოლოსთვის კოდი განისაზღვრება და ჩაიწერება სიმბოლოების კოდების მასივში:

$$
\begin{aligned}
&i = 1 \\
&S_{ASCII\{i\}} = S_{\{i\}}F, L \\
&i = i + 1;
\end{aligned}
\tag{6}
$$

ვიდრე $i \le n_1$

რის შედეგაც მიიღება სიმბოლოების კოდების ერთობლიობისაგან შემდგარი რიცხვები, რომლებშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსის კოდი:

$$S_{ASCII\{i\}}F, L = (S_{ASCII\{1\}}, S_{ASCII\{2\}}, ..., S_{ASCII\{n_1\}}) \tag{7}$$

შემდეგ უნდა შევავსოთ სიტყვა დამატებითი სიმბოლოებით. ამისათვის შემოვიტანოთ აღნიშვნა - P_1, რომელიც წარმოადგენს სიტყვის შევსების პარამეტრს ანუ რა რაოდენობისაგან უნდა შედგებოდეს სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით შედგენილი სიტყვა.

თავდაპირველად უნდა განისაზღვროს დამატებითი სიმბოლოების რაოდენობა – n_2.

$$n_2 = p_1 - n_1 \qquad (8)$$

ვადგენთ მასივს, სადაც უნდა ჩაიწეროს დამატებითი სიმბოლოები:

$$D_{\{j\}}F, L \qquad j = \overline{1, n_2} \qquad (9)$$

სადაც $D_{\{j\}}F$ არის დამატებითი სიმბოლოების სიტყვის დასაწყისი, $D_{\{j\}}L$ არის დამატებითი სიმბოლოების სიტყვის დასასრული, n_2 არის დამატებითი სიმბოლოების რაოდენობა სიტყვაში.

შემდგომ ცალკეული სიმბოლოს განსაზღვრული კოდისთვის განისაზღვრება მოდიფიცირებული კოდები. ამისათვის შემოვიღოთ აღნიშვნა – b_k, რომელიც არის დამატებითი სიმბოლოების შევსებისთვის საჭირო ძირითად სიმბოლოებში გასავლელი ბიჯების რაოდენობა. $k = \overline{1, m}$, სადაც m - არის ბიჯების რაოდენობა

ამისათვის შემოვიღოთ მასივი, სადაც ჩაიწერება მოდიფიცირებული კოდები:

$$D_{ASCII\{j\}}F, L \qquad j = \overline{1, n_2} \qquad (10)$$

სადაც $D_{ASCII\{j\}}F$ არის დამატებითი სიმბოლოების კოდების დასაწყისი, $D_{ASCII\{j\}}L$ არის დამატებითი სიმბოლოების კოდების დასასრული, n_2 არის დამატებითი სიმბოლოების კოდების რაოდენობა.

მოცემული მეთოდის მიზანი მოდიფიცირებული კოდებით დასაშიფრი სიმბოლოების გადაყვანა სპეციალურ სიმბოლოებში. ASCII(decimal) კოდირების სისტემაში სიმბოლოების კოდები შეესაბამება

32-დან 126-ის ჩათვლით, ხოლო სპეციალური სიმბოლოების კოდები შეესაბამება 128-დან 255-ის ჩათვლით.

სიმბოლოების კოდების გარდაქმნა ხდება შემდეგნაირად. აიღება სიტყვის პირველი სიმბოლოს კოდი $S_{ASCII\{1\}}$, გადამოწმდება მისი მდებარეობის არეალი. თუ კოდი მდებარეობს 32-დან 50-ის ჩათვლით, მაშინ შესრულდება შემდეგი მოქმედება: სიმბოლოს კოდს დაემატება მისი რიგითობა ანუ ინდექსი, შემდეგ მეორე სიმბოლოს კოდს დაემატება მეორე ინდექსი და ა.შ. სიტყვის ბოლომდე. თუ კოდი მდებარეობს 51-დან 126-ის ჩათვლით, მაშინ აკლდება. მიღებული ახალი კოდებით დგება დამატებითი სიმბოლოების ჯგუფი. ეს პროცესი მიმდინარეობს იქამდე, ვიდრე არ დაკმაყოფილდება p_1 პარამეტრის მნიშვნელობა. თუ b_k-სთვის $k=1$, ანუ პირველი ბიჯია, მაშინ სიმბოლოების რიგითობა იწყებს 1-დან, თუ $k=2$ - მე-2 ბიჯი, 2-დან და ა.შ.

$$
\begin{aligned}
&b_k = 1 \\
&\text{თუ } 32 \le S_{ASCII\{i\}}F,L \le 50, \text{ მაშინ} \\
&D_{ASCII\{j\}}F,L = S_{ASCII\{i\}}F,L + S_{ASCII\{i\}} \\
&\text{თუ } 51 \le S_{ASCII\{i\}}F,L \le 126, \text{ მაშინ} \\
&D_{ASCII\{j\}}F,L = S_{ASCII\{i\}}F,L - S_{ASCII\{i\}} \\
&k = k+1;\ \ i = i+1;\ \ j = j+1
\end{aligned}
\qquad (11)
$$

მიღებული ახალი მოდიფიცირებული კოდებით დგება დამატებითი სიმბოლოების ჯგუფი:

$$
\begin{aligned}
&j = 1 \\
&D_{\{j\}} = D_{ASCII\{j\}}F,L \\
&j = j+1 \\
&\text{ვიდრე } \ j \le n_2
\end{aligned}
\qquad (12)
$$

რის შედეგაც მიიღება დამატებითი სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$D_{\{j\}}F, L = (D_{\{1\}}, D_{\{2\}}, ..., D_{\{n_2\}}) \qquad (13)$$

მიღებული სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით იქმნება „გართულებული“ სიტყვა (პაროლი), რომელსაც ემატება მიმდინარე თარიღისა და დროის რიცხობრივი მნიშვნელობები. შემოვიტანოთ აღნიშვნები – *DateTime*, რომელშიც ფიქსირდება მიმდინარე თარიღისა და დროის რიცხობრივი მონაცემი - *DateTime=now()*; $SD_{\{i\cup j\}}F, L$, რაშიც იწერება გაერთიანებული სიტყვა:

$$SD_{\{i\cup j\}}F, L = S_{\{i\}}F, L + D_{\{j\}}F, L + DateTime \qquad (14)$$

სადაც $i = \overline{1, n_1}$; $j = \overline{1, n_2}$

შედეგად მიიღება სიმბოლოებისაგან და დამატებითი სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$SD_{\{i\cup j\}}F, L = (S_{\{1\}}, S_{\{2\}}, ..., S_{\{n_1\}}, ..., D_{\{1\}}, D_{\{2\}}, ..., D_{\{n_2\}}) \qquad (15)$$

შემდეგ ხდება მიღებული სიტყვის დაშლა (ჯგუფების შექმნა) სისტემაში დაყენებული პარამეტრის მიხედვით. ამისათვის შემოვიტანოთ აღნიშვნები – p_2, რომელიც წარმოადგენს დასაშლელი სიტყვის რაოდენობას, ანუ რა რაოდენობით უნდა დაიშალოს მიღებული სიტყვა; $G_{\{\ell\}}SD_{\{i\cup j\}}F, L$, სადაც ფიქსირდება ჯგუფში შემავალი სიმბოლოები და ჯგუფის ინდექსი; m – ჯგუფების რაოდენობა.

დაშლილი სიტყვების რაოდენობა აღვნიშნოთ -ით და იგი გამოითვლება შემდეგნაირად:

$$\ell = (n_1 + n_2 + DateTime_{Count})divp_2; \qquad (16)$$

$$\ell = \overline{1,m}$$

სადაც *div* – ნიშნავს გაყოფას ნაშთის გარეშე. $DateTime_{Count}$ – თარიღისა და დროის რიცხობრივ მაჩვენებლებში სიმბოლოების რაოდენობა. შედეგად მივიღებთ ჯგუფების ერთობლიობას:

$$G_{\{\ell\}}SD_{\{i\cup j\}}F,L = (G_{\{1\}}SD_{\{i\cup j\}}, G_{\{2\}}SD_{\{i\cup j\}},..., G_{\{m\}}SD_{\{i\cup j\}}) \quad (17)$$

შემდეგ თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში ხდება მათი შესაბამისი კოდების განსაზღვრა.

$$G_{ASCII\{\ell\}}SD_{\{i\cup j\}} = G_{\{\ell\}}SD_{\{i\cup j\}}F,L$$
$$\ell = \ell + 1 \quad (18)$$
ვიდრე $\ell \le m$

რის შედეგაც მიიღება ჯგუფის სიმბოლოების კოდების ერთობლიობისაგან შემდგარი რიცხვები, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსის კოდი:

$$G_{ASCII\{\ell\}}SD_{\{i\cup j\}}F,L = (G_{ASCII\{1\}}SD_{\{i\cup j\}}, G_{ASCII\{2\}}SD_{\{i\cup j\}},..., G_{ASCII\{m\}}SD_{\{i\cup j\}}) \quad (19)$$

მიღებული კოდების რიცხობრივი მნიშვნელობა გარდაიქმნება სხვა რიცხობრივ მნიშვნელობად და მიიღება ახალი კოდების სიმრავლე. მიღებული სიმბოლოების კოდების გარდაქმნა ხდება შემდეგნაირად. აიღება სიტყვის პირველი სიმბოლოს კოდი $G_{ASCII\{\ell\}}$, გადამოწმდება მისი მდებარეობის არეალი. თუ კოდი მდებარეობს 32-დან 99-ის ჩათვლით, მაშინ შესრულდება შემდეგი მოქმედება: სიმბოლოს კოდს დაემატება პარამეტრის მნიშვნელობა, რომლიც აღვნიშნოთ - p_3. სადაც $96 \le p_3 \le 156$. ხოლო, თუ კოდი მდებარეობს 100-დან 126-ის ჩათვლით, მაშინ სიმბოლოს კოდს დაემატება პარამეტრის მნიშვნელობა, რომლიც აღვნიშნოთ – P_4. სადაც $28 \le p_4 \le 129$.

თუ $32 \le G_{ASCII\{\ell\}}F,L \le 99$, მაშინ

$$P_{ASCII\{g\}}F,L = G_{ASCII\{\ell\}}F,L + p_3$$

თუ $100 \le G_{ASCII\{\ell\}}F,L \le 126$, მაშინ (20)

$$P_{ASCII\{g\}}F,L = G_{ASCII\{\ell\}}F,L + p_4$$

$$g = g + 1;\ \ \ell = \ell + 1;\ \ g = \overline{1,t}$$

სადაც $P_{ASCII\{g\}}F,L$ არის სპეციალური სიმბოლოების მოდიფიცირებული კოდებისაგან შემდგარი ერთობლიობის მასივი, რომელიც ფიქსირდება ჯგუფების მიხედვით.

მიღებული ახალი მოდიფიცირებული კოდებით დგება სპეციალური სიმბოლოების ჯგუფი:

$$\begin{aligned} &g = 1 \\ &P_{\{g\}} = P_{ASCII\{\ell\}}F,L \\ &g = g + 1 \end{aligned} \qquad (21)$$

ვიდრე $g \le t$

შედეგად მივიღებთ სპეციალური სიმბოლოების ჯგუფების ერთობლიობას:

$$G_{\{\ell\}}P_{\{g\}}F,L = (G_{\{1\}}P_{\{g\}}, G_{\{2\}}P_{\{g\}}, ..., G_{\{m\}}P_{\{g\}}) \qquad (22)$$

სპეციალური სიმბოლოებისაგან შემდგარი ჯგუფების გაერთიანებით მიიღება სპეციალური სიმბოლოების ერთობლიობისგან შემდგარი დაშიფრული ინფორმაცია:

$$W_{\{\ell\}}F,L = G_{\{\ell\}}P_{\{g\}} \qquad (23)$$

$$\ell = \overline{1,m};\ \ g = \overline{1,t}$$

დაშიფრული ინფორმაცია ცენტრალურ სერვერს მიეწოდება ჯგუფების სახით. თუ პირველი ჯგუფის იდენტიფიკაცია წარმატებით დასრულდა, სერვერი ატყობინებს და ბრძანებას გამოსცემს მეორე ჯგუფის გამოშვებაზე და ა.შ. ჯგუფის ბოლომდე. თუ რომელიმე ჯგუფი არ დაემთხვა, სერვერი მაშინვე ბლოკავს აღნიშნულ მომხმარებელს. დაშიფრული ინფორმაციის ამოშიფვრა ცენტრალური სერვერის მიერ ხდება ზემოთგანხილული მეთოდის უკუალგორითმის საშუალებით იმავე პარამეტრების გამოყენებით.

დაშიფვრისა და ამოშიფვრის გასაღები სისტემაში გამოყენებული სპეციალური პარამეტრების წყალობით არის უნიკალური ანუ მომხმარებლის ყოველი ავტორიზაციის დროს გასაღებები იცვლება და არასდროს არ განმეორდება.

2.3. კორპორაციული ქსელები, მათი კომპონენტების და სისტემების მიმოხილვა, ქსელში არსებული მოწყვლადობების აღმოჩენა, კლასიფიცირება, პრიორიტიზირება და აღმოფხვრა

მოწყვლადობების მართვა არის პროცესი, რომლის საშუალებითად ხდება ქსელში არსებული მოწყვლადობების აღმოჩენა, კლასიფიცირება, პრიორიტიზირება და აღმოფხვრა. ეს პროცესი არის ინფორმაციული უსაფრთხოების ერთ-ერთი შემადგენელი კომპონენტი. საკუთრივ მოწყვლადობების მართვის პროცესი შედგება სხვადასხვა კომპონენტებისაგან.

მოწყვლადობების ძირითადი გამომწვევი მიზეზი არის პროგრამული უზრუნველყოფის მომართვისას დაშვებული შეცდომები და მათი განუახლებელი ვერსიები.

მოწყვლადობები პროგრამული უზრუნველყოფის "სიცოცხლის ციკლის" განუყოფელი ნაწილია. არ არსებობს 100%-ით დაცული პროგრამული უზრუნველყოფა. ადრე თუ გვიან აუცილებლად აღმოჩნდება მოწყვლადობა მასში და ეს ნორმალურია.

არსებობს სხვადასხვა პროექტი სადაც უსაფრთხოების ანალიტიკოსები/ინჟინრები ცდილობენ იპოვონ სისუტეები სხვადასხვა ინფორმაციულ სისტემებში, შესაბამისი ანაზღაურების სანაცვლოდ. სისუსტის აღმოჩენის შემდეგ ინფორმაცია გადაეცემა მწარმოებელს, რომლის სისტემაშიც აღმოჩენილია ეს სისუსტე. ამის შემდეგ მწარმოებელი როგორც წესი უშვებს უსაფრთხოების განახლებას, რომლითაც აღმოფხვრის სისუსტეს. არსებობს ბევრი პლათფორმა, რომელიც გამოიყენება ამ

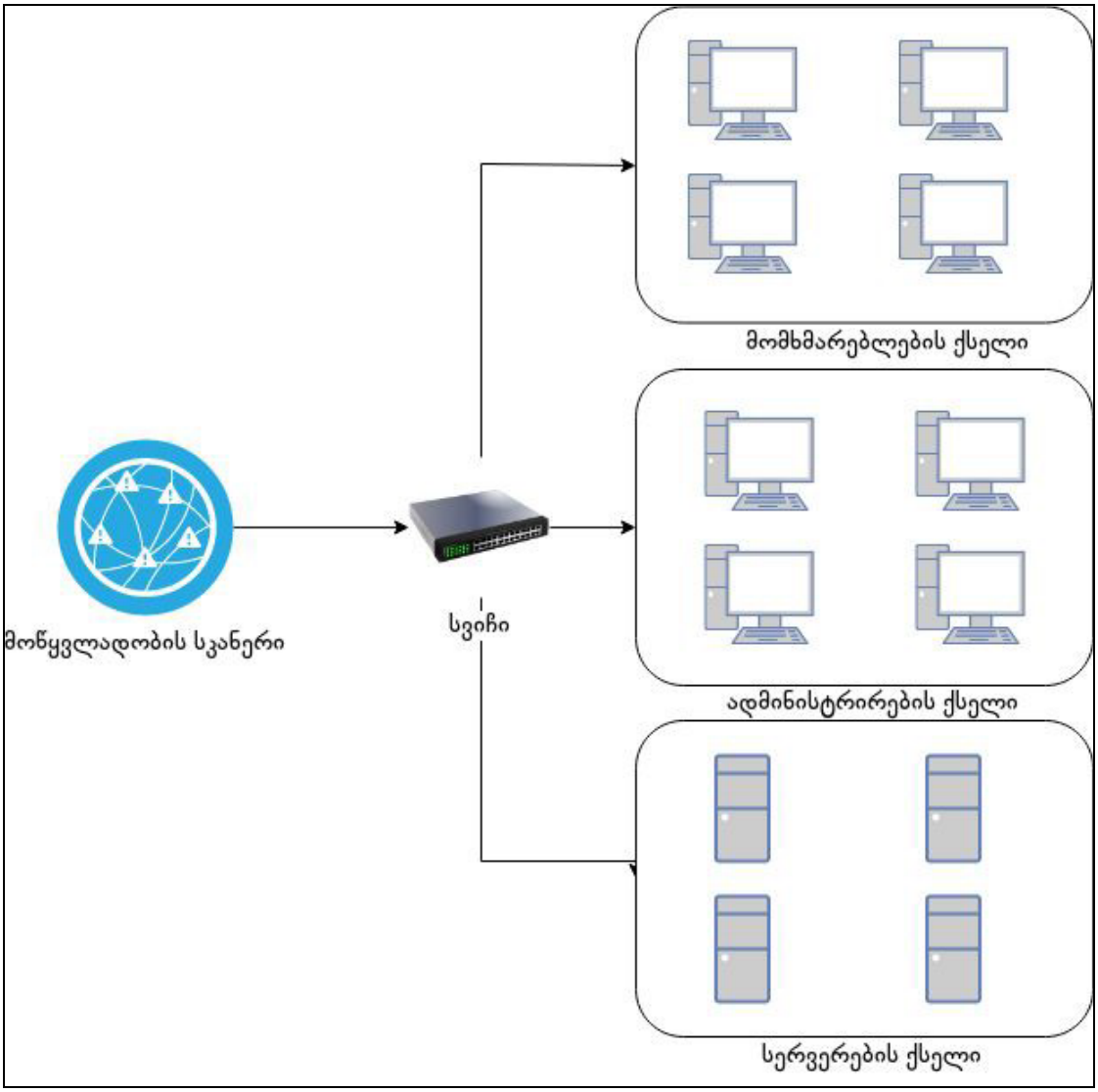
საქმიანობისთვის. მაგალითად, Zerodium, Hakerone, ZDI, Safehats, Bugcrowd და სხვა. ასეთ პლათფორმებზე მუშაობენ ეგრედ წოდებული თეთრი ქუდის(whitehat), ან ნაცრისფერი ქუდის(grayhat) ჰაკერები. თუმცა ჩამოთვლილი პლათფორმების გარდა არსებობს შავი ბაზარი. სადაც შესაძლებელია ეგრედ წოდებული 0 დღის(Zero Day) სისუსტეზე ინფორმაციის და ამ სისუსტის გამოყენებაზე მიმართული პროგრამული კოდის(exploit) ყიდვა. ამ დროს სისუტეზე ინფორმაცია არ მიეწოდება მწარმოებელს. ასეთ სისუსტეებს იყენებენ ჰაკერული დაჯგუფებები მიზანმიმართული შეტევებისთვის.

აღმოჩენილი სისუსტეები არის მიზეზი იმისა, რომ გამოდის ეგრედ წოდებული უსაფრთხოების პაჩები. პროგრამული განახლების ეს ტიპი (უსაფრთხოების განახლება) არ აფართოებს პროგრამული უზრუნველყოფის შესაძლებლობებს. ის მხოლოდ აღმოფხვრის არსებულ სისუსტეს პროგრამულ უზრუნველყოფაში.

მართალია აუცილებელია ყოველთვის განახლებული გვქონდეს პროგრამული უზრუნველყოფა თუმცა, მხოლოდ პროგრამული უზრუნველყოფის განახლება ვერ დაგვიცავს სისუსტეებისგან. თუკი სისტემა დაკონფიგურირებულია არასწორად, იმგვარად, რომ კონფიგურაცია იწვევს სისუსტეს, მხოლოდ პროგრამული განახლება ვერ აღმოფხვრის მას. ამისათვის საჭიროა მივყვეთ საუკეთესო პრაქტიკებს. ვაკეთოთ სისტემების ეგრედ წოდებული გამარგრება (hardening). რისი საშუალებითაც შევამცირებთ სავარაუდო სისუსტეების რაოდენობას სისტემებზე.

მოწყვლადობების აღმოჩენისთვის გამოიყენება მოწყვლადობის სკანერები. მათი საშუალებით შესაძლებელია სკანირების ჩატარება ქსელზე და მოწყვლადობების გამოვლენა. მოწყვლადობების აღმოჩენა შესაძლებელია როგორც ქსელის სკანირებით, ასევე აგენტის გამოყენებით. ქსელის სკანირების დროს ქსელში არსებობს გამოყოფილი კომპონენტი (სკანერი) რომელსაც აქვს წვდომა დასასკანირებელ სისტემებთან. ქვემოთ

მოცემულია მოწყვლადობის სკანერის განთავსების ლოგიკური ტოპოლოგია ქსელში (ნახ. 35).



ნახ. 35. მოწყვლადობის სკანერის განთავსება ქსელში

არსებობობს სხვადასხვა ტიპის სკანერები. ზოგიერთი მათგანი ახორციელებს ზოგად სკანირებას, აღმოაჩენს ღია პორტებს. სერვისებს, რომლებიც პასუხისმგებლები არიან ამ პორტებზე. მათ ვერსიებს და ასე შემდეგ. ზოგიერთი მათგანს აქვს ფუნქციონალი, აღმოაჩინოს სისუსტეები კონკრეტული მიმართულებით, მაგალითად: სისუსტეები ვებ სერვისების მიმართულებით, სისუსტეები კონკრეტული კონტენტის მართვის სისტემის მიმართულებით, სისუსტეები კონკრეტულ მოწყვლადობაზე და ასე შემდეგ.

Nmap(Network Mapper) არის ღია კოდის მქონდე უფასო ქსელური სკანერი. ის შექმნა გორდონ ლიონმა (Gordon Lyon), რომელიც ასევე ცნობილია თავისი ფსევდონიმით ფიოდორ ვასკოვიჩი (Fyodor Vaskovich). Nmap განკუთვნილია ქსელში არსებული კვანძების და სერვისების აღმოჩენისათვის. Nmap პირველად გამოჩნდა 1997 წელს ჟურნალ Phrack Magazine_ში სორს კოდთან ერთად. ის საკმაოდ პოპულარული ხელსაწყოა ქსელური თუ სისტემური ადმინისტრატორებისთვის. პროგრამა თავსებადია სხვადასხვა ოპერაციულ სისტემებთან. ის შესაძლებელია დაყენდეს როგორც Linux_ზე, ასევე Windows_სა და Mac OS_ზე. მისი გამოყენება შესაძლებელია როგორც გრაფიკულ ინტერფეისით (ZenMap) ასევე კომანდ ლაინ ინტერფეისით.

Nmap-ის საშუალებით შესაძლებელია როგორც ქსელში არსებული კვანძების და სერვისების აღმოჩენა, ასევე ამ სერვისების ვერსიების გაგება, კვანძებზე არსებული ოპერაციული სისტემების აღმოჩენა. სკანირებისას ასევე შესაძლებელია სკრიპტების გამოყენება, რომელიც აფართოებს სკანერის ფუნქციონალს. სკრიპტებით შესაძლებელია მოწყვლადობების აღმოჩენა, სერვისის აღმოენისას დეტალური ინფორმაციის ჩვენება და სხვა. Nmap_ის ერთ-ერთ თავისებურებას ასევე წარმოადგენს ის, რომ ის „ერგება“ ქსელში არსებულ სიტუაციას დაყოვნებიდან და დატვირთვიდან გამომდინარე.

Nikto არის ღია კოდის მქონე ვებ სერვერების სკანერი. მისი 1.00 ბეტა ვერსია გამოვიდა 2001 წლის 27 დეკემბერს, რომელსაც ძალიან სწრაფად მოყვა 1.01 ვერსიის რელიზი. Nikto არის ღია კოდის მქონდე ვებ სერვერების სკანირების ხელსაწყო, რომელსაც შეუძლია შეამოწმოს ვებ სერვისები სხვადასხვა სისუსტეზე, მათ შორისაა 6700-ზე მეტი საფრთხის შემცველი ფაილი/პროგრამა, რომელზეც ის ამოწმებს ვებ სერვერებს. მას შეუძლია შეამოწმოს სისტემები ვადაგასულ ვერსიებზე, ვერსიებისთვის სპეციფიურ სისუსტეებზე. მას ასევე შეუძლია შეამოწმოს ვებ სერვისების

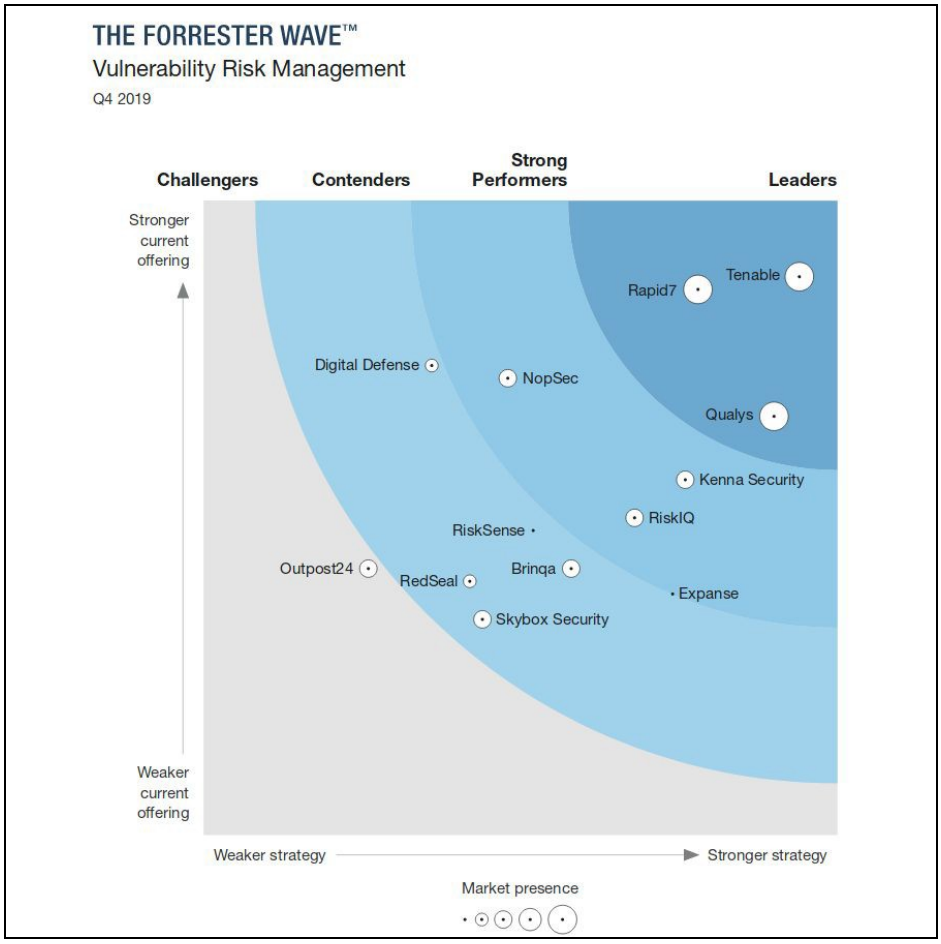
კონფიგურაციები, მაგალითად რამოდენიმე ინდექს ფაილზე, HTTP სერვერის მომართვებზე და სხვა.

Nikto ისეა არქიტექტურულად აგებული, რომ იყოს მაქსიმალურად შეუმჩნეველი. ის ამოწმებს ვებ სერვერბს მაქსიმალურად მცირე დროში. მას ასევე აქვს LibWhisker_ის ანტი IDS მეთოდი, რომლის საშუალებითაც, შესაძლოა ზოგიერთი IDS/IPS სისტემის მოტყუება. ცხადია Nikto არ ამოწმებს ვებ სერვერებს მხოლოდ სისუსტეებზე, მისი საშუალებით შესაძლებელია ინფორმაციის მოპოვება, რომელიც შესაძლებელია სულაც არ იყოს საფრთხის შემცველი, თუმცა ამ ინფორამციის გამოყენება სისტემებზე ინფორმაციის მოპოვებისთვის ნამდვილად გამოსადეგია.

SQLMap არის ღია კოდის მქონე პროგრამა რომელიც გამოიყენება მონაცმთა ბაზებში არსებული სისუსტეების აღმოჩენისთვის და შეტევისთვის. მისი საშუალებით შესაძლებელია SQL ინექციის აღმოჩენა და შეტევის განხორციელება ავტომატურ რეჟიმში. პროგრამა თავსებადია როგორც Linux სისტემასთან, ასევე Windows_სა და MacOS_თან. მისი ისტორია იწყება 2005 წელს, როდესაც დანიელ ბელუჩიმ(Daniele Bellucci) დაარეგისტრირა SQLMap_ის პროექტის SourceForge პლათფორმაზე. იგივე წელს დანიელი ტოვებს პროექტს და პროექტს აგრძელებს ბერნარდო დამელე ა.გ.(Bernardo Damele A.G.) სისუსტეების აღმოჩენასთან ერთად SQLMap_ით შესაძლებელია, სისუსტეების ექსპლოიტირება და უშუალოდ მონაცემთა ბაზებან ინტერაქცია. შესაძლებელია განხორციელდეს ქმედებები, როგორიცაა ცხრილების ნახვა, ცვლილება, წაშლა და ასე შემდეგ. პროგრამას აქვს სხვადასხვა მონაცემთა ბაზის მხარდაჭერა: MySQL, Oracle, PostgreSQL, MS SQL Server, IBM DB2 და სხვა.

ზემოთ ჩამოთვლილი სკანერები ძირითადად გამოიყენება შეღწევადობის ტესტირების დროს. როდესაც ადამიანი ახორციელებს შეღწევადობის ტესტირებას. ადამიანის მიერ განხორციელებული შეღწევადობის ტესტირება უფრო სიღრმისეულია. სკანერებს ავტომატურ რეჟიმში არ შეუძლიათ ისეთი სიღრმისეული ანალიზის გაკეთება, როგორც

ადამიანს. მაგრამ ადამიანის მიერ ტესტირებას აქვს ერთი ნაკლი, ეს არის დანახარჯი, როგორც ადამიანური ასევე ფულადი რესურსისა. სისუსტეების ავტომატიზაციისთვის გამოიყენება მოწყვლადობების სკანერების გადაწყვეტილებები. ბაზარზე არსებობს, ბევრი სხვადასხვა მოწყვლადობის სკანერის გადაწყვეტილება. მათი არჩევისას აუცილებელია გათვალისწინებული იქნეს ბიზნესის მოთხოვნა. ქვემოთ მოცემულია Forester_ის მოწყვლადობების რისკის მართვის (Vulnerability Risk Management) რეპორტი, რომელშიც მოცემულია ტოპ ვენდორები ამ მიმართულებით. მოცემული რეპორტი გვიქმნის ზოგად წარმოდგენას, თუ რა ვენდორები არსებობს დღეს ბაზარზე (ნახ.36).

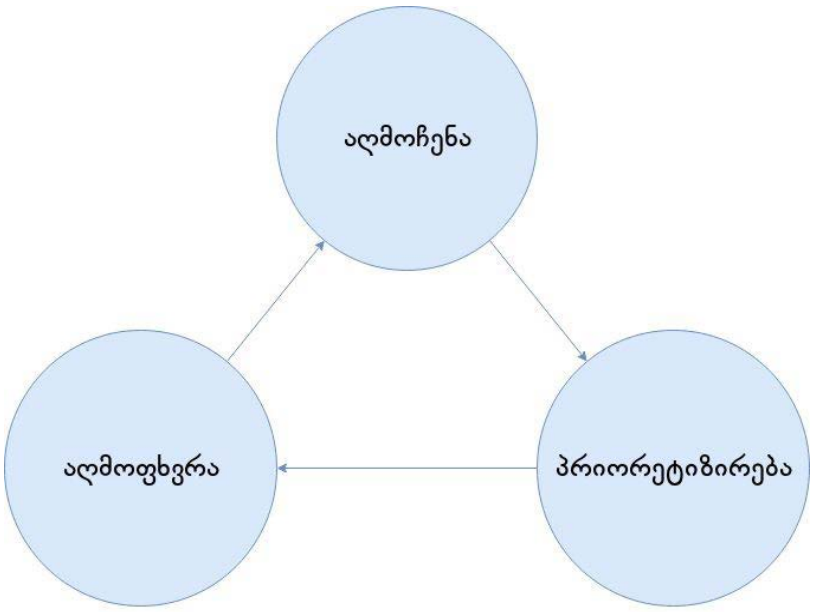


ნახ. 36. მოწყვლადობების რისკის მართვის ფანჯარა

როგორც ნახაზიდან ვხედავთ, მოწინავე ადგილებს იკავებენ Tenable, Rapid7 და Qualys ვენდორები. გასათვალისწინებელია ის ფაქტი, რომ

მიუხედავად ინფრასტრუქტურაში არსებული მოწყვლადობის სკანერისა, აუცილებელია გარკვეული პერიოდულობით ჩატარდეს ადამიანის ან ადამიანთა ჯგუფის მიერ ინფრასტრუქტურაზე შეღწევადობის ტესტირება. მოწყვლადობის სკანერი არ ხსნის ადამიანის მიერ ჩატარებულ შეღწევადობის ტესტირების აუცილებლობას.

მოწყვლადობების მართვის პროცესს აქვს თავისი სასიცოცხლო ციკლი. სხვადასხვა კომპანია სხვადასხვანაირად უდგება ამ პროცესს. პროცესის გასამარტივებლად და მის ნათლად წარმოსაჩენად გამოვიყენებთ გამარტივებულ მეთოდს, რომელიც შეიცავს შემდეგ ნაბიჯებს: აღმოჩენა, პრიორეტიზირება, აღმოფხვრა. ცხადია ეს პროცესი მეტ-ნაკლებად განსხვავებულია ყველა კომპანიისთვის. ინფრასტრუქტურიდან გამომდინარე ეს პროცესი ცვალებადია, თუმცა ზოგადი იდეა იგივე რჩება. ამ პროცესის მიზანია ინფრასტრუქტურაში არსებული სისუსტეების აღმოჩენა და მათი აღმოფხვრა. ასევე გასათვალისწინებელია, რომ თუკი გავითვალისწინებთ ზემოთ გამოთვლილ საუკეთესო პრაქტიკების რჩევებს ინფრასტრუქტურაში არსებული სისუსტეების რაოდენობა საგრძნობლად შემცირდება (ნახ. 37).



ნახ. 37. მოწყვლადობების მართვის სასიცოცხლო ციკლი

აღმოჩენა არის პირველი ეტაპი. სისტემებზე სისუსტეების აღმოჩენა შესაძლებელია როგორც ხელით, ასევე ავტომატურ რეჟიმში სხვადასხვა ხელსაწყოს გამოყენებით. სწორედ აღმოჩენის ავტომატიზაციაში გვეხმარება მოწყვლადობის სკანერი. მოწყვლადობის სკანერში იქმნება პოლიტიკა, რომლის მიხედვით გარკვეული პერიოდულობით, მაგალითად კვირაში ერთხელ სისტემა ასკანერებს ქსელში ჩართულ კვანძებს და ცდილობს აღმოაჩინოს სისუსტეები.

პრიორეტიზაცია არის პროცესი, რომლის დროსაც სისტემებს და სისუსტეებს ვალაგებთ მათი მნიშვნელობიდან გამომდინარე. მაგალითისათვის სერვერი რომელზეც მუშავდება მნიშვნელოვანი მონაცემები უფრო მნიშვნელოვანია, ვიდრე საბოლოო მომხმარებლის სამუშაო მაგიდა. შესაბამისად სისუსტეების აღმოფხვრის დროს პირველ რიგში მოვაგვარებთ პრობლემას სერვერზე შემდეგ კი სამუშაო მაგიდაზე. ესაა ზოგადი მაგალითი იმისა, თუ როგორ ხდება აქტივების პრიორეტიზირება, თუმცა ყველა ინფრასტრუქტურა ინდივიდუალურია და საჭიროებს ინდივიდუალურ მიდგომას.

ასეტების მნიშვნელობასთან ერთად გასათვალისწინებელია, სისუსტეების ბოროტმოქმედების მიერ გამოყენების ალბათობა და გამოყენების შემთხვევაში ზემოქმედების დონე. რაც პირველ რიგში გულისხმობს იმას, თუ რამდენად არის შესაძლებელი სისუსტის რეალურად გამოყენება, არსებობს თუ არა ცნობილი პროგრამული კოდი, რომელიც იყენებს კონკრეტულ სისუსტეს, რამდენად რთულია ამ სისუსტის გამოყენება. მეორე რიგში კი, თუკი ბოროტმოქმედმა გამოიყენა სისუსტე რა სახის ზიანი მიადგება ამით სისტემას. ბოროტმოქმედი შეძლებს ინფორმაციის მოპარვას, სისტემაზე უფლებების მოპოვებას, თუ რა სახის ზიანის განხორციელებას შეძლებს ის.

აღმოჩენის და პრიორეტიზირების შედეგად ვიცით რა სახის სისუსტეები გვაქვს და რომელი სისუსტიდან უნდა დავიწყოთ მათი აღმოფხვრა. აღმოფხვრის პროცესი ინდივიდუალურია ყველა

სისტემისათვის. ზოგიერთ მოწყვლადობის სკანერი სისუსტის აღმოჩენის შემდეგ გვაძლევს გარკვეულ "რჩევას" თუ როგორ აღმოვფხვრათ სისუსტე. იქნება ეს უბრალო რჩევა სისტემის განახლების შესახებ, კონფიგურაციის ცვლილებაზე, თუ ბმული სტატიაზე სადაც განხილულია თუ როგორ უნდა აღმოიფხვრას სისუსტე. უმეტეს შემთხვევაში სისუსტის აღმოფხვრა შესაძლებელია პროგრამული უზრუნველყოფის განახლებით ან კონფიგურაციის ცვლილებით.

OpenVAS არის ღია კოდის მქონე მოწყვლადობის სკანერი. თავდაპირველად მას სახელად ერქვა GNessUs, იქიდან გამომდინარე, რომ ის არის ბაზირებული იმჟამინდელი ღია კოდის მქონდე Nessus მოწყვლადობის სკანერზე, რომელიც ამჟამად კომპანია Tenable_ს პროდუქტია და არ აქვს ღია კოდი. GNessUs იგივე OpenVAS პროექტ Nessus_ს გამოეყო 2005 წლის ოქტომბერში მას შემდეგ რაც Nessus_მა თავისი სორს კოდი გახადა დახურული. ამჟამად OpenVAS_სის განვითარებაზე ზრუნავს კომპანია Greenbone Networks რომელიც დაარსდა 2008 წელს გერმანიაში. ზემოთ ჩამოთვლილ მწარმოებლების(Rapid7, Tenable, Qualys) პროდუქტებთან შედარებით OpenVAS_ს ფუნქციონალური თვალსაზრისით უფრო ნაკლები შესაძლებლობები გააჩნია, თუმცა პატარა და საშუალო კომპანიებისთვის ნამდვილად ხელსაყრელი ხელსაწყოა. როგორც აღვნიშნეთ OpenVAS არის ღია კოდის მქონდე პროდუქტი შესაბამისად, მისი გამოყენება შეუძლია ნებისმიერს უსასყიდლოდ. Greenbone Networks_ს OpenVAS_ზე აქვს ბაზირებული საკუთარი გადაწყვეტილებებიც, რომლის გამოსაყენებლად საჭიროა მათი შესყიდვა.

ზემოთ აღნიშნულიდან შევძელით გვენახა, თუ როგორ შეიძლება მარტივი სკანირებით კვანძზე/ქსელში არსებული სისუსტეების გამოვლენა. სკანირების შემდგომ საჭიროა შედეგების ანალიზი და მათ აღმოსაფხვრელად შესაბამისი ზომების მიღება, იქნება ეს კონფიგურაციის ცვლილება, პროგრამული განახლება თუ სხვა.

2.4. უსაფრთხოების უზრუნველყოფის ალგორითმების დამუშავება

უსაფრთხოების მხარდამჭერი სისტემა რომ გაცილებით უფრო ეგექტური იყოს, აუცილებელია განხილული იქნას მისი ალგორითმული უზრუნველყოფა, რომელიც წარმოჩენილია ცალკეული ალგორითმების სახით.

ცალკეული ალგორითმული ბლოკი უნდა იყოს იმისთვის გათვალისწინებული, რომ უსაფრთხოების ყველა ფუნქცია თანმიმდევრულად იქნას შესრულებული. ამასთანავე გასათვალისწინებელია ის მომენტიც, რომ უნდა იყოს პროგრამირების პროცესიც წარიმართოს მარტივად.

ცალკეულად მოვიყვანოთ ყველა მეთოდის ალგორითმული ბლოკი, რომელსაც გააჩნია თავისი ფუნქციონალური დანიშნულებები.

სიმბოლოების დაშიფვრის კომბინირებული დამუშავების ალგორითმის მიხედვით ხდება მომხმარებლის მიერ შეტანილი გამოსახულების (პაროლი ან სიმბოლოებისაგან შემდგარი სიტყვები) დაშიფვრა, მისი ამოცნობა და შესაბამისად მონაცემთა ბაზების ფორმირება.

განვიხილოთ სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ალგორითმი (ნახ. 38).

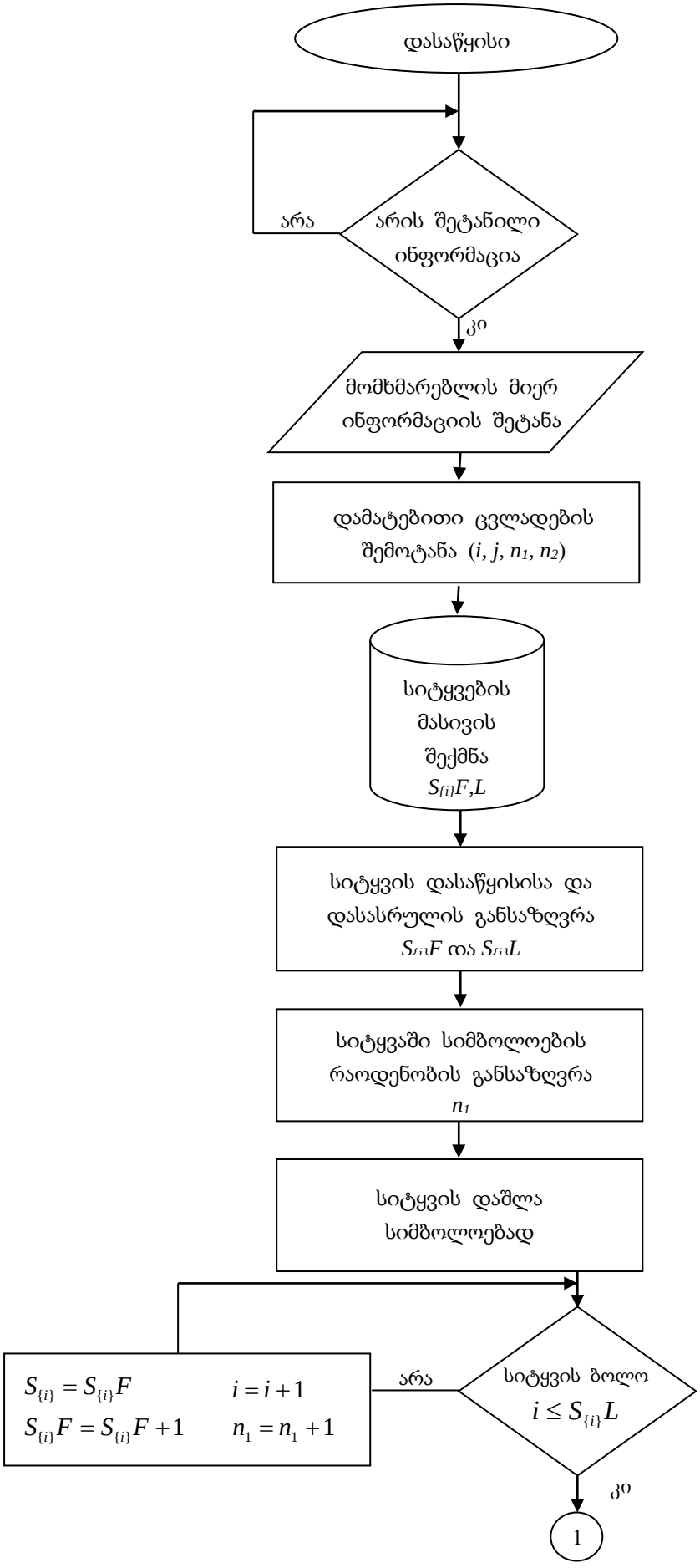
ალგორითმის მუშაობის საწყის ეტაპზე ხდება იმის განსაზღვრა, შეტანილია თუ არა მომხმარებლის მიერ ინფორმაცია. პირველ ეტაპზე მომხმარებლის მიერ შეტანილი პაროლი იწერება სპეციალურ მასივში, სადაც განსაზღვრულია სიტყვის დასაწყისი და დასასრული. აგრეთვე ხდება სიტყვის დაშლა სიმბოლოებად და ცალკეული სიმბოლოსთვის განსაზღვრულია მისი ინდექსი.

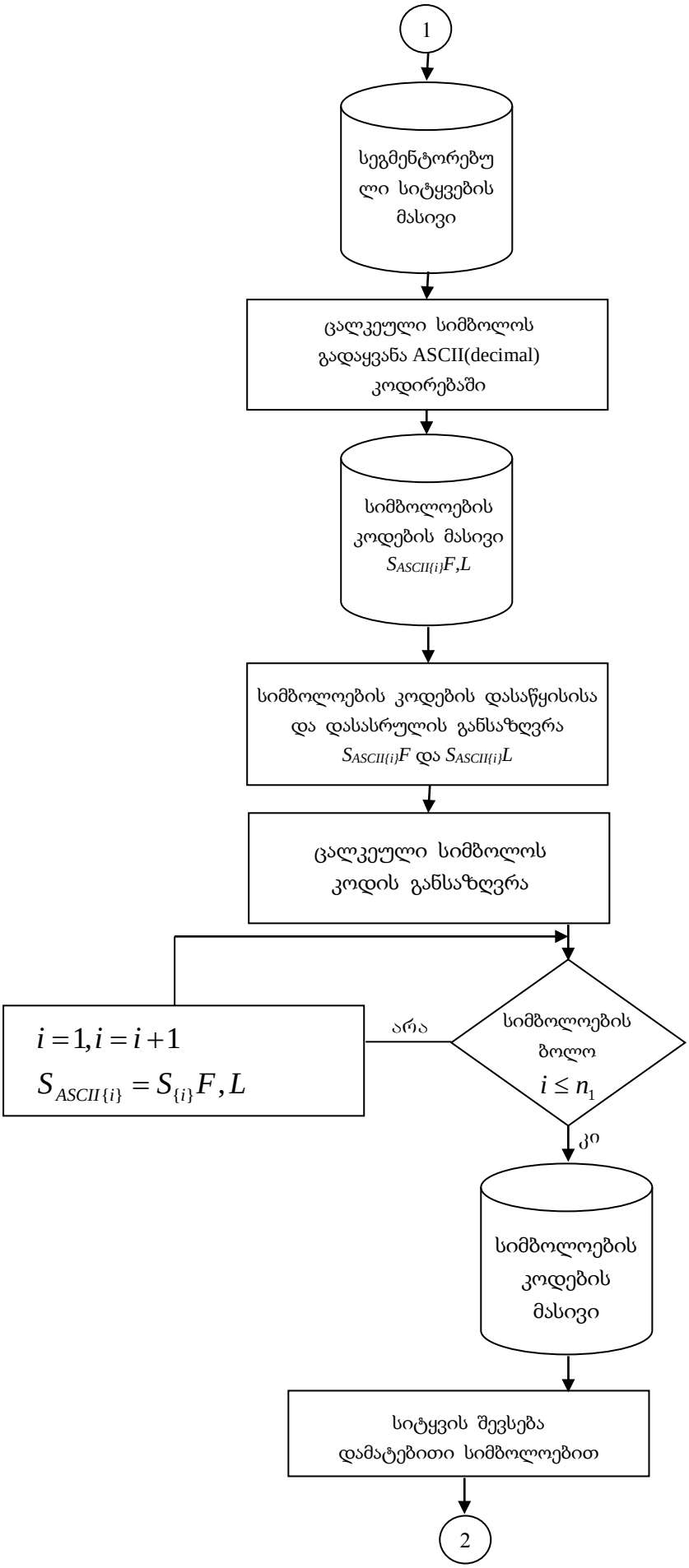
სისტემაში შემოდის დამატებითი ცვლადები, რათა განისაზღვროს სიმბოლოებისა და დამატებითი სიმბოლოების ინდექსები თავისი რაოდე ნობებით.

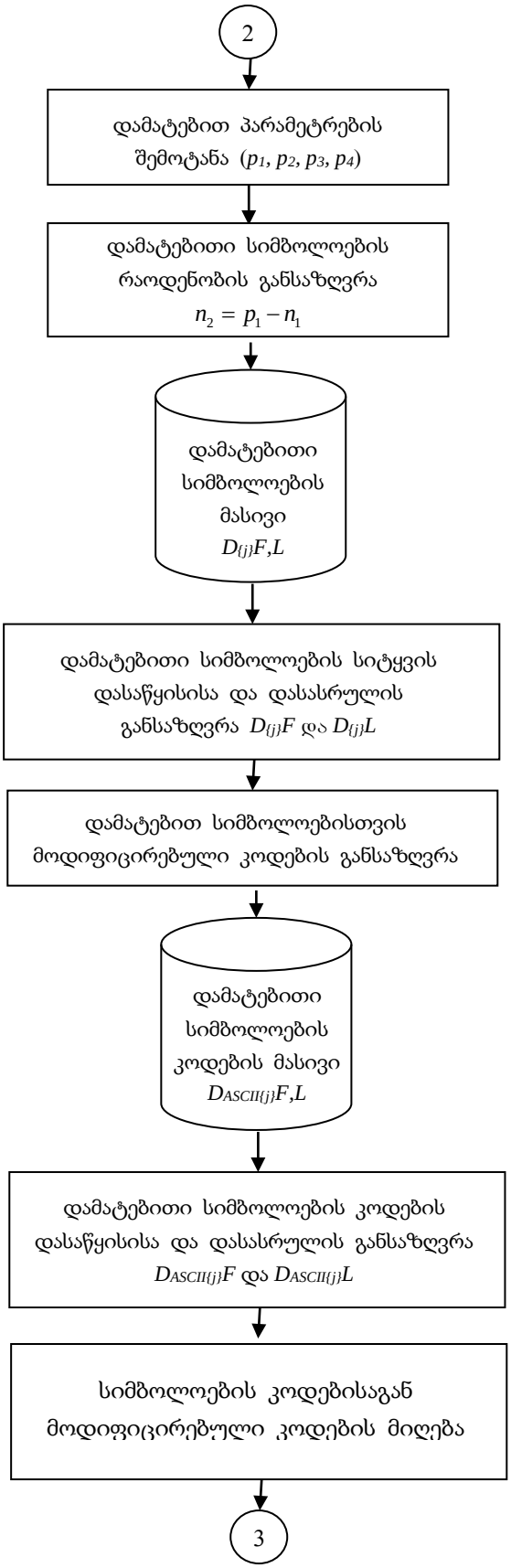
შემდეგ ხდება სიტყვაში სიმბოლოების დაშლა და ცალკეული სიმბოლოსთვის ინდექსის განსაზღვრა, რის შედეგაც მიიღება სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი.

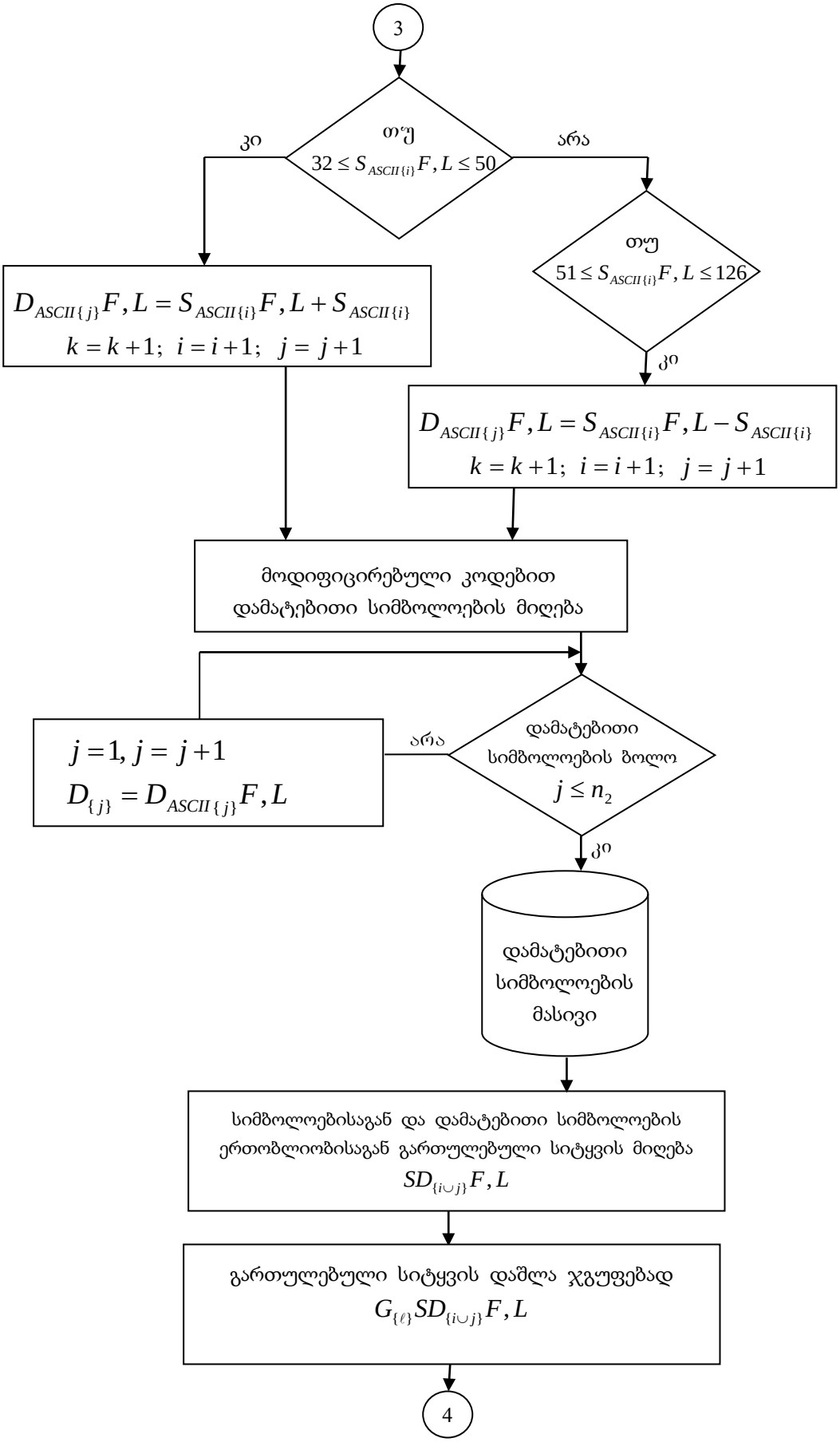
თითოეული სიმბოლო განიხილება ASCII(decimal) კოდირებაში და მათთთვის განისაზღვრება კოდები. ამისათვის შემოღებულია მასივი, სადაც განსაზღვრულია სიმბოლოების კოდების დასაწყისი და დასასრული. შემდეგ ხდება ცალკეული სიმბოლოსთვის კოდის განსაზღვრა და მისი ჩაწერა სიმბოლოების კოდების მასივში, რის შედეგაც მიიღება სიმბოლოების კოდების ერთობლიობისაგან შემდგარი რიცხვები, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსის კოდი. შემდეგ უნდა მოვახდინოთ სიტყვის შევსება დამატებითი სიმბოლოებით გარკვეული პარამეტრის დაყენებით. თავდაპირველად განისაზღვრება დამატებითი სიმბოლოების რაოდენობა, შემდეგ დგება მასივი, სადაც იწერება დამატებითი სიმბოლოები, რაშიც განსაზღვრულია დამატებითი სიმბოლოების სიტყვის დასაწყისი და დასასრული. შემდგომ ცალკეული სიმბოლოს განსაზღვრული კოდისთვის განისაზღვრება მოდიფიცირებული კოდები, რომელიც იწერება სპეციალურ მასივში, რაშიც განსაზღვრულია დამატებითი სიმბოლოების კოდების დასაწყისი და დასასრული.

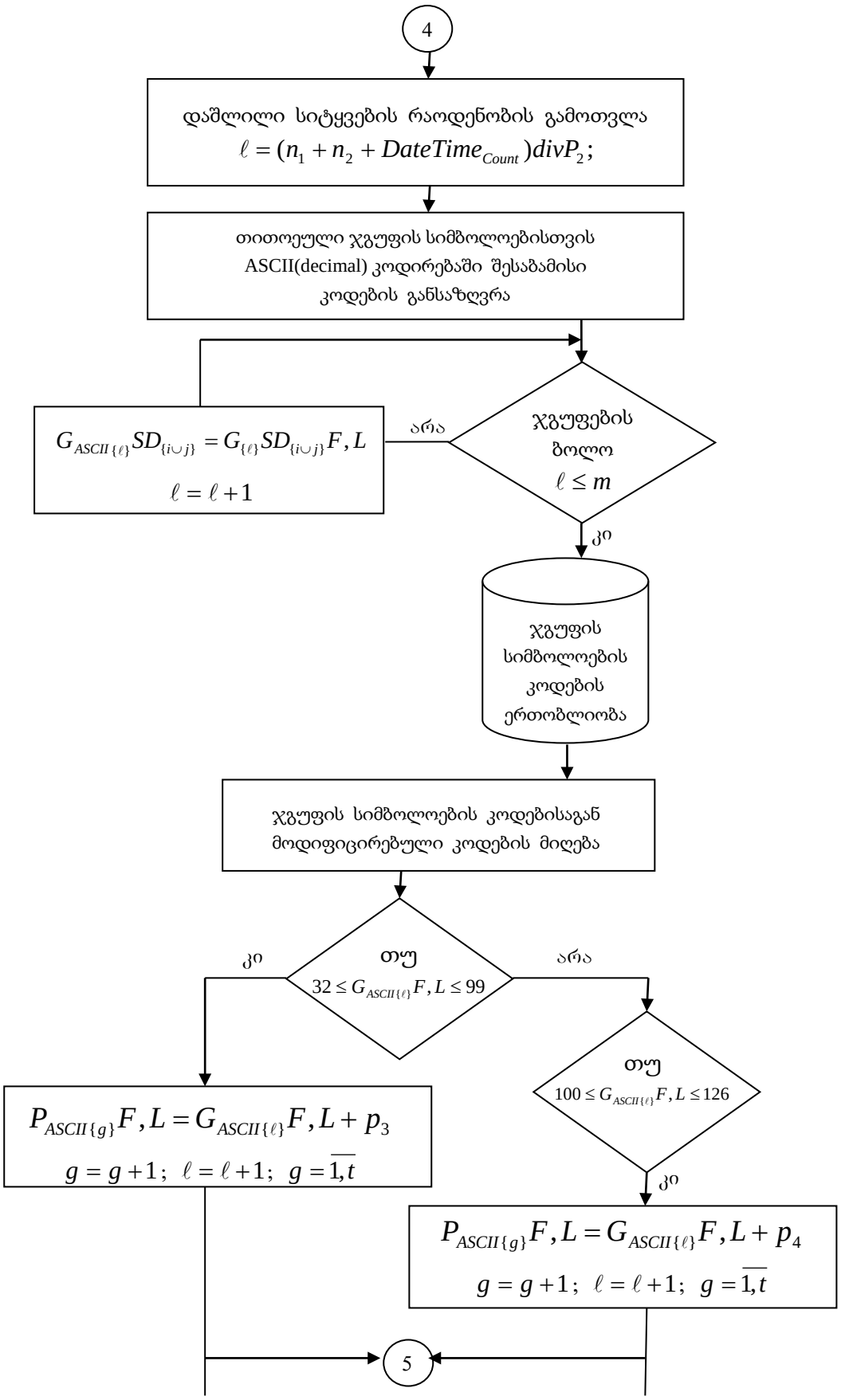
მოცემული მეთოდის მიზანი მოდიფიცირებული კოდებით დასაშიფრი სიმბოლოების გადაყვანა სპეციალურ სიმბოლოებში. ASCII(decimal) კოდირების სისტემაში სიმბოლოების კოდები შეესაბამება 32-დან 126-ის ჩათვლით, ხოლო სპეციალური სიმბოლოების კოდები შეესაბამება 128-დან 255-ის ჩათვლით.

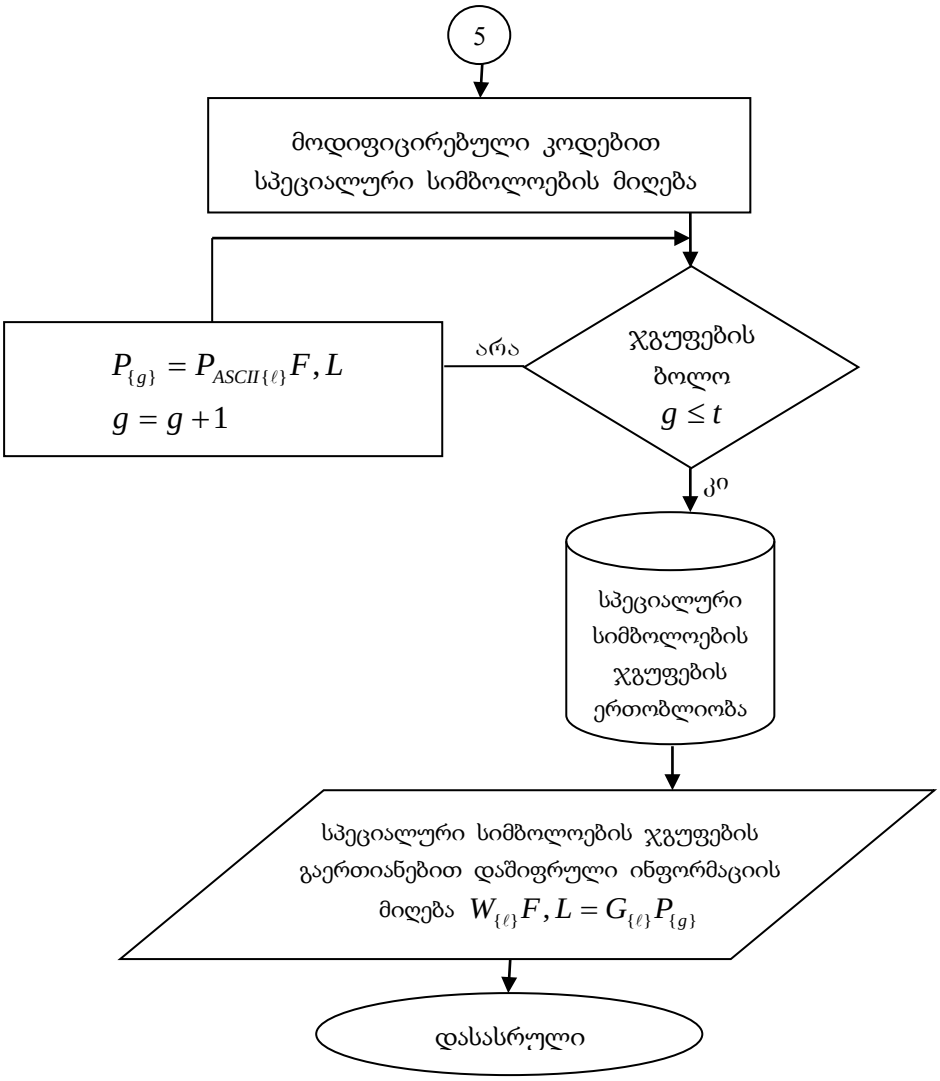

დასაწყისი
არის შეტანილი ინფორმაცია
არა
კი
მომხმარებლის მიერ ინფორმაციის შეტანა
დამატებითი ცვლადების შემოტანა (i, j, n1, n2)
სიტყვების მასივის შექმნა S{i}F,L
სიტყვის დასაწყისისა და დასასრულის განსაზღვრა S{i}F და S{i}L
სიტყვაში სიმბოლოების რაოდენობის განსაზღვრა n1
სიტყვის დაშლა სიმბოლოებად
სიტყვის ბოლო i ≤ S{i}L
არა
S{i} = S{i}F i = i + 1
S{i}F = S{i}F + 1 n1 = n1 + 1
კი
1


1
სეგმენტორებუ
ლი სიტყვების
მასივი
ცალკეული სიმბოლოს
გადაყვანა ASCII(decimal)
კოდირებაში
სიმბოლოების
კოდების მასივი
$S_{ASCII\{i\}}F,L$
სიმბოლოების კოდების დასაწყისისა
და დასასრულის განსაზღვრა
$S_{ASCII\{i\}}F$ და $S_{ASCII\{i\}}L$
ცალკეული სიმბოლოს
კოდის განსაზღვრა
$i=1, i=i+1$
$S_{ASCII\{i\}} = S_{\{i\}}F, L$
არა
სიმბოლოების
ბოლო
$i \le n_1$
კი
სიმბოლოების
კოდების
მასივი
სიტყვის შევსება
დამატებითი სიმბოლოებით
2


2
დამატებით პარამეტრების შემოტანა (p_1, p_2, p_3, p_4)
დამატებითი სიმბოლოების რაოდენობის განსაზღვრა $n_2 = p_1 - n_1$
დამატებითი სიმბოლოების მასივი $D_{[j]}F,L$
დამატებითი სიმბოლოების სიტყვის დასაწყისისა და დასასრულის განსაზღვრა $D_{[j]}F$ და $D_{[j]}L$
დამატებით სიმბოლოებისთვის მოდიფიცირებული კოდების განსაზღვრა
დამატებითი სიმბოლოების კოდების მასივი $D_{ASCII[j]}F,L$
დამატებითი სიმბოლოების კოდების დასაწყისისა და დასასრულის განსაზღვრა $D_{ASCII[j]}F$ და $D_{ASCII[j]}L$
სიმბოლოების კოდებისაგან მოდიფიცირებული კოდების მიღება
3


3
თუ
$32 \le S_{ASCII\{i\}}F, L \le 50$
კი
არა
თუ
$51 \le S_{ASCII\{i\}}F, L \le 126$
კი
$D_{ASCII\{j\}}F, L = S_{ASCII\{i\}}F, L + S_{ASCII\{i\}}$
$k = k+1;\ i = i+1;\ j = j+1$
$D_{ASCII\{j\}}F, L = S_{ASCII\{i\}}F, L - S_{ASCII\{i\}}$
$k = k+1;\ i = i+1;\ j = j+1$
მოდიფიცირებული კოდებით
დამატებითი სიმბოლოების მიღება
$j = 1, j = j+1$
$D_{\{j\}} = D_{ASCII\{j\}}F, L$
არა
დამატებითი
სიმბოლოების ბოლო
$j \le n_2$
კი
დამატებითი
სიმბოლოების
მასივი
სიმბოლოებისაგან და დამატებითი სიმბოლოების
ერთობლიობისაგან გართულებული სიტყვის მიღება
$SD_{\{i \cup j\}}F, L$
გართულებული სიტყვის დაშლა ჯგუფებად
$G_{\{\ell\}}SD_{\{i \cup j\}}F, L$
4


4
დაშლილი სიტყვების რაოდენობის გამოთვლა
$\ell = (n_1 + n_2 + DateTime_{Count})divP_2;$
თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში შესაბამისი კოდების განსაზღვრა
ჯგუფების ბოლო
$\ell \le m$
არა
$G_{ASCII\{\ell\}}SD_{\{i\cup j\}} = G_{\{\ell\}}SD_{\{i\cup j\}}F, L$
$\ell = \ell + 1$
კი
ჯგუფის სიმბოლოების კოდების ერთობლიობა
ჯგუფის სიმბოლოების კოდებისაგან მოდიფიცირებული კოდების მიღება
თუ
$32 \le G_{ASCII\{\ell\}}F, L \le 99$
კი
არა
თუ
$100 \le G_{ASCII\{\ell\}}F, L \le 126$
კი
$P_{ASCII\{g\}}F, L = G_{ASCII\{\ell\}}F, L + p_3$
$g = g + 1;\ \ell = \ell + 1;\ g = \overline{1,t}$
$P_{ASCII\{g\}}F, L = G_{ASCII\{\ell\}}F, L + p_4$
$g = g + 1;\ \ell = \ell + 1;\ g = \overline{1,t}$
5



ნახ. 38. სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ალგორითმი

სიმბოლოების კოდების გარდაქმნა ხდება შემდეგნაირად. აიღება სიტყვის პირველი სიმბოლოს კოდი, გადამოწმდება მისი მდებარეობის არეალი. თუ კოდი მდებარეობს 32-დან 50-ის ჩათვლით, მაშინ შესრულდება შემდეგი მოქმედება: სიმბოლოს კოდს დაემატება მისი რიგითობა, ანუ ინდექსი, შემდეგ მეორე სიმბოლოს კოდს დაემატება მეორე ინდექსი და ა.შ. სიტყვის ბოლომდე. თუ კოდი მდებარეობს 51-დან 126-ის ჩათვლით, მაშინ აკლდება. მიღებული ახალი კოდებით დგება დამატებითი სიმბოლოების ჯგუფი. ეს პროცესი მიმდინარეობს იქამდე, ვიდრე არ დაკმაყოფილდება გარკვეული პარამეტრის მნიშვნელობა. მიღებული ახალი მოდიფიცირებული კოდებით დგება

დამატებითი სიმბოლოების ჯგუფი, რის შედეგაც მიიღება დამატებითი სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი.

მიღებული სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით იქმნება „გართულებული“ სიტყვა (პაროლი), რომელსაც ემატება მიმდინარე თარიღისა და დროის რიცხობრივი მნიშვნელობები.

შემდეგ ხდება მიღებული სიტყვის დაშლა (ჯგუფების შექმნა) სისტემაში დაყენებული პარამეტრის მიხედვით. შემდეგ თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში ხდება მათი შესაბამისი კოდების განსაზღვრა, რის შედეგაც მიიღება ჯგუფის სიმბოლოების კოდების ერთობლიობისაგან შემდგარი რიცხვები, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსის კოდი.

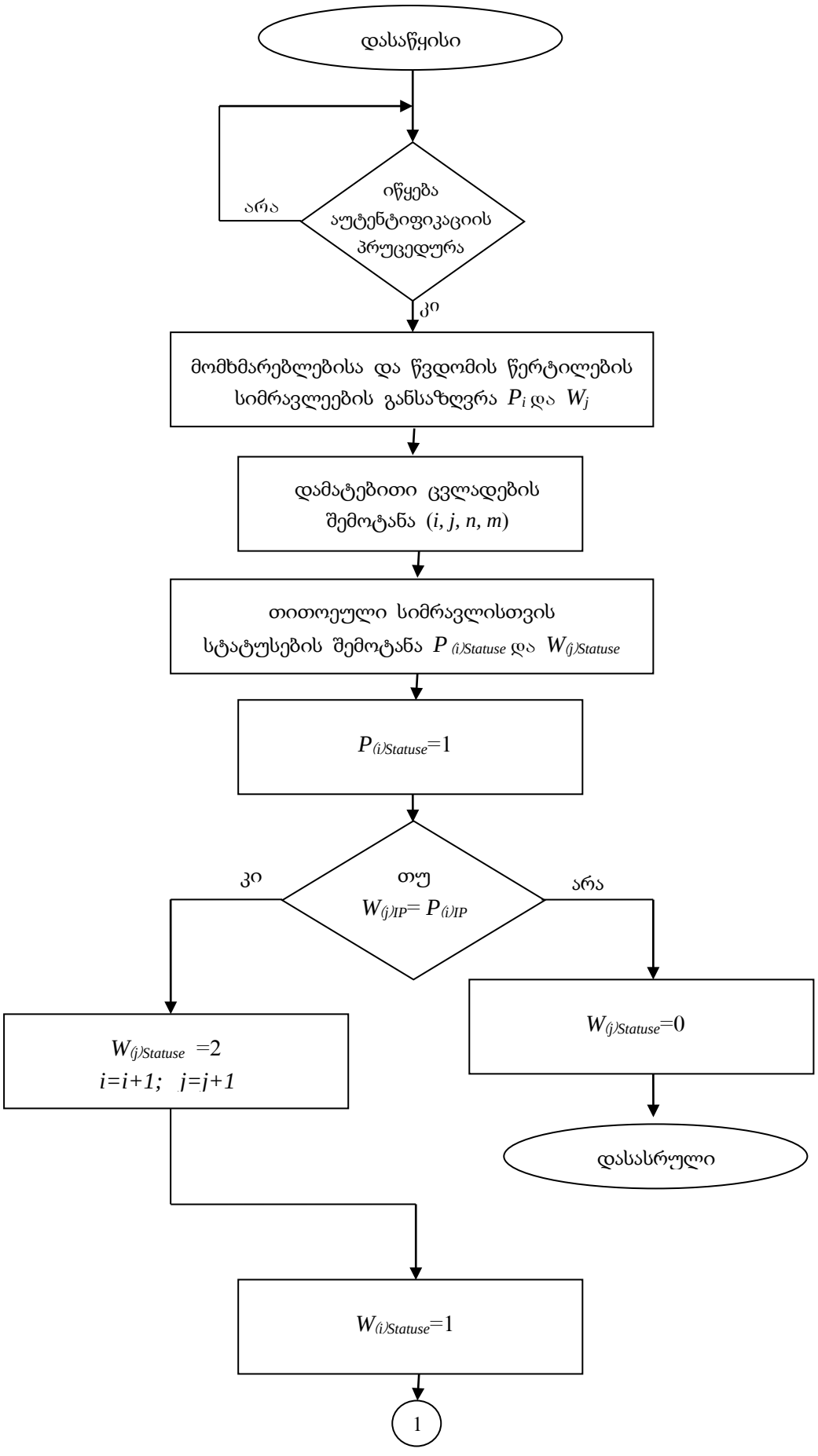
მიღებული კოდების რიცხობრივი მნიშვნელობა გარდაიქმნება სხვა რიცხობრივ მნიშვნელობად და მიიღება ახალი კოდების სიმრავლე. მიღებული სიმბოლოების კოდების გარდაქმნა ხდება შემდეგნაირად. აიღება სიტყვის პირველი სიმბოლოს კოდი, გადამოწმდება მისი მდებარეობის არეალი. თუ კოდი მდებარეობს 32-დან 99-ის ჩათვლით, მაშინ შესრულდება შემდეგი მოქმედება: სიმბოლოს კოდს დაემატება პარამეტრის მნიშვნელობა, ხოლოს თუ კოდი მდებარეობს 100-დან 126-ის ჩათვლით, მაშინ სიმბოლოს კოდს დაემატება პარამეტრის მნიშვნელობა. მიღებული ახალი მოდიფიცირებული კოდებით დგება სპეციალური სიმბოლოების ჯგუფი. სპეციალური სიმბოლოებისაგან შემდგარი ჯგუფების გაერთიანებით კი მიიღება სპეციალური სიმბოლოების ერთობლიობისგან შემდგარი დაშიფრული ინფორმაცია.

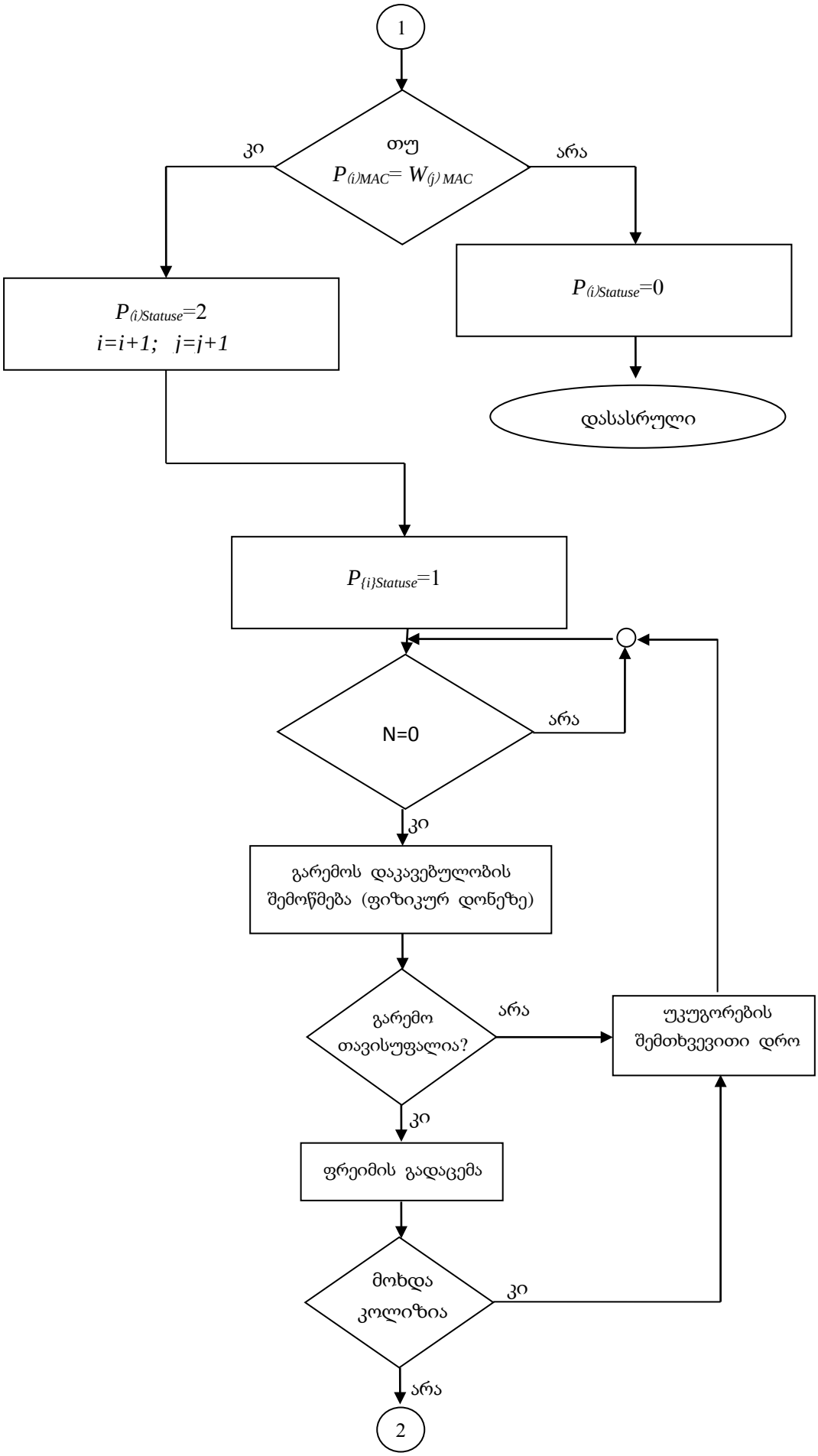
დაშიფრული ინფორმაცია ცენტრალურ სერვერს მიეწოდება ჯგუფების სახით. თუ პირველი ჯგუფის იდენტიფიკაცია წარმატებით დასრულდა, სერვერი ატყობინებს და ბრძანებას გამოსცემს მეორე ჯგუფის გამოშვებაზე და ა.შ. ჯგუფის ბოლომდე. თუ რომელიმე ჯგუფი არ დაემთხვა სერვერი მაშინვე ბლოკავს აღნიშნულ მომხმარებელს.

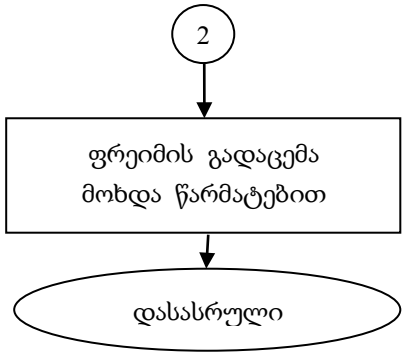
დაშიფრული ინფორმაციის ამოშიფვრა ცენტრალური სერვერის მიერ ხდება ზემოთგანხილული მეთოდის უკუალგორითმის საშუალებით იგივე პარამეტრების გამოყენებით. (ნახ. 39).

ქსელში არსებულ მოწყობილობას გააჩნია უნიკალური MAC და IP მისამართები, რომლის საშუალებითაც ხდება ინფორმაციის გაცვლა მოწყობილობებს შორის. აგრეთვე ხდება მომხმარებლების აუტენტიფიკაციის პროცესები, ამისათვის დაგვჭირდება მომხმარებლების სიმრავლე და ქსელში არსებული ქსელური მოწყობილობების სიმრავლე. ყველა სიმრავლისთვის შემოღებულია სტატუსები, რომლებსაც ენიჭება გარკვეული რუცხობრივი მნიშვნელობები.

მომხმარებლის მიერ როდესაც ხდება მიმართვა ქსელურ მოწყობილობებთან, მიმდინარეობს სტატუსის მნიშვნელობების ცვლილება, ხოლოდ როდესაც არ ხდება დაკავშირება, სტატუსს ენიჭება მნიშვნელობა - 0 და წყდება კავშირი.


დასაწყისი
იწყება აუტენტიფიკაციის პრუცედურა
არა
კი
მომხმარებლებისა და წვდომის წერტილების სიმრავლეების განსაზღვრა P_i და W_j
დამატებითი ცვლადების შემოტანა (i, j, n, m)
თითოეული სიმრავლისთვის სტატუსების შემოტანა $P_{(i)Statuse}$ და $W_{(j)Statuse}$
$P_{(i)Statuse}=1$
თუ $W_{(j)IP}= P_{(i)IP}$
კი
არა
$W_{(j)Statuse}=2$
$i=i+1;\ \ j=j+1$
$W_{(j)Statuse}=0$
დასასრული
$W_{(i)Statuse}=1$
1


1
თუ
$P_{(i)MAC}= W_{(j)MAC}$
კი
არა
$P_{(i)Statuse}=2$
$i=i+1;\ \ j=j+1$
$P_{(i)Statuse}=0$
დასასრული
$P_{\{i\}Statuse}=1$
N=0
არა
კი
გარემოს დაკავებულობის შემოწმება (ფიზიკურ დონეზე)
გარემო თავისუფალია?
არა
უკუგორების შემთხვევითი დრო
კი
ფრეიმის გადაცემა
მოხდა კოლიზია
კი
არა
2



ნახ. 39. კორპორაციულ ქსელში უსაფრთხოების ამაღლების ალგორითმი

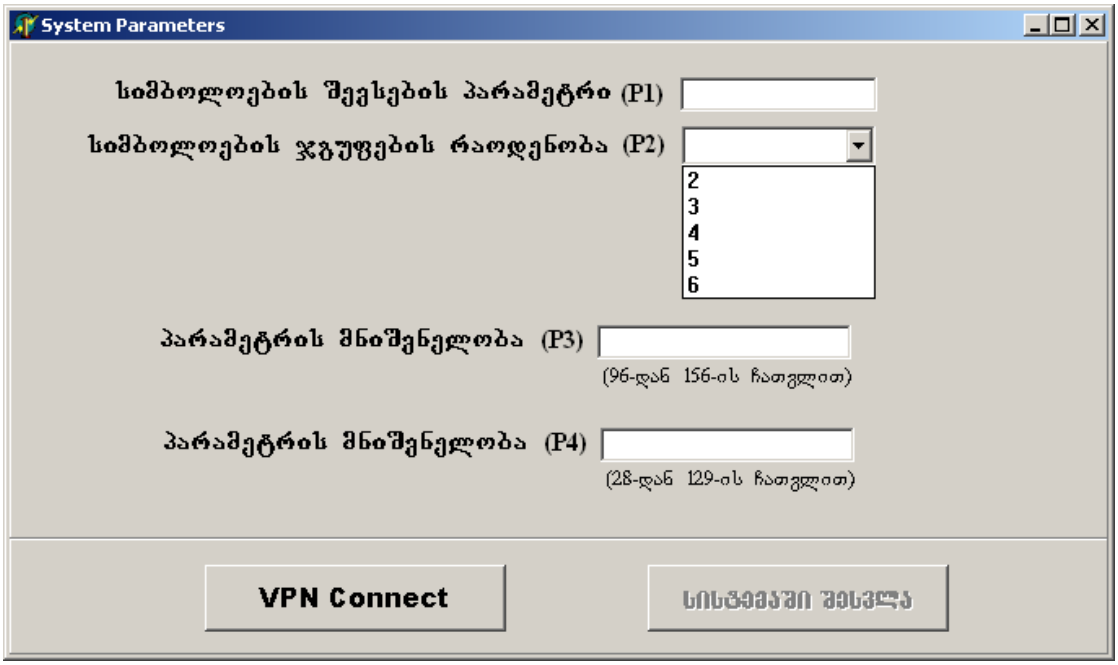
2.5. დიალოგური (ეკრანული) ფორმების შემუშავება

კორპორაციული ქსელების უსაფრთხოების მხარდამჭერ ავტომატიზებულ სისტემის შექმნის დროს დიდი მნიშვნელობა ენიჭება ეკრანული ფორმების შემუშავებას, ვინაიდან ნებისმიერი მომხმარებლისათვის ადვილი იყოს სისტემასთან მუშაობა.

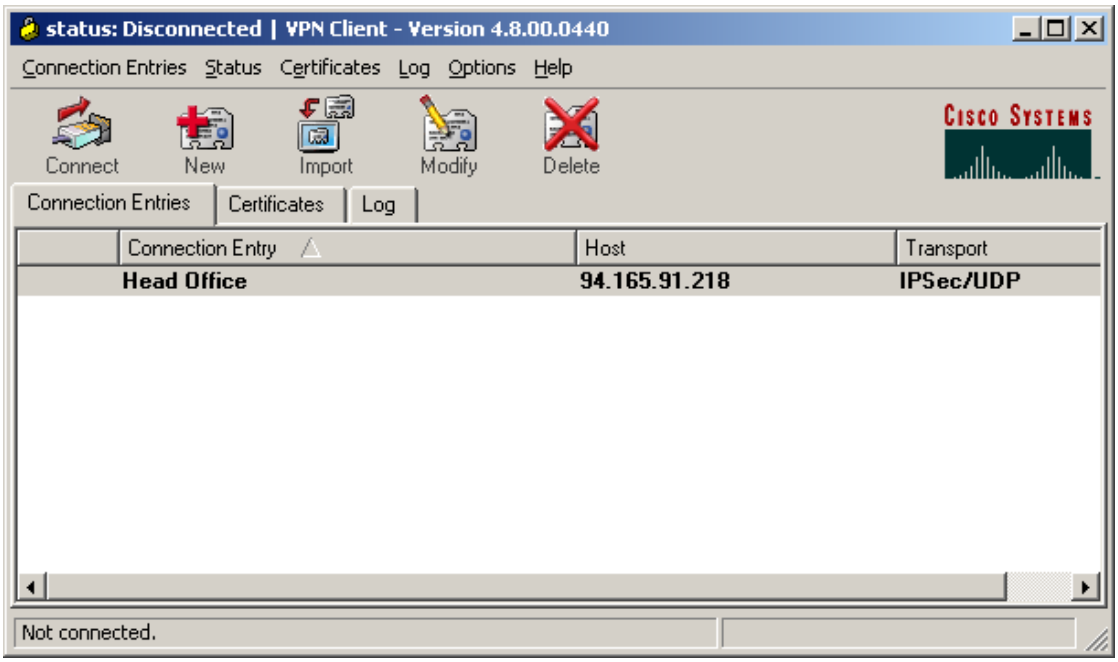
ეკრანული ფორმები განვიხილოთ და აღვწეროთ ცალკ-ცალკე.

თავდაპირველად სისტემის გაშვების შემდეგ გამოდის ძირითადი ფანჯარა, სადაც მომხმარებელს ეძლევა დააყენოს სისტემის პარამეტრები და აირჩიოს შესაბამისი ღილაკი (ნახ. 40).

პარამეტრების დაყენების შემდეგ საჭიროა ვირტუალური კერძო (დაცული) ქსელის (VPN) საშუალებით ცენტრალიზებულ ზედამხედველობის სისტემასთან კავშირის დამყარება. VPN Connect ღილაკის დაჭერის შემდეგ გამოდის სტანდარტული ფორმა (ნახ.41).

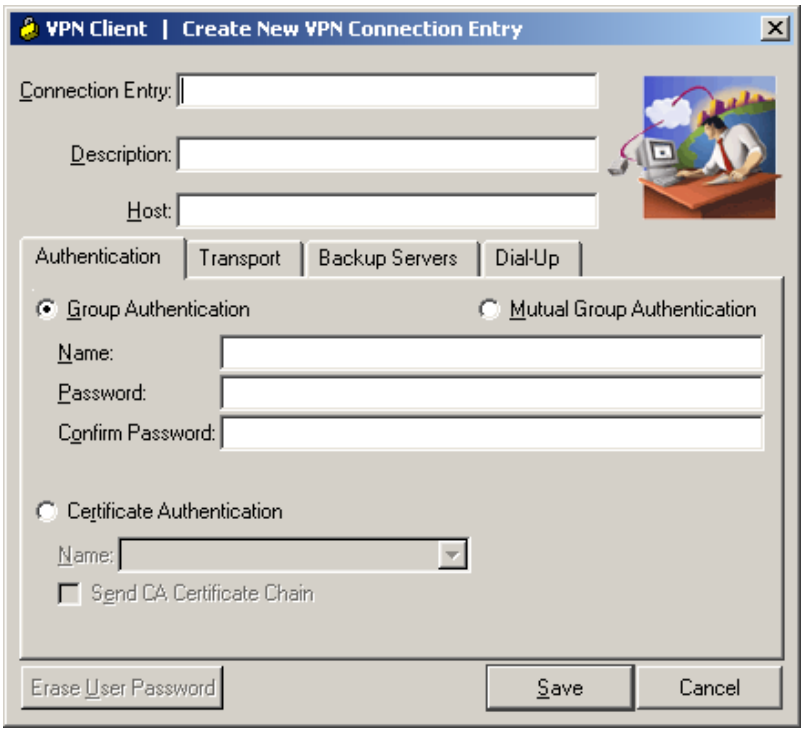


ნახ 40. სისტემის პარამეტრების ძირითადი ფორმა



ნახ 41. VPN-ის ძირითადი ფორმა

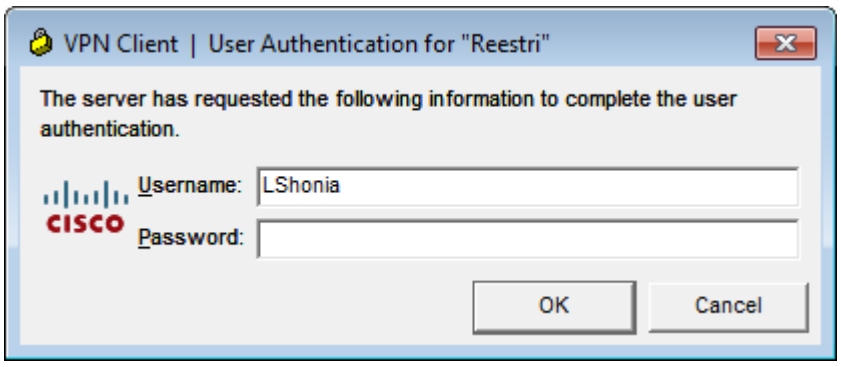
ფორმაზე მოცემული New-ზე როდესაც დავაჭერთ, გამოდის ახალი ფანჯარა, სადაც საშუალება გვეძლევა შეტანილი იქნას ადმინისტრატორის მიერ გადმოცემული მონაცემები (ნახ. 42).



ნახ 42. ახალი ჩანაწერის შექმნა

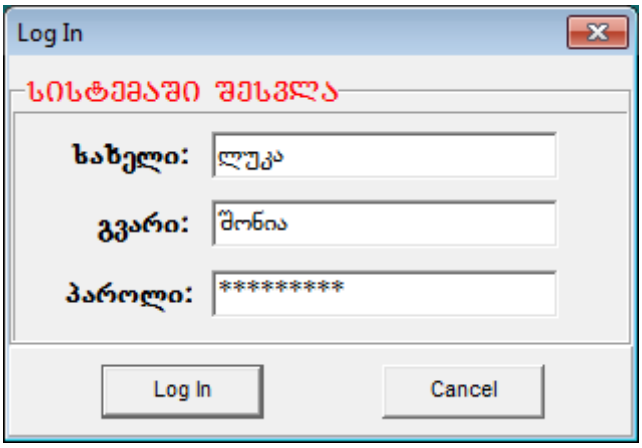
გამოსულ ფორმაში ხდება თითოეული მონაცემის შევსება და შეიქმნება ახალი ჩანაწერი.

იმისათვის რომ დავამყაროთ კავშირი ცენტრალურ სერვერთან, უნდა დავაჭიროთ ღილაკს Connect და გამოვა ფორმა, სად ხდება მომხმარებლის აუტენტიფიკაცია, რომელის დაშიფრული სახით გადაეცემა მთავარ სისტემას (ნახ. 43).



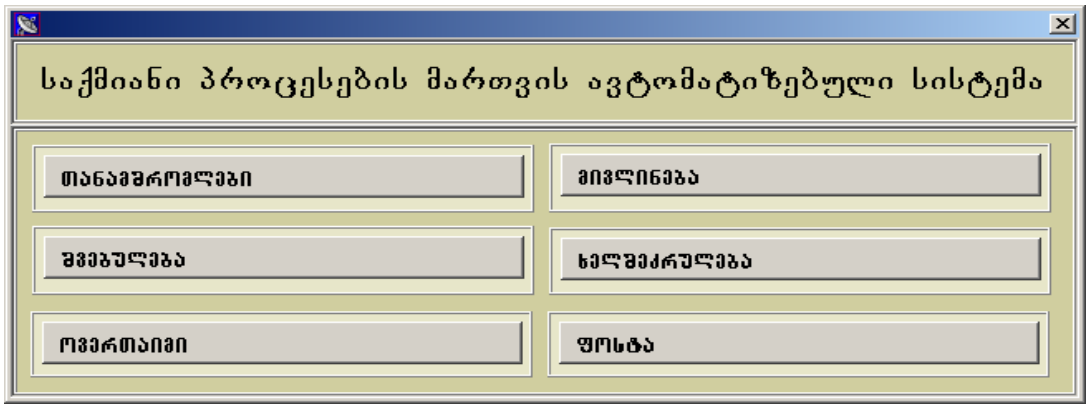
ნახ 43. აუტენტიფიკაციის ფორმა

აუტენტიფიკაციის წარმატებით დასრულების შემდეგ ხდება მთავარ ფორმაზე გადასვლა და იქაც საჭიროა შეტანილი იქნას მომხმარებლის პაროლი. შემდეგ ხდება დოკუმენტბრუნვის სისტემის მართვა, ობიექტებზე წვდომის გრაფიკების დამუშავება და ანალიზი, ერთიანი ინფორმაციული არქივის შექმნა და სტატისტიკური ანალიზი და სხვა (რა თქმა უნდა მომხმარებლების წვდომის დონეების მიხედვით) (ნახ 44).



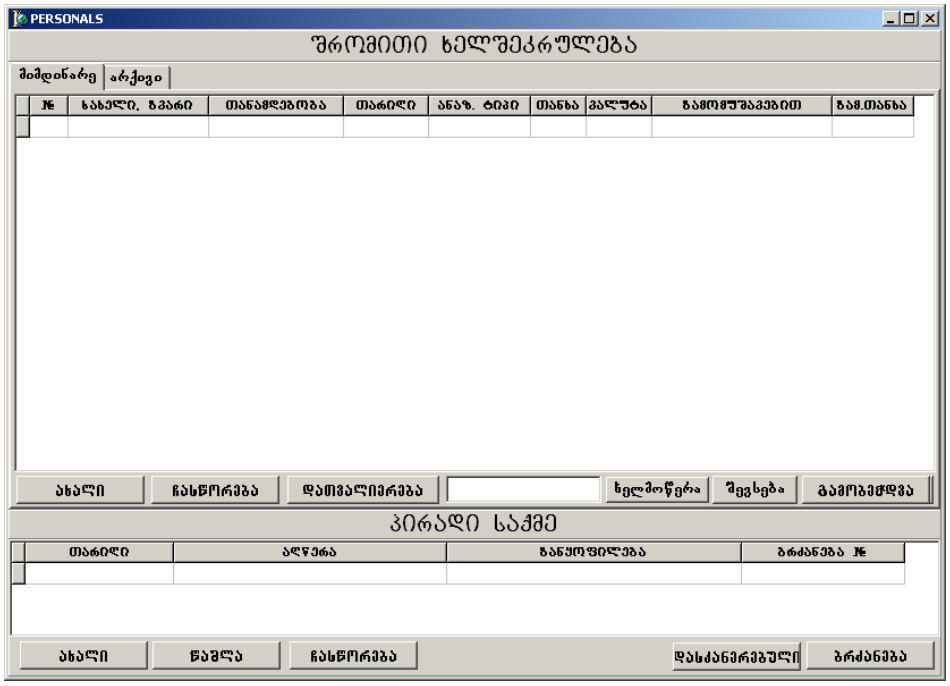
ნახ. 44. სისტემაში შესვლის ფანჯარა

შემდეგ გამოდის ძირითადი ფორმა, სადაც მომხმარებელს ეძლევა საშუალება აირჩიოს, თუ რომელ მოდულში სურს მუშაობა (ნახ. 45).



ნახ 45. მოდულების არჩევის ფორმა

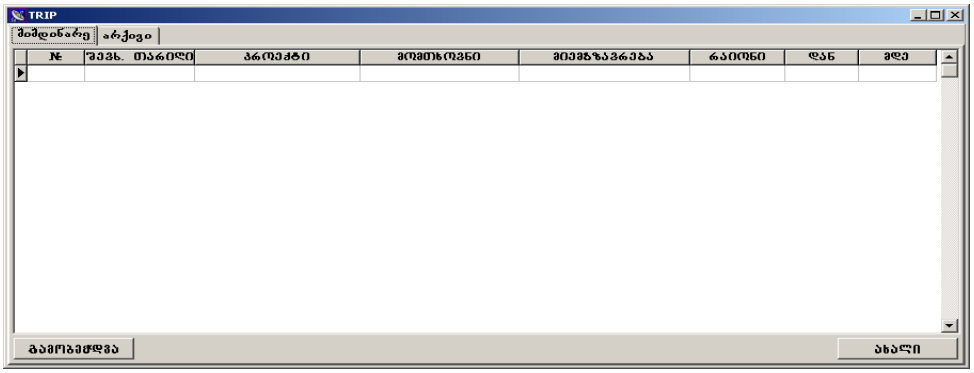
„თანამშრომლები“-ს მოდულის არჩევის შემდეგ გამოდის შემდეგი ფორმა (ნახ. 46)



ნახ 46. მომხმარებლების ფორმა

ამ ფორმაზე წვდომა აქვს მხოლოდ გარვეულ პირებს. ფორმაში საშუალება გვაქვს ვიხილოთ თანამშრომლების მიმდინარე და ასევე არქივში მოთავსებული შრომითი ხელშეკრულებები, ფორმაში არჩეულ კონკრეტულ თანამშრომელზე გამოდის მისი პირადი საქმე, სადაც მითითებულია თანამშრომლის მიღების თარიღი, განყოფილების დასახელება და ბრძანების ნომერი. ფორმასი ასევე შესაძლებელია ახალი ხელშკრულების დამატება, საჭიროების შემთხვევაში ხელშეკრულების გამობეჭდვა და სხვა.

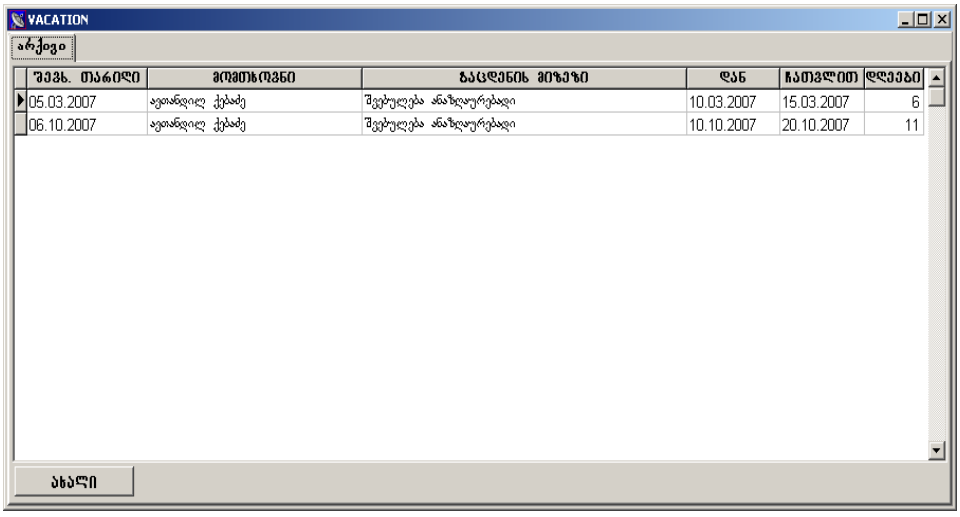
ძირითადი ფორმის „მივლინება“ ღილაკის დაჭერის შემდეგ გამოდის შემდეგი ფორმა (ნახ. 47).



ნახ 47. მივლინების ფორმა

ამ ფორმის საშუალებით მომსახურე პერსონალს შეუძლია შეავსოს მივლინების მოთხოვნა. აგრეთვე განყოფილების ხელმძღვანელს შეუძლია მისცეს დასტური ან უარყოს კონკრეტული მივლინების მოთხოვნა. თანამშრომლის მიმდინარე ფორმაში გვაქვს მივლინებების მიმდინარე და არქივის ფორმა, სადაც იწერება შევსების თარიღი, პროექტი, მომთხოვნი, გამგზავრების ადგილი და პერიოდი. აქვე შესაძლებელია ფორმის გამობეჭდვა ან ახლის შექმნა. მივლინების ფორმაში იწერება თანამშრომლის სახელი გვარი, რომელიც მიემგზავრება მივლინებით, ასევე მიეთითება, გამგზავრების ადგილი, პერიოდი, პროექტის დასახელება და გამგზავრების მიზანი და ა.შ..

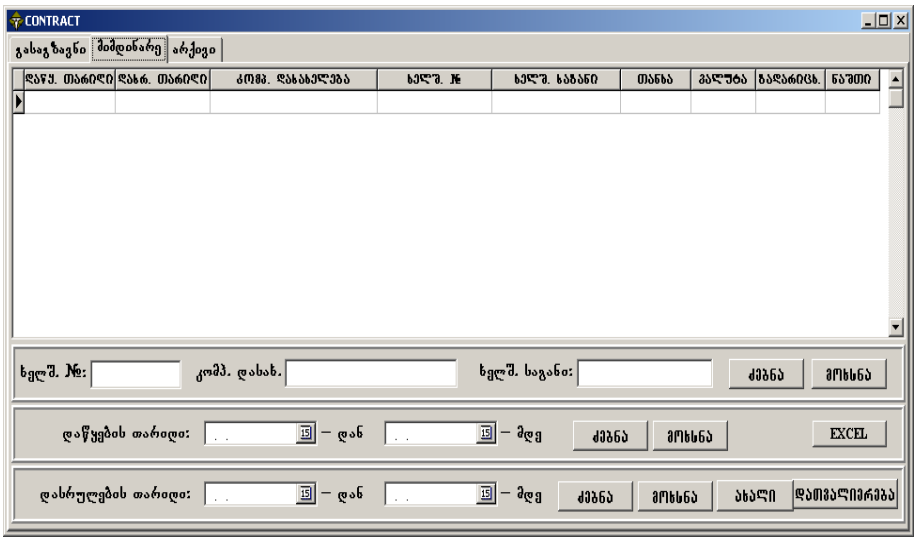
ძირითადი ფორმის „შვებულება“ ღილაკის დაჭერის შემდეგ გამოდის შემდეგი ფორმა (ნახ. 48).



ნახ 48. შვებულების ფორმა

აღნიშნულ ფორმაში მოცემულია არქივი სადაც, ნაჩვენებია შვებულების შევსების თარიღი, მომთხოვნი თანამშრომელი, გაცდენის მიზეზი, პერიოდი და გაცდენილი დღეების რაოდენობა. ხოლო ღილაკით „ახალი“ შესაძლებელია ახლის შექმნა. შვებულების ბაზაში ახალი ჩანაწერის ჩასამატებლად საჭიროა შეივსოს შესაბამისი ფორმა, სადაც მითითებულ უნდა იქნას პროექტის დასახელება, გაცდენის მიზეზი. ფორმაში ნაჩვენებია წლიური ლიმიტი და დარჩენილი დღეების რაოდენობა. დასრულებისას ღილაკით OK - შევსებული ფორმა ჩაემატება შვებულების ბაზაში, ხოლო ღილაკით Cancel ჩანაწერი გაუქმდება.

ძირითადი ფორმის „ხელშეკრულება“ ღილაკის დაჭერის შემდეგ გამოდის ადმინისტრაციული მენეჯერის ხელშეკრულების ფორმა (ნახ. 49).



ნახ 49. ხელშეკრულების ფორმა

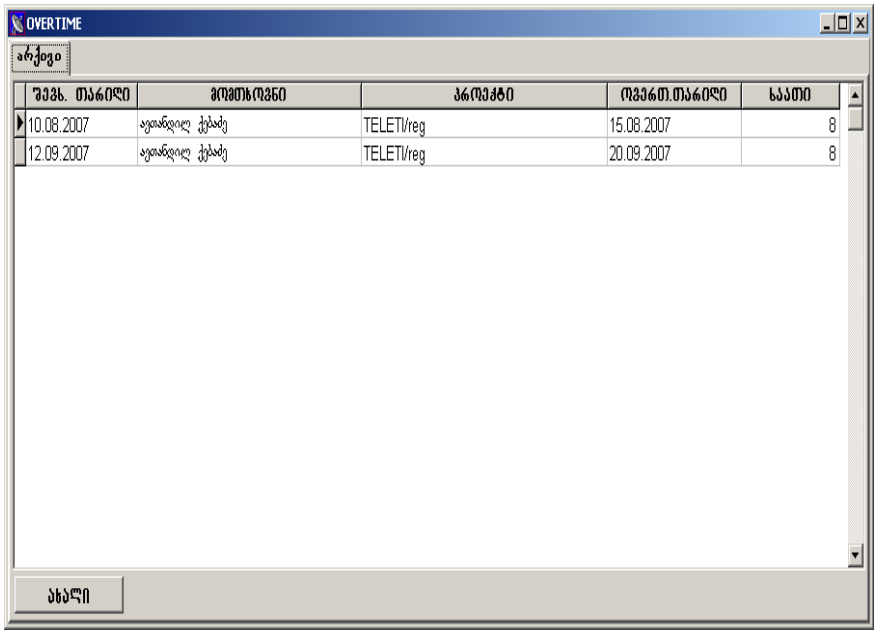
ადმინის ტრაციული მენეჯერის მიმდინარე ფორმაში ნაჩვენებია, ხელშეკრულებების რაოდენობა, თარიღების, კომპანიების, ხელშეკრულების ნომრების და თანხების მიხედვით, ჩანაწერებში მითითებული აქვს ასევე ვალუტა, გადარიცხვები და ნაშთი. ადმინის-ტრაციული მენეჯერს შეუძლია მოძებნა, ფილტრის მოხსნა და ახალი

ჩანაწერის შექმნა. „ახალი“ ღილაკის დაჭერის შემდეგ გამოდის ჩამატების ფორმა.

ახალი ხელშეკრულების ბაზაში ჩასამატებლად საჭიროა ფორმაში შეივსოს შესაბამისი ველები, ჩაიწეროს ხელშეკრულების ნომერი, დაწყების თარიღი, დასრულების თარიღი, კომპანიის დასახელება, ხელშეკრულების საგანი, თანხა, ვალუტა და საჭიროების შემთხვევაში გაუკეთდეს კომენტარი.. ხელშეკრულების ბაზაში ჩამატების შემდეგ ის ეგზავნება დირექტორს, რომლის ველშიც დეტალურად ჩანს ხელშეკრულების მონაცემები. დირექტორი განიხილავს მათ, რის შემდეგადაც აძლევს დასტურს ან უარყოფს, საჭიროების შემთხვევაში უკეთებს შესაბამის კომენტარს.

ძირითადი ფორმის „ოვერთაიმი“ ღილაკის დაჭერის შემდეგ გამოდის თანამშრომლის „ოვერთაიმის“ ფორმა (ნახ. 50).

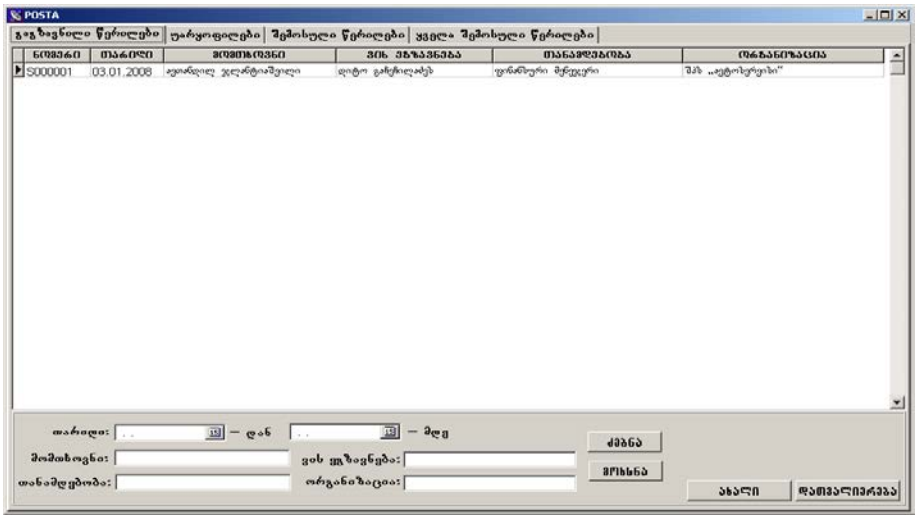
ფორმაში მოცემულია არქივი, რომელშიც წარმოდგენილია თანამშრომლის მიერ გამოყენებული ოვერთაიმები, შევსების თარიღის, მომთხოვნი თანამშრომლის სახელით და გვარით, პროექტის დასახელებით, ოვერთაიმის თარიღისა და საათის მითითებით, ასევე შესაძლებელია აქვე ახალი ოვერთაიმის შექმნა.



ნახ 50. „ოვერთაიმის“ ფორმა

ოვერთაიმის ბაზაში ჩასამატებლად საჭიროა მოცემულ ფორმაში ველების შევსება, სადაც უნდა მიეთითოს პროექტის დასახელება, ოვერთაიმის თარიღი, საათების რაოდენობა.

ძირითადი ფორმის „ფოსტა“ ღილაკის დაჭერის შემდეგ გამოდის შემდეგი ფორმა (ნახ. 51).



ნახ 51. შემოსული და გასული კორესპონდენციების ფორმა

გაგზავნილი წერილებში მოცემულია წერილის ნომერი, გაგზავნის თარიღი, მომთხოვნი, ადრესატის სახელი გვარი, განყ. უფროსს შეუძლია მოძებნოს კონკრეტული წერილი თარიღის, მომთხოვნის, თანამდებობობის ადრესატის ან ორგანიზაციის დასახელების მიხედვით, ასევე შეუძლია უარყოფილი, შემოსული წერილების და ყველა შემოსული წერილების დათვალიერება. შექმნილი ჩანაწერი გადაიგზავნება დირექტორთან, დირექტორის ფორმაში ნაჩვენებია წერილი ნომრისა და თარიღის მიხედვით, თუ ვის მიერ არის გაგზავნილი წერილი და მითითებულია ადრესატის თანამდებობა და ორგანიზაციის დასახელება. ამავე ფორმაში მითითებულია შემოსული წერილებიც. საბოლოოდ დირექტორს შეუძლია ეს წერილი გააგზავნოს თავის ხელმოწერით. ხელმოწერილი და დასკანერებული კორესპონდენციები (წერილები) ხვდება განყოფილების უფროსთან.

ადმინისტრაციული ასისტენტის ფორმაში შემოსულ წერილებში ჩანს ახალი წერილი, რომელსაც მითითებული აქვს წერილის ნომერი, თარიღი, გამომგზავნის სახელი გვარი, თანამდებობა, ორგანიზაციის დასახელება, ვის სახელზეა ეს წერილი და ასევე მოყვება დანართი თუ არა. ადმინისტრაციული ასისტენტი წერილის ნომრის მიხედვით ასკანერებს. აქვე შეუძლია შექმნას ახალი ჩანაწერი. ჩანაწერის შევსების შემდეგ წერილი გადაიგზავნება შესაბამის თანამშრომელთან.

თავი 3. კორპორაციულ საინფორმაციო სისტემებში ინფორმაციული ნაკადების შეფასების მოდელი და უსაფრთხოების სისტემის ექსპერიმენტული შემოწმება

3.1. კორპორაციული საინფორმაციო სისტემებში ინფორმაციული ნაკადების შეფასების მოდელი

ორგანიზაციის ხელმძღვანელების უმეტესობისთვის პრობლემას წარმოადგენს მართვის ინფორმატიზაციის ვიწრო ფუნქციური განხილვა, ამის მიზეზი ბევრია, მაგრამ ხშირად დომინირებს მაღალი დონის მენეჯერების გარკვეული ტექნოფობია. პერსონალური კომპიუტერი განიხილება არა როგორც იარაღი მმართველობითი შრომის ეექტურობის ამაღლებისა, არამედ, სამწუხაროდ, როგორც ნაწილი ინტერიერისა. უმეტეს შემთხვევაში ინფორმაციული მენეჯმენტით დაკავებულნი არიან მუშაკები ტექნიკურ თანამდებობებზე, რომლებიც ორგანიზაციას უგროვებენ მონაცემებს და აპროექტებენ შიდა კორპორაციულ ქსელებს. დრო და დრო ისინი ამზადებენ „დოსიეს“ ხელმძღვანელობისათვის ინფორმაციის განყოფილების სპეციალისტების თვალთახედვით. ასეთ მიდგომას ძალზე ძნელია ვუწოდოთ ინფორმატიზაცია, ვინაიდან მას არ გააჩნია არაფერი საერთო სისტემურ მიდგომასთან მომხმარებლების უზრუნველყოფისა მმართველობითი რელევანტური ინფორმაციით. მაღალპროდუქტიული ინფორმაიული სისტემები, როგორც წესი ძალიან ძვირადღირებული და ხელმიუწვდომელია საწარმოთა უმეტესობისათვის. და ბოლოს, საწარმოების უმეტესობის მთავარი პრობლემა - ესაა მენეჯმენტის ხარისხი და შესაბამისად დონე რელევენტური ინფორმაციული რესურსებით, ნაკეთობებით და პროდუქტებით უზრუნველყოფისა.

შესაბამისად აქტუალურია საწარმოების მართვის პრობლემა ინფორმაციისა და კომუნიკაციების საფუძველზე (ნახ.52).

ნახ. 52. კომპიუტერული ქსელი

უამრავი მეცნიერული შრომაა მიძღვნილი პრობლემებისადმი: მართვის სრულყოფა, ინფორმაციული უზრუნველყოფა, ინფორმაციული მენეჯმენტი, შექმნა და გამოყენება თანამედროვე მართვის სისტემების, ინფორმაციული მოღვაწეობის ეკონომიკური საკითხები. აღნიშნულ ნაშრომებში დაფიქსირებული მიდგომები ერთმანეთისგან განსხვავდება ამა თუ იმ ფაქტორების ჯგუფების გათვალისწინების სისრულის ხარისხით, რომლებიც გათვალისწინებულ უნდა იქნას საწარმოების მართვისას და რომელთა დახმარებითაც ფასდება გავლენა მათი მოღვაწეობის ეფექტურობაზე. ამ დროს არ არსებობს ერთიანი თეორიული მიდგომა საწარმოების, როგორც სოციალურ-ეკონომიკური სისტემების, ინფორმაციისა და კომუნიკაციის ბაზაზე. მართვის პრობლემების კვლევისადმი ართულებს მათ ანალიზს და იწვევს მომქმედი პრაქტიკული რეკომენდაციების არ არსებობას საწარმოების მართვის სრულყოფასთან დაკავშირებით.

შედეგები. მმართველობითი ინფორმაცია შემომავალი ნაკადის სახით გადაწყვეტილებების მომზადებისა და მიღებისათვის უნდა წარმოადგენდეს მრავლობით რიცხვს გარკვეულად მოწესრიგებული, გადამუშავებული და გაანალიზებული სასარგებლო ცნობებისა. იმისათვის, რომ ცნობებმა

მიიღონ მმართველობითი ინფორმაციის სტატუსი, მათ უნდა გაიარონ ანალიზურ-სინთეზური დამუშავება. ამ ცნობების მოცულობა განისაზღვრება მონაცემებიით სხვა და სხვა მხარეებზე, შედეგებსა და პირობებზე ობიექტის ფუნქციონირებისა, რომლებიც გამოიყენება მართვის სუბიექტის მიერ მმართველობითი გავლენის ორგანიზაციისათვის, ჩათვლით პარამეტრების მომზადებაზე, მიღებასა და რეალიზაციაზე, მმართველობითი გადაწყვეტილებების მიღებასა და მათზე დაფუძნებული მართვის აქტებზე.

მმართველობითი ინფორმაცია ტრანსფორმირებულ უნდა იქნას მმართველობით გადაწყვეტილებაში, ხოლო ეს უკანასკნელი - ხელმძღვანელობით გავლენაში. მმართველობითი ინფორმაცია შედგება არამარტო ცნობებისაგან ობიექტის მოღვაწეობის პარამეტრების შესახებ, ის მოიცავს ასევე განკარგულებების, რეკომენდაციებისა და მითითებების პარამეტრებს, რომლებსაც ღებულობს მართვის სუბიექტი ზემდგომი ორგანოების მხრიდან. უტყუარი ასპექტი წინასწარ განისაზღვრება პარამეტრებით წყაროების ცნობებიდან, რომლებიც ფორმალურად არ შედიან ამ მართვის სისტემაში. ამ დროს ინფორმაციის მოცულობა და ხარისხი წარმოადგენს უმნიშვნელოვანეს პირობას მმართველობითი გადაწყვეტილების მიღების პროცესის ეფექტურობისა.

ყველაფერი ეს წინასწარ განსაზღვრავს მოთხოვნილებას შესაბამისი საშუალებების მოძიებისა მმართველობითი გადაწყვეტილებათა მომზადების და მიღების პროცესში ინფორმაციის შეგროვების, დამუშავების, შენახვის და გაცემის ეფექტურობის ასამაღლებად.

თანამედროვე მმართველობითი გადაწყვეტილებების მხარდამჭერი ავტომატიზებული საინფორმაციო სისტემები მხარს უჭერენ მათ მიღებას დროის რისკის და განუსაზღვრელობის ფაქტორების მოქმედების პირობებში. ეს ხდება, როცა ფაქტორები ობიექტის შიდა და გარე გარემოში არაა ცნობილი, ან როდესაც მათი ფაქტიური მნიშვნელობადროის ვიწრო მონაკვეთში არაა გარკვეული, რაც დაკავშირებულია კავშირის არხების

გამტარუნარიანობასთან. იგივე შეიძლება ითქვას გადაწყვეტილებებზეც, რომელთა მიღებაც ხდება რისკის პირობებში, როდესაც სიტუაციის შეფასებისთვის გამოიყენება მახასიათებლებია, რომლებიც მიახლოებით ასახავენ ალბათობის ამა თუ იმ ხარისხს.

ემპირიულად გამოყვანილია აქსიომა, რომ მართვის სისტემებში ჭარბი ინფორმაცია არანაკლებ საზიანოა, ვიდრე მისი უკმარისობა. ჭარბი ინფორმაცია მიმოფანტავს ხელმძღვანელის ყურადღებას და ართულებს რელევანტური მონაცმების მიღებას. ხოლო მონაცემების არასაკმარისი შეპირისპირებისა და ანალიზის ანტროპია იცვლება პიროვნების სუბიექტური შეფასებებით. ამრიგად, მსვლელობაში მოდიან ევრისტიკული ფაქტორები. ასეთ შემთხვევაში გადაწყვეტილებების მიღება გადადის მართვის მეცნიერების სფეროდან მართვის ხელოვნების სფეროში.

ინფორმაციულ-ანალიზური უზრუნველყოფის ინფორმატიზაცია მოწოდებულია მოხსნას აღნიშნული პრობლემების სიმძლავრე, ინფორმაციული ნაკადების საჭირო გაჯერებულობის რეგულირებით. საამისოდ სოციალური მართვის სისტემაში იქმნება ისეთი კომპიუტერული ინფორმაციული სისტემები, რომლებიც წყვეტენ პრობლემას. ისინი ახდენენ ორგანიზაციულ-სამართლებრივი მექანიზმის ეფექტურობის ტრანსფორმაციას ინფორმაციული კავშირებისა და ურთიერთობების მოწესრიგებით, რომლებიც წარმოიშობიან, ხორციელდებიან და ქრებიან მართვის სუბიექტებსა და ობიექტებს შორის. მმართველობითი გადაწყვეტილების დამუშავების პროცესის ინფორმატიზაცია ახდენს ინფორმაციის დაგროვების, დამუშავების, შენახვისა და გადაცემის განსაზღვრული მეთოდების და საშუალებების გამოყენების პროცესების ოპტიმატიზაციას. მნიშვნელოვან ფაქტორს წარმოადგენს მონაცემების მიწოდების პროცესის ოპტიმატიზაცია მისი წარმომშობი წყაროებიდან კონკრეტული მართვის ორგანოების და რგოლებისთვის, რომლებიც იყენებენ მათ როგორც ინფორმაციას მათზე დაკისრებული მმართველობითი ამოცანების გადასაწყვეტად.

3.2. სიმბოლოების დაშიფვრის კომბინირებული მეთოდის ექსპერიმენტული შემოწმება

კომბინირებული დამუშავების მეთოდის ალგორითმის მოქმედება განვიხილოთ კონკრეტულ მაგალითზე. ვთქვათ, მომხმარებლის მიერ შეტანილი იქნა სიტყვა – „paroli“.

შემდეგ სიტყვაში სიმბოლოები იშლება და ცალკეული სიმბოლოსთვის ინდექსის განისაზღვრება, მიიღება სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, რაშიც ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$S_{\{1\}} = p; S_{\{2\}} = a; S_{\{3\}} = r; S_{\{4\}} = o; S_{\{5\}} = l; S_{\{6\}} = i. \quad (24)$$

აქედან გამომდინარე:

$$S_{\{i\}} F, L = (p; a; r; o; l; i) \quad (25)$$

თითოეული სიმბოლო განიხილება ASCII(decimal) კოდირებაში და მათთთვის განისაზღვრება კოდები, რის შედეგადაც მიიღება სიმბოლოების კოდების ერთობლიობისაგან შემდგარი რიცხვები. მათში ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსის კოდი:

$$\begin{aligned} S_{ASCII\{1\}} &= 112; \\ S_{ASCII\{2\}} &= 97; \\ S_{ASCII\{3\}} &= 114; \\ S_{ASCII\{4\}} &= 111; \\ S_{ASCII\{5\}} &= 108; \\ S_{ASCII\{6\}} &= 105. \end{aligned} \quad (26)$$

აქედან გამომდინარე:

$$S_{ASCII\{i\}} F, L = (112;97;114;111;108;105) \quad (27)$$

შემდეგ სიტყვა უნდა შევავსოთ დამატებითი სიმბოლოებით. ამისათვის შემოვიტანოთ აღნიშვნა (პარამეტრი) და მივანიჭოთ მნიშვნელობა _ $P_1=11$, რომელიც წარმოადგენს სიტყვის შევსების პარამეტრს ანუ რა რაოდენობისაგან უნდა შედგებოდეს სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით შედგენილი სიტყვა.

განვსაზღვროთ დამატებითი სიმბოლოების რაოდენობა _ n_2.

$$n_2 = 11 - 6 = 5 \qquad (28)$$

შემდგომ ცალკეული სიმბოლოს განსაზღვრული კოდისთვის განისაზღვრება მოდიფიცირებული კოდები. ბიჯების რაოდენობა ამ შემთხვევაში $m=1$.

$$D_{ASCII\{j\}}F, L = (111;95;111;107;103) \quad (29)$$

მიღებული ახალი მოდიფიცირებული კოდებით დგება დამატებითი სიმბოლოების ჯგუფი, რის შემდეგაც მიიღება დამატებითი სიმბოლოების ერთობლიობისაგან შემდგარი სიტყვა, მასში ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$D_{\{1\}} = o; D_{\{2\}} = \_; D_{\{3\}} = o; D_{\{4\}} = k; D_{\{5\}} = g \qquad (30)$$

აქედან გამომდინარე:

$$D_{\{j\}}F, L = (o; \_; o; k; g) \qquad (31)$$

მიღებული სიმბოლოებითა და დამატებითი სიმბოლოების გაერთიანებით იქმნება "გართულებული" სიტყვა (paroli), რომელსაც ემატება მიმდინარე თარიღისა და დროის რიცხობრივი მნიშვნელობები, ასევე, ცალკეული სიმბოლოსთვის განსაზღვრულია თავისი ინდექსი:

$$SD_{\{i\cup j\}}F, L = (p; a; r; o; l; i; o; \_; o; k; g; 0;5;0;6;1;2;1;5;0;5) \quad (32)$$

შემდეგ მიღებული სიტყვა იშლება (ჯგუფების შექმნა) სისტემაში დაყენებული პარამეტრის მიხედვით. ამისათვის შემოვიტანოთ აღნიშვნები და მივანიჭოთ მნიშვნელობა - $P_2=3$, რომელიც წარმოადგენს დასაშლელი

სიტყვის რაოდენობას ანუ რა რაოდენობით უნდა დაიშალოს მიღებული სიტყვა. დაშლილი სიტყვების რაოდენობა აღვნიშნოთ ℓ-ით და გამოვთვალოთ:

$$\ell = (6+5+10)div3 = 21 \;\; div \;\; 3 = 7 \qquad (33)$$

შედეგად მიიღება სიმბოლოების 3 ჯგუფი (ნაშთის დარჩენის შემთხვევაში, ნაშთი განსაზღვრავს ახალ ჯგუფს):

$$G_{\{1\}}F, L = (p; a; r; o; l; i; o) \quad \text{I ჯგუფი}$$
$$G_{\{2\}}F, L = (\_; o; k; g; 0; 5; 0) \quad \text{II ჯგუფი} \qquad (34)$$
$$G_{\{3\}}F, L = (6; 1; 2; 1; 5; 0; 5) \quad \text{III ჯგუფი}$$

შემდეგ თითოეული ჯგუფის სიმბოლოებისთვის ASCII(decimal) კოდირებაში ხდება მათი შესაბამისი კოდების განსაზღვრა:

$$G_{ASCII\{1\}}F, L = (112; 97; 114; 111; 108; 105; 111) \quad \text{I ჯგუფი}$$
$$G_{ASCII\{2\}}F, L = (95; 111; 107; 103; 48; 53; 48) \quad \text{II ჯგუფი} \qquad (35)$$
$$G_{ASCII\{3\}}F, L = (54; 49; 50; 49; 53; 48; 53) \quad \text{III ჯგუფი}$$

მიღებული კოდების რიცხობრივი მნიშვნელობა გარდაიქმნება სხვა რიცხობრივ მნიშვნელობად და მიიღება ახალი კოდების სიმრავლე. მიღებული სიმბოლოების კოდების გარდაქმნა ხდება შემდეგნაირად. აიღება სიტყვის პირველი სიმბოლოს კოდი, გადამოწმდება მისი მდებარეობის არეალი. თუ კოდი მდებარეობს 32-დან 99-ის ჩათვლით, მაშინ სიმბოლოს კოდს დაემატება პარამეტრის მნიშვნელობა, რომელიც დავუშვათ - $P_3 = 96$, ხოლო, თუ კოდი მდებარეობს 100-დან 126-ის ჩათვლით, მაშინ სიმბოლოს კოდს დაემატება პარამეტრის მნიშვნელობა, რომელიც დავუშვათ - $P_4 = 28$.

ჩვენი მაგალითის შემთხვევაში პირველი სიმბოლოა – „p“, მისი კოდია – 112. ვინაიდან ეს რიცხვი მდებარეობს 100-სა და 126 ინტერვალში, მაშინ:

$$P_{ASCII\{g\}}F,L = 112 + 28 = 140 \quad (36)$$

აქედან გამომდინარეობს, რომ პირველი სიმბოლოს კოდი 112 შეიცვალა 140-ით და, ანალოგიურად, ასევე, უნდა გაკეთდეს ყველა სიმბოლოსთვის. შედეგად მივიღებთ სპეციალური სიმბოლოების მოდიფიცირებული კოდებისაგან შემდგარ ერთობლიობის მასივს, რომელიც ფიქსირდება ჯგუფების მიხედვით:

$$G_{\{1\}}P_{ASCII\{g\}}F,L = (140;193;142;139;136;133;139) \quad \text{I ჯგუფი}$$
$$G_{\{1\}}P_{ASCII\{g\}}F,L = (191;139;135;131;144;149;144) \quad \text{II ჯგუფი} \quad (37)$$
$$G_{\{1\}}P_{ASCII\{g\}}F,L = (150;145;146;145;149;144;149) \quad \text{III ჯგუფი}$$

მიღებული ახალი მოდიფიცირებული კოდებით დგება სპეციალური სიმბოლოების ჯგუფი, რომელსაც აქვს შემდეგი სახე:

$$G_{\{1\}}P_{\{g\}}F,L = (Œ; Á; Ž; ‹; ˆ; ...; ‹) \quad \text{I ჯგუფი}$$
$$G_{\{2\}}P_{\{g\}}F,L = (¿; ‹; ‡; ƒ; □; •; □) \quad \text{II ჯგუფი} \quad (38)$$
$$G_{\{3\}}P_{\{g\}}F,L = (–; ‘; ’; ‘; ↄ; □; •) \quad \text{III ჯგუფი}$$

სპეციალური სიმბოლოებისაგან შემდგარი ჯგუფების გაერთიანებით მიიღება სპეციალური სიმბოლოების ერთობლიობისგან შემდგარი დაშიფრული ინფორმაცია:

$$W_{\{\ell\}}F,L = (Œ; Á; Ž; ‹; ˆ; ...; ‹; ¿; ‹; ‡; ƒ; □; •; □; –; ‘; ’; ‘; ↄ; □; •) \quad (39)$$

დაშიფრული ინფორმაცია ცენტრალურ სერვერს მიეწოდება ჯგუფების სახით. თუ პირველი ჯგუფის იდენტიფიკაცია წარმატებით დასრულდა, სერვერი ატყობინებს და ბრძანებას გამოსცემს მეორე ჯგუფის გამოშვებაზე და ა.შ. ჯგუფის ბოლომდე. თუ რომელიმე ჯგუფი არ დაემთხვა, სერვერი მაშინვე ბლოკავს აღნიშნულ მომხმარებელს. დაშიფრული ინფორმაციის ამოშიფვრა ცენტრალური სერვერის მიერ

ხდება ზემოთ განხილული მეთოდის უკუალგორითმის საშუალებით იმავე პარამეტრების გამოყენებით.

და, საბოლოოდ, რაც მთავარია, დაშიფვრისა და ამოშიფვრის გასაღები სისტემაში გამოყენებული სპეციალური პარამეტრების წყალობით არის უნიკალური ანუ მომხმარებლის ყოველი ავტორიზაციის დროს გასაღებები იცვლება და არასდროს არ განმეორდება.

დასკვნა

ამრიგად, უსაფრთხოების უზრუნველყოფის პრობლემისადმი კომპლექსური მიდგომა ეფუძნება კონკრეტული კორპორაციული სისტემებისთვის შემუშავებულ უსაფრთხოების პოლიტიკას. უსაფრთხოების პოლიტიკა ახდენს კორპორაციული სისტემების დაცვის საშუალებების მუშაობის ეფექტურობის რეგლამენტირებას. იგი მოიცავს ინფორმაციის დამუშავების ყველა თავისებურებას, განსაზღვრავს რა სისტემის ქცევას განსხვავებულ სიტუაციებში. ქსელის უსაფრთხოების საიმედო სისტემის შექმნა შეუძლებელია ქსელური უსაფრთხოების პოლიტიკის გარეშე.

ინფორმაციულ ურთიერთობებში სუბიექტების ინტერესების დასაცავად უნდა იყოს ერთმანეთთან შეხამებული შემდეგი დონის ზომები:

- საკანონმდებლო (სტანდარტები, კანონები, ნორმატიული აქტები და ა.შ.);

- ადმინისტრაციულ-ორგანიზაციული (საერთო ხასიათის მოქმედებები, რომლებსაც ახორციელებენ ორგანიზაციის ხელმძღვანელები და უსაფრთხოების კონკრეტული ზომები, რომლებიც დაკავშირებულია ადამიანებთან);

- პროგრამულ-ტექნიკური.

კორპორაციული სისტემის ყველა დონეზე დაცვის საშუალებების კომპლექსის გამოყენება საშუალებას იძლევა აიგოს ინფორმაციული უსაფრთხოების უზრუნველყოფის საიმედო სისტემა.

სადისერტაციო ნაშრომში განხილული კორპორაციული ქსელების უსაფრთხოების უზრუნველყოფის მეთოდებისა და საშუალებების კვლევის შედეგების ანალიზის საფუძველზე, შეიძლება გაკეთდეს შემდეგი დასკვნა:

1. წარმოდგენილია ძირითადი ცნობები კორპორაციული ქსელების ტექნოლოგიებისა და კომპონენტების შესახებ. მოკლედ განხილულია უსადენო ქსელების ყველა ნაირსახეობა, აღწერილია მათი სტრუქტურის თავისებურებები და გამოყენების მეთოდები.

2. მოყვანილია კორპორაციულ ქსელებთან დაკავშირებული უსაფრთხოების საკითხები და ჩატარებულია მათი ანალიზი. ჩამოყალიბებულია კორპორაციული ქსელების უსაფრთხოების პრობლემის აქტუალურობის საკითხები. წარმოდგენილია უსადენო ქსელების გამოყენებასთან დაკავშირებული საფრთხეების ყველაზე გავრცელებული ფორმები და თითოეული მათგანი დახასიათებულია თავისი თვისებებით.

3. წამოდგენილია სხვადასხვა კავშირგაბმულობის არხების გამო-
ყენების ტენდეციები უსაფრთხოების სისტემებში. მოყვანილია მსგავსი მეთოდები და მოდელები, თავისი დადებითი და უარყოფითი მხარეებით. დახასიათებულია უსაფრთხოების ავტომატიზებული სისტემის ძირითადი ამოცანები თავიანთი ფუნქციონალური დანიშნულებებით.

4. ნაშრომში დიდი ყურადღება ექცევა (VPN) აგების პრინციპებს, რომელიც უზრუნველყოფს დაცული ქსელის შექმნას. განხილულია VPN ქსელში უსაფრთხოების უზრუნველსაყოფად არსებული კრიპტოგრაფიული მეთოდები, მოყვანილია მათი დადებითი და უარყოფითი მხარეები და არსებული პრობლემებიდან გამომდინარე შემუშავებულია სიმბოლოების დაშიფვრის კომბინირებული მეთოდი.

5. დეტალურად განხილულია კორპორაციული ქსელის კომპონენტები და სისტემები, საფრთხეების აღმოსაფხვრელად შემოთავაზებულია ახალი მეთოდები, რაც უზრუნველყოფს უსაფრთხოების დონის ამაღლებას.

გამოყენებული ლიტერატურა

1. ხელნაწერი სიმბოლოების ანალიზი და შედარების პროცესების ფორმირება მინი-მაქსის პრინციპით. სტუ, არჩილ ელიაშვილის მართვის სისტემების ინსტიტუტი, შრომათა კრებული N 18, თბ. 2014. 244-246. ო. შონია, ი. ქართველიშვილი, ლ. შონია.
2. Algorithm of Combined Method for Symbol Encoding in Virtual Private Networks (VPN). Journal of Technical Science and Technologies, Internacional Black Sea University, ¹2, 2012. 15-20 O. Shonia, T. Kaishauri, I. Kartvelishvili, L. Shonia, Z. Beridze I. Didmanidze
3. ინფორმაციული სისტემის დაცვის უზრუნველყოფის ამოცანის დასმის ეფექტურობა. სტუ, შრომები "მართვის ავტომატიზებული სისტემები" ¹1(13) 2012. 77-81. ო. შონია, ლ. შონია.
4. ვირტუალურ კერძო ქსელებში (VPN) სიმბოლოების დაშიფრვის კომბინირებული მეთოდი. სტუ, შრომები "მართვის ავტომატიზებული სისტემები" ¹1(12) 2012. 121-125. ო. შონია, ი. ქართველიშვილი, ზ. ბერიძე, ლ. შონია.
5. Recognition of symbols using the method of gravity center. Nova science publishers Computer Tecnology and Applications 2017-3rd Quarter. 9 O. Shonia, J. Kartvelishvili, N. Chorkhauli, L. Shonia.
6. Algorithm of Combined Method for Symbol Encoding In Virtual Private Networks (VPN). Journal of Technical Science & Technologies. No.2 (Vol.1), 2012. 6. O. Shonia, T. Kaishauri, L. Shonia, Z. Beridze, I. Didmanidze.
7. ვირტუალური კერძო ქსელის (VPN) აგების კონცეფცია, ქსელის ფუნქციები და მათი კლასიფიკაცია., Georgian Technical University. AUTOMATED CONTROL SYSTEMS-2(26), 2018; 205. J. Kartvelishvili, L. Shonia.
8. Development of Software of Testing system generation of Examination Prangishvili A.I., Shonia O.B., Kartvelishvili I.SH., Shonia L.O., IX Московская международная конференция по исследованию операций (ORM2018) Москва, 22–27 октября 2018 ТРУДЫ.
9. უსადენო ქსელების უსაფრთხოების საკითხები და მათი ანალიზი. ოთარ შონია, იოსებ ქართველიშვილი, ლუკა შონია // SECURITY ISSUES OF WIRELESS NETWORKS AND THEIR ANALYSIS. Shonia Otar,

Kartvelishvili Ioseb, Shonia Luka. 109-113. საქართველოს ტექნიკური უნივერსიტეტი, შრომები 2020 1(30).

10. კორპორაციული სისტემების ინფორმაციული უსაფრთხოების უზრუნველყოფასთან დაკავშირებული რისკების ანალიზი. ოთარ შონია, იოსებ ქართველიშვილი, ლუკა შონია // ANALYSIS OF THE RISKS ASSOCIATED WITH ENSURING INFORMATION SEFURITY OF CORPORATE INFORMATION SYSTEMS. Shonia Otar, Kartvelishvili Ioseb, Shonia Luka. 113-118. საქართველოს ტექნიკური უნივერსიტეტი, შრომები 2020 1(30).
11. შონია ო., ქართველიშვილი ი., ნარეშელაშვილი გ. უსადენო ქსელების უსაფრთხოება. თბილისი, სტუ 2018. CD-3975.
12. გოგიჩაიშვილი გ., ოდიშარია კ,, შონია ო. ინფორმაციის დაცვა ავტომატიზებულ სისტემებში თბილისი სტუ 2008; 681.142/10.13.
13. შონია ო., შეროზია თ. ინფორმაციული ტექნოლოგიები და უსაფრთხოება თბილისი სტუ 2008 681.142/10.14.
14. შონია ო., თოფურია ნ., მაისურაძე გ. ინფორმაციის უსაფრთხოების სისტემის აგება, კორპორაცია Microsoft ტექნოლოგიის გამოყენებით თბილსი, სტუ 2009. 681.142(02)/136.
15. შონია ო., თოფურია ნ. „მონაცემთა დაცვის ლოკალური და ღრუბლოვანი სერვისები“, თბილისი, 2017. 004.056(02)/21.
16. სურგულაძე გ., პეტრიაშვილი ლ., ვიზუალური დაპროგრამება C# ენის ბაზაზე ინფორმაციული სისტემებისათვის. თბილისი, სტუ-ს „IT-კონსალტინგის სამეცნიერო ცენტრი”, 2019. ISBN 978-9941-8-1708-3.
17. სურგულაძე გ., გულუა დ., კახელი ბ. პროგრამული აპლიკაციების აგება ვირტუალიზაციის პირობებში. თბილისი, სტუ-ს „IT-კონსალტინგის სამეცნიერო ცენტრი”, 2019. ISBN 978-9941-8-0627-8.
18. George S. Oreku, Tamara Pazynyuk. Security in Wireless Sensor Networks, ISBN: 978-3-319-21268-5, U.S.A. 2016. CD-4125.
19. Tyler Wrightson. Wireless Network Security, ISBN: 978-0-07-176095-9, U.S.A. 2012. CD-4126.
20. Malcolm Harkins. Managing Risk and Information Security, ISBN: 978-1-4302-5114-9, U.S.A. 2013. CD-4123.
21. 11. Tajinder Kalsi. Practical Linux Security Cookbook. Packt Publishing, ISBN 978-1-78528-642-1, 2016. CD-4143.
22. 12. Joseph Migga Rizza. Computer Network Security. Springer, ISBN-13: 978-03872-0473-4, 2005. CD-4148.
23. 13. Martti Lehto, Pekka Neittaanmäki. Cyber Security: Analytics, Technology and Automation, ISBN: 978-3-319-18302-2, U.S.A. 2015. CD-4120.
24. 14. Ali Ismail Awad, Aboul Ella Hassanien, Kensuke Baba, Advances in Security of Information and Communication Networks, ISBN: 978-3-642-40597-6, U.S.A. 2013. CD-4117.
25. 15. Mark Rhodes-Ousley. Information Security, ISBN: 978-0-07-178436-8, U.S.A. 2013. CD-4141.

26. 16. Chuck Easttom, Computer Security Fundamentals, ISBN-10: 0-7897-4890-8, U.S.A. 2012. CD-4142.
27. 17. ElGamal T. A public-key cryptosystem and a signature scheme based on discrete logarithms. Advances in Cryptology: Proceedings of CRYPTO 84, Springer-Verlag, pp. 10-18, 1985.
28. 18. Menezes A., Van Oorschot P. and Vanstone S. Handbook of applied cryptography. CRS Press, 1996. © 1997.
29. 19. Баричев С. В. Криптография без секретов. –М.: Наука, 1998.
30. 20. Ростовцев А. Г., Михайлова Н. В. Методы криптоанализа классических шифров. –М.: Наука, 1995. –208 с.
31. 21. Ростовцев А. Г. Решеточный криптоанализ // Безопасность информационных технологий, 1997. Вып. 2. С. 53–55.
32. 22. Ростовцев А. Г. Метод обращения итерированной хэш-функции // Тезисы докладов конференции “Методы и технические средства обеспечения безопасности информации”. — СПб: Изд-во СПбГТУ, 2001.
33. 23. A. Mishra, Security and Quality of Service in Add Hoc Wireless Networks, Cambridge University Press, 2008.
34. 24. W. Stallings, Cryptography and Network Security Principles and Practices, Fourth Edition, Prentice Hall, Nov 2005.
35. 25. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, October 1996.
36. 26. L. Hu and D. Evans, “Using Directional Antennas to Prevent Wormhole Attacks,” Network and Distributed System Security Symposium, San Diego, CA, 5–6 Feb. 2004.
37. 27. Котенко И. В., Саенко И. Б., Полубелова О. В., Чечулин А. А. Применение технологии управления информацией и событиями безопасности для защиты информации в критически важных инфраструктурах // Тр. СПИИРАН. 2012.Вып. 1(20).С. 27-56.
38. 28. Kotenko I. And DoynikovaE. Security Assessment of Compiuter Networks based on Attack Graphs and Security Events //Proc.of the 2014 Asian Conf. On Availability, Reliability, and Security, LNCS, 2014. P.462-471.
39. 29. Poolsappasit N., Dewri R., Eay I. Dynamic Security Risk Management Using Bayesian Attack Graphs // IEEE Transactions on Dependable and Security Computing. 2012. Vol. 9. N1 P. 61-74.
40. 30. Федорченко А. В., Чечулин А. А., Котенко И. В. Исследование открытыж баз уязвимостей и оценка возможности их применения в системах анализа зашишенности компьютерных систем и сетей // Информациооно-управляющие состемы.2014. №5.С. 72-79.