საქართველოს ტექნიკური უნივერსიტეტი

ანზორი ბაბუნაშვილი

ჩაშენებული დაცვის სისტემების პროგრამული ტექნოლოგიები

წარმოდგენილია დოქტორის აკადემიური ხარისხის მოსაპოვებლად

სადოქტორო პროგრამა: „მართვის სისტემები, ავტომატიზაცია და ტესტ-ინჟინერინგი“

შიფრი 0403

საქართველოს ტექნიკური უნივერსიტეტი

თბილისი, 0175, საქართველო

2019 წ.

საქართველოს ტექნიკური უნივერსიტეტი

ინფორმატიკისა და მართვის სისტემების ფაკულტეტი

ჩვენ, ქვემორე ხელისმომწერნი ვადასტურებთ, რომ გავეცანით ანზორი ბაბუნაშვილის მიერ შესრულებულ სადისერტაციო ნაშრომს დასახელებით: “ჩაშენებული დაცვის სისტემების პროგრამული ტექნოლოგიები” და ვაძლევთ რეკომენდაციას საქართველოს ტექნიკური უნივერსიტეტის ინფორმატიკისა და მართვის სისტემების ფაკულტეტის საუნივერსიტეტო სადისერტაციო საბჭოში მის განხილვას დოქტორის აკადემიური ხარისხის მოსაპოვებლად.

- - - - - -, - - - - - - 2019 წელი

ხელმძღვანელი: პროფესორი ია მოსაშვილი

რეცენზენტი:

რეცენზენტი:

საქართველოს ტექნიკური უნივერსიტეტი
2019 წ

ავტორი: ანზორი ბაბუნაშვილი
დასახელება: ჩაშენებული დაცვის სისტემების პროგრამული
ტექნოლოგიები
სადოქტორო პროგრამა: მართვის სისტემები, ავტომატიზაცია და ტესტ-
ინჟინერინგი
ხარისხი: ინჟინერიის დოქტორი
სხდომა ჩატარდა:
- -

ავტორის ხელმოწერა

რეზიუმე

ორგანიზაციის, კომპანიის, ოფისის, სამრეწველო, საცხოვრებელ და სხვა ტიპის შენობა ნაგებობების დაცვის სისტემები არის ორგანიზაციის სტაბილური ფუნქციონირების გარანტი. სრული უსაფრთხოებისთვის დასაცავ ობიექტზე გამოიყენება კომპლექსური კონტროლის საშუალებები: სახანძრო და დაცვის სიგნალიზაცია, ვიდეო-აუდიო კონტროლი და წვდომის სისტემები.

ობიექტისადმი წაყენებული მოთხოვნები დაცვის თვალსაზრისით დამოკიდებულია მის კატეგორიაზე, არქიტექტურულ გადაწყვეტაზე, მუშაობის რეჟიმზე და მრავალ სხვა ფაქტორზე, რომელიც აუცილებლად უნდა იქნას გათვალისწინებული უსაფრთხოების სისტემის პროექტირებისას. თითოეული ჯგუფის ობიექტს უნდა შეესაბამებოდეს გარკვეული დაცვის კლასი და უსაფრთხოების უზრუნველყოფის ტექნიკური საშუალებები.

თანამედროვე უსაფრთხოების კომპლექსური სისტემები განიხილავს ობიექტის დაცვას ოთხი განუყოფელი ქვესისტემის მეშვეობით: დამცავი და საგანგაშო სიგნალიზაციის სისტემები, სახანძრო სიგნალიზაციის სისტემები, შესვლის ნებართვისა და წვდომის სისტემები და ტელე-ვიდეო თვალთვალისა და კონტროლის სისტემები, მათ შეიძლება დაემატოს სხვადასხვა დამხმარე მოწყობილობები.

სპეციალიზებული ციფრული მოწყობილობების შესაქმნელად უკვე დიდი ხანია იყენებენ მაღალტექნოლოგიურ ბაზას-პროგრამირებად ლოგიკურ ინტეგრალურ სქემებს, სპეციალიზებული კონტროლერების, კომუნიკაციის სისტემების, სიგნალების ციფრული დამუშავების სფეროში და ა.შ. განსაკუთრებით მათი გამოყენება აქტუალურია მაღალი მწარმოებლურობის ისეთი სქემების რეალიზებისას, რომლებიც ორიენტირებულნი არიან აპარატურულ რეალიზაციაზე. სხვადასხვა სახის ამოცანების აპარატურული რეალიზაცია უზრუნველყოფს პროცესის განპარალელებას და შესაბამისად ამაღლებს მწარმოებლურობას პროგრამულ გადაწყვეტასთან შედარებით.

დაცვის სისტემების შექმნისა და პროექტირებისათვის გამოვიყენე „გამჭოლი“ პროექტირების სისტემა „PROTEUS”-ი, რომელიც საშუალებას იძლევა რეალური მოწყობილობის აწყობის გარეშე დაალაგოს სქემის მუშაობა, მოძებნოს პროექტირების სტადიაზე დაშვებული შეცდომები, მოხსნას აუცილებელი მახასიათებლები და მრავალი სხვა. Proteus-ს აქვს კომპონენტების ძალიან ფართო ბიბლიოთეკა, მათ შორის პერიფერიული მოწყობილობებისთვისაც: შუქდიოდები და ინდიკატორები, ტემპერატურული გადამწოდები, რეალური დროის საათები, ასევე შეტანა-გამოტანის ინტერაქტიური ელემენტები: ღილაკები, გადამრთველები, ვირტუალური პორტები და გამზომი ხელსაწყოები, ხოლო მთელი რიგი მიკროკონტროლერების, კომპონენტებისა და მიკროსქემების დამატებით იგი გახდა უფრო ძლიერი და საშუალებას იძლევა მთლიანად შემოწმდეს

მიკროკონტროლერების ბაზაზე შექმნილი მოწყობილობები, აგრეთვე ამ სისტემის უპირატესობას წარმოადგენს მოქნილი სიმულაციური გარემო, კერძოდ მას შეუძლია რეალური სისტემების შექმნა, დიზაინერს კი შეუძლია შექმნას სწორი და ეფექტური დიზაინი მანამ, სანამ სისტემა რეალურად შეიქმნება. კონკრეტული დიზაინის შექმნის ფაზები და დრო ამცირებს სისტემის თვითღირებულებას. სისტემის უპირატესობაა აგრეთვე კომპონენტების განთავსებისა და შემაერთებელი ხაზების მარშრუტიზაციის სიმარტივე, მას აქვს შესაძლებლობა სხვადასხვა დონის აბსტრაქცია იქნას შესწავლილი და შეცდომის აღმოჩენის შემთხვევაში, მოხდეს მისი გასწორება ქვედა დონეზე, რაც გამოასწორებს საბოლოო შედეგს.

იგი წარმოადგენს არქიტექტურას, რომელშიც დამატებითი ანიმირებული მოდელები შეიძლება შეიქმნას ნებისმიერად, მათი ტიპების უმრავლესობა შეიძლება იყოს კოდირებისადმი მიმართვის გარეშე, შესაბამისად PROTEUS-ი საშუალებას აძლევს პროფესიონალ ინჟინრებს გაუშვან რეალური პროექტების ინტერაქტიური სიმულაცია, და ჯილდოდ მიიღონ შედეგი, რომელიც შეესაბამება სქემის სიმულაციას. თუ ესეც არ იქნება საკმარისი, შექმნილია მთელი რიგი პოპულარული მიკროკონტროლერების სიმულაციის მოდელები, რის შედეგადაც შესაძლებელია სრული მიკროკონტროლერების სისტემების სიმულირება და მათთვის პროგრამების შემუშავება მათი ფიზიკური პროტოტიპებისადმი მიმართვის გარეშე.

Proteus-ის საშუალებით გადავწყვიტე სიგნალიზაციის სქემის აწყობა, ამ სქემის ერთ-ერთი მთავარი მოწყობილობაა მიკროკონტროლერი, სქემის საიმედობისათვის და ფუნქციონალურად სრულყოფისათვის გადავწყვიტე შემერჩია მიკროკონტროლერი Arduino Mega 2560, კონკრეტული მიკროკონტროლერის საშუალებით სრულდება არა მარტო სიგნალიზაციის სქემები, არამედ ბევრი სხვა პროექტები, როგორიცაა „ჭკვიანი“ სახლი, ავტომატიზებული საქვაბე, სასათბურე მეურნეობები ნიადაგის მარილების შემადგენლობისა და ტენიანობის ავტომატური კონტროლით, მეტეოსადგურები და მრავალი სხვა.

ჩემს მიერ აწყობილი სქემა შეიძლება გამოყენებული იქნას, როგორც სახელმწიფო ობიექტებზე, ასევე კერძო შენობებისა და ფართების დაცვისათვის. სქემაში გამოყენებულია შესასვლელი ერთჯერადი პაროლი, თუმცა პროგრამულად შეიძლება მისი შეცვლაც, კარის გაღებისას სიგნალი აქტიურია 10 წამის განმავლობაში, შემსვლელი პირი სიგნალის განგაშის შესაჩერებლად კრებს 4 ციფრიან პაროლს, შესაძლებელია პაროლის შეცვლა, პაროლის შეცლის შემდეგ განგაშის შეჩერებას შევძლებთ მხოლოდ ახალი პაროლის აკრებით, თუ პაროლი შეყვანილია არასწორად, ეკრანზე მივიღებთ შეტყობინებას „კიდევ სცადეთ“.

ამრიგად შეგვიძლია ვთქვათ, რომ:

1. შემუშავებული სქემა წარმოადგენს სახელმწიფო ობიექტის სიგნალიზაციის ერთ-ერთ შესაძლო ვარიანტს, რომელიც წარმატებით უზრუნველყოფს სხვადასხვა ტიპის ობიექტების დაცვას.
2. იგი აწყობილია მიკროპროცესორულ ბლოკზე და წარმოადგენს მოქნილ

მოწყობილობას ფუნქციონალური ცვლილების თვალსაზრისით, მარტივია დასამზადებლად.
3. იაფია თვითღირებულებით, საიმედოა და აკმაყოფილებს თანამედროვე მოთხოვნებს, მისი მხოლოდ უმნიშვნელო ცვლილება უზრუნველყოფს აგრეთვე ერთდროულად რამდენიმე ობიექტის დაცვას, სისტემა საიმედოა შეუღწევლობის უზრუნველყოფით.
4. შესაძლებელია SMS შეტყობინებების გაგზავნა, მათი დამახსოვრება, ხასიათდება კვების მრავალსაათიანი ავტონომიურობით, მისი გამოყენება მცირე პროგრამული და აპარატურული ცვლილებებით შესაძლებელია საკმაოდ ფართო სპექტრის ობიექტებისათვის.

Abstract

Software technologies of the embedded security systems

Security systems of the organization, company, office, industrial, housing and other types of buildings are the guarantee of their stable functioning. Complex control facilities are used for the safety of the entire unit: fire and security alarms, video-audio control and access systems.

Demands of the object by means of security depends on its category, architectural solution, working mode and many other factors that should be taken into account when designing a security system. The object of each group should be in compliance with certain security class and technical means of security system.

Modern complex security systems consider the protection of the object through four integral subsystems: protective and alarm systems, fire alarm systems, entry permission and access systems, and TV-video surveillance and control systems, various helper devices can be added to them.

High-technological base - programmable, logical integration schemes, have long been used to create specialized digital devices in the sphere of specialized controllers, communication systems, digital processing of signals, etc. Their usage is particularly actual in the realization of schemes of high productivity that are oriented to hardware realization . The hardware realization of different tasks ensures the parallelization of the process and thus increases the productivity compared to the software solution.

I have used "penetrating" system of "PROTEUS" for creating and designing security systems, which allows to sort out the work of the scheme without building a real device, find the errors that have been made during designing, remove the necessary features and many more. Proteus has a wide range of components, including those for peripheral devices: LEDs and indicators, temperature sensors, real time clocks, as well as input-output interactive elements: buttons, switches, virtual ports and measuring devices, but by adding a range of microcontrollers, components and microschemes, it has become more powerful and it gives an opportunity to completely check the microcontroller-based devices. Also, the advantage of this system is a flexible simulation environment, in particular it can create real systems, and the designer can create the proper and effective design before the system is actually created. The phases and the time of creating a particular design reduces the system cost price. The advantage of the system is also the simplification of replacing the components and connecting lines' easy route, it has the ability to study the abstraction of different levels and if the error occurs it will detect and correct it at the lower level, which will rectify the final result.

It is an architecture in which any additional models can be created in any case, most of their types can be used without addressing to coding, accordingly PROTEUS allows professional engineers to start the interactive simulation of real projects and get the result as an award, which corresponds to the scheme simulation. If this is not enough, the simulation models of a number of popular

microcontrollers have been created, by mens of which it's possible to simulate the whole systems of microcontrollers and develop programs without addressing to their physical prototypes.

With the help of the Proteus I've decided to set up a scheme for signaling, one of the main devices of this scheme is the microcontroller, for the scheme reliability and its functional improvement I have chosen the microcontroller Arduino Mega 2560, with the help of this particular microcontroller not only signaling schemes but many other projects are managed, such as "smart" home, automated boiler, greenhouse industries with automatic control of soil moisture and salt composition, meteo stations and many more.

The scheme set up by me, can be used for the protection of state buildings, as well as private buildings and spaces. In the scheme, one time password is used to enter, but it can be changed with the help of the program, the signal is active for 10 seconds, while opening the door, the entrants are able to pick up a 4-digit password in order to stop the alarm. If the password is entered incorrectly, We'll get a message "try again" on the scream.

Thus, we may say that:

1. The designed scheme is one of the possible options of signaling on the state unit which successfully ensures the protection of different types of objects.
2. It is made on a microprocessor block and is a flexible device by means of function changing, its easy to make.
3. The cost is low, it's reliable and it satisfies modern requirements, the only minor change in it ensures the protection of several objects at the same time, the system is reliable by providing impenertability.
4. It's possible to send SMS messages, remember them, it is characterized by multi-hour feed authentication, it can be used for a wide range of objects with small software and hardware changes.

შ ი ნ ა ა რ ს ი

ნახაზების ნუსხა

შ ე ს ა ვ ა ლ ი

თემის აქტუალობა. თანამედროვე ცხოვრებაში სულ უფრო მეტი ადამიანი მიდის იმ დასკვნამდე, რომ მხოლოდ სახელმწიფო სამართალდამცავი ორგანოების ძალისხმევა არ არის საკმარისი ისეთი პრობლემის გადასაჭრელად, როგორიცაა სახელმწიფო ობიექტების დაცვა და მათი უსაფრთხოების უზრუნველყოფა.

ჩვენი ეპოქის დამახასიათებელი ნიშანია კრიმინოგენური სიტუაციის მკვეთრი გაუარესება, ძალიან ბევრი შემთხვევაა, როცა საიმედო, მაგრამ არასწორად დაყენებული ტექნიკური საშუალებები ვერ უზრუნველყოფენ საკუთრების დაცვას, ამიტომ სრული დაცვის ორგანიზებისათვის არ არის საკმარისი სამრეწველო ობიექტები გადავტვირთოთ რთული და ძვირადღირებული ელექტრონული საშუალებებით, ასევე აუცილებელია გარკვეული წესებისა და ზომების მიღება, რომელთა შესრულება სულაც არ არის რთული, თუმცა მათ არ შესრულებას მივყავართ მძიმე შედეგებამდე. ობიექტების დაცვის ამოცანის გადაწყვეტა დამყარებულია ისეთ ტექნიკურ საშუალებათა კომპლექსის გამოყენებაზე, რომლებმაც უნდა დააფიქსირონ სხვადასხვა საფრთხის მოახლოება ან დაწყება - ხანძრიდან და ავარიიდან დაწყებული და დამთავრებული ობიექტზე ან კომპიუტერულ ქსელში შეჭრით. ეფექტური დაცვის სისტემის პროექტირება პროგრამულ-აპარატურულ საშუალებათა გათვალისწინებით წარმოადგენს უძნელეს მრავალგანზომილებიან ამოცანას, რომელთა გადაჭრა შეუძლებელია სისტემის სტრუქტურის, ფუნქციონალური შესაძლებლობების და მუშაობის პრინციპების ღრმა შესწავლის გარეშე [31,32,33].

კვლევის საგანი და პრობლემატიკა. კვლევის საგანია სხვადასხვა ტიპისა და სახეობების ობიექტების დაცვის მეთოდებისა და საშუალებების შემუშავება, ხოლო პრობლემატიკაა:

- დასაცავი ობიექტების სახესხვაობების დადგენა;
- თანამედროვე ტექნიკური მოწყობილობების გამოყენებით

კომპიუტერულ სისტემებთან თავსებადი დაცვის სისტემების შემუშავება;

აღნიშნული საკითხების გადასაწყვეტად წარმოდგენილია დაცვის ობიექტის მათემატიკური მოდელი და მისი საშუალებით შევისწავლეთ პრობლემატური საკითხები.

კვლევის მიზანი და ამოცანები. კვლევის მიზანია თანამედროვე ტიპის, მაღალი სიზუსტისა და საიმედობის და სხვადასხვა ტიპის ობიექტებზე გათვლილი დაცვის სისტემის შექმნა, რომელიც მაქსიმალურად იქნება დაცული გარე პირების შეღწევისაგან. ამ მიზნის მისაღწევად გადასაწყვეტია შემდეგი ამოცანები:

- თანამედროვე დაცვის სისტემების შესწავლა;
- ობიექტების ტიპებისა და სახეობების მიხედვით დაცვის სისტემების შერჩევა;
- დაცვის სისტემების ფუნქციონირების შემოწმება ტესტირების მეთოდით;
- პროგნოზირებადი დაცვის სისტემების დამუშავება;

კვლევის მეთოდები. კვლევის მიზნის მისაღწევად გამოყენებულია იდენტიფიკაციისა და აუტენტიფიკაციის მეთოდები.

კვლევის ობიექტს წარმოადგენს სხვადასხვა ტიპისა და სახეობის ობიექტებზე გათვლილი სიგნალიზაციის სისტემა;

მეცნიერული სიახლე. ნაშრომში განხილულია თეორიული და ექსპერიმენტული გამოკვლევების ძირითადი შედეგები, მათ შორის:

1. შემუშავებული სქემა წარმოადგენს სახელმწიფო ობიექტის სიგნალიზაციის ერთ-ერთ შესაძლო ვარიანტს, რომელიც წარმატებით უზრუნველყოფს სხვადასხვა ტიპის ობიექტების დაცვას.

2. იგი აწყობილია მიკროპროცესორულ ბლოკზე და წარმოადგენს მოქნილ მოწყობილობას ფუნქციონალური ცვლილების თვალსაზრისით, მარტივია დასამზადებლად.

3. იაფია თვითღირებულებით, საიმედოა და აკმაყოფილებს თანამედროვე

მოთხოვნებს, მისი მხოლოდ უმნიშვნელო ცვლილება უზრუნველყოფს აგრეთვე ერთდროულად რამდენიმე ობიექტის დაცვას, სისტემა საიმედოა შეუღწევლობის უზრუნველყოფით.

4. შესაძლებელია SMS შეტყობინებების გაგზავნა, მათი დამახსოვრება, ხასიათდება კვების მრავალსაათიანი ავტონომიურობით, მისი გამოყენება მცირე პროგრამული და აპარატურული ცვლილებებით შესაძლებელია საკმაოდ ფართო სპექტრის ობიექტებისათვის.

დაცვაზე გამოტანილი დებულებები:

- დაცვის სისტემების არსებული მეთოდებისა და საშუალებების მიმოხილვა და ანალიზი.
- სამრეწველო ობიექტების დაცვის ვიდეო დაკვირვების სისტემები.
- დაცვის ინტელექტუალური სისტემის პარამეტრების მართვის სიმულაციური მოდელი.

სამუშაოს შედეგების დასაბუთება მიღწეულია თეორიული და ექსპერიმენტული კვლევითი შედეგების ანალიზით.

სამუშაოს პრაქტიკული ღირებულება მდგომარეობს შემდეგში: განხილული მეთოდები და საშუალებები იძლევა იმის შესაძლებლობებს, რომ შეიქმნას ისეთი სიგნალიზაციის სიტემა, რომელიც იქნება მაღალი საიმედობის, მოქნილი იმგვარად, რომ საჭიროების შემთხვევაში ადვილად მოხდეს მისი მოდიფიცირება, სისტემას ადვილად შეიძლება მიუერთდეს სხვადასხვა დამატებითი მოდულები, რაც ზრდის მის ფუნქციონალურ შესაძლებლობებს და იმის შანსს, რომ იგი ადვილად მოვარგოთ სხვადასხვა დაცვის სისტემებზე.

სამუშაოს აპრობაცია, სადისერტაციო ნაშრომის ძირითადი დებულებები წარმოდგენილი იყო სხვადასხვა ჟურნალებში და გამოცემებში, მათ შორის:

- პერიოდული სამეცნიერო ჟურნალი „ხანძთა“;
- საქართველოს ტექნიკური უნივერსიტეტის მართვის ავტომატიზებული სისტემების შრომები;

პუბლიკაციები. სადისერტაციო თემის ირგვლივ გამოქვეყნებულია ხუთი სამეცნიერო ნაშრომი.

სამუშაოს სტრუქტურა და მოცულობა. დისერტაცია შედგება შესავლის, სამი თავისა და ძირითადი დასკვნებისაგან, სამუშაო შეიცავს კომპიუტერზე ნაბეჭდ 102 გვერდს, ძირითად დასკვნებს, ოთხ ნახაზსა და და ლიტერატურის 38 ჩამონათვალს.

თავი 1. დაცვის სისტემების არსებული მეთოდებისა და საშუალებების მიმოხილვა და ანალიზი.

მატერიალური ქონების დაცვის მოთხოვნილება წარმოიშვა „კერძო საკუთრების“ ცნებასთან ერთად, ადამიანის მიერ თავისი ქონების დამალვის, მისთვის საიმედო სამალავის მოძებნა თითქმის ინსტიქტების დონეზეა, ამიტომ ასეთი ადგილის აღმოჩენისათვის წინააღმდეგობის გაწევის პირველი სტადია გახდა დამცავ-პრევენციული ზომების მიღება, ყველანაირი თხრილებისა და ქვების გორებისაგან, რომლითაც იფარებოდა განძის შესანახი ადგილების შესასვლელები, ევოლუციის პროცესში კაცობრიობა შეუფერხებლად გადავიდა დამხმარე ხელსაწყოების გამოყენებაზე, რათა:

ა) აღმოეჩინა ბოროტმოქმედი, რომელიც ცდილობდა არასანქცირებულად შეეღწია დაცულ ტერიტორიაზე;

ბ) სხვადასხვა სახის სიგნალების საშუალებით ეცნობებინა პატრონისა და დაცვის სამსახურისათვის, რომელიც პასუხისმგებელია ქონების მთლიანობაზე, ფაქტის შესახებ;

გ) აღეკვეთა შეღწევის მცდელობა და თუ შესაძლებელია ხელი შეეწყო ბოროტმოქმედის დაკავებისათვის[31,32];

პირველ ეტაპზე ასეთი „მოწყობილობის“ რანგში გამოიყენებოდნენ ძაღლები, რომლებსაც სპეციალურად წვრთნიდნენ იმგვარად, რომ სიგნალის მიღებისთანავე მაშინვე გაენეიტრალებინათ დამრღვევი, ამასთან დასაცავ ობიექტზე ძაღლის არსებობა ითვლებოდა საკმაოდ ქმედით პრევენციულ ზომად.

1853 წელს დაპატენტებული იქნა პირველი ელექტრული დაცვის სიგნალიზაცია ავგუსტ რასსელ პოუპის მიერ მასაჩუსეტის შტატში, მისი ბლოკი მუშაობდა ბატარეებზე და თითოეული კარისა და ფანჯრისასთვის საჭიროებდა ინდივიდუალურ ბლოკს. მაგრამ მხოლოდ მას შემდეგ რაც ედვინ ჰოლმსმა იყიდა მისი პატენტი, შესაძლებელი გახდა მისი გაყიდვაში გაშვება, მაგრამ მაინც თავიდან ხალხი სკეპტიკურად უყურებდა

ელექტროობის გამოყენებას სიგნალიზაციებში, ამიტომ ბიზნესი არ განვითარდა, მაგრამ როცა ჰოლმსმა ნოუ-იორკში შექმნა სიგნალიზაციათა ქსელი, რომელიც კონტროლდებოდა ცენტრალური სადგურიდან, ხალხი სერიოზულად დაინტერესდა ამ სიახლით. შემდეგ მან თავისი შვილი გაგზავნა ბოსტონში, იგივე მისიით, მაგრამ მან იმის მაგიერ, რომ შეექმნა დამოუკიდებელი საკაბელო სისტემა, მიუერთდა არსებულ სატელეფონო ხაზებს, ამით მან შექმნა სისტემა 700 აბონენტზე, რაც შემდგომში გაიმეორა მამამისმა ნიუ-იორკში და ამის შემდეგ სატელეფონო სისტემების განვითარების კვალდაკვალ ვითარდებოდა დაცვის სიგნალიზაციის სისტემები[31].

მატერიალური ფასეულობების დატაცების წინააღმდეგ ბრძოლისა და დაცვის ზომების კვლევამ საშუალება მოგვცა ჩამოგვეყალიბებინა ის ამოცანები, რომლებიც დგას მომხმარებლის წინაშე, როდესაც ის ქმნის დამცავი ზომების სისტემას თანამედროვე პირობებში. განვითარების მიხედვით, ადამიანები ცვლიან არასტაბულურ და არა ყოველთვის ეფექტურ ბიოლოგიური წარმოშობის ელემენტებს ტექნიკურად სრულყოფილ სისტემებზე, რომლებიც განუხრელად ვითარდებიან და უკეთესები ხდებიან. მექანიკური და ელექტრული მოწყობილობებიდან თანამედროვე სპეციალისტები მივიდნენ დაცვის აპარატურის მთლიან კომპლექსებამდე, რომლებიც თავის თავში აერთიანებენ ტექნიკის ამ ორ მიმართულებას.

1.1 დასაცავი ობიექტების კლასიფიკაცია

ობიექტისადმი წაყენებული მოთხოვნები დაცვის თვალსაზრისით დამოკიდებულია მის კატეგორიაზე, არქიტექტურულ გადაწყვეტაზე, მუშაობის რეჟიმზე და მრავალ სხვა ფაქტორზე, რომელიც აუცილებლად უნდა იქნას გათვალისწინებული უსაფრთხოების სისტემის პროექტირებისას [9,10,11].

დასაცავი ობიექტების კლასიფიცირება შეიძლება მოვახდინოთ შემდეგი ნიშნების მიხედვით:

1. ობიექტის ზომის მიხედვით, მის მიერ დაკავებული ფართობის მიხედვით:

ა) მცირე ობიექტები (100 კვ. მ-მდე) - ბინები, მცირე ოფისები, ცალკე განლაგებული სავაჭრო ჯიხურები, რომლებიც მოთავსებულია შენობების მიშენებებში, ყოფილ სამსახურეობრივ სათავსოებში.

ბ) საშუალო ობიექტები (100 კვ. მ-დან 500 კვ. მ-მდე) მსხვილგაბარიტიანი ბინები, კერძო სახლები მიშენებებით, ცალკე მდგომი ან ერთმანეთთან მიდგმული სხვა საწარმოო შენობებთან, ვალუტის გაცვლის მსხვილი პუნქტები, მცირე ზომის კომერციული ბანკები ან ავტოსადგომები 50-60 მანქანაზე და ა.შ.

გ) დიდი სტაციონარული ობიექტები (500 კვ. მ-დან 4000 კვ. მ-მდე- საწარმოები მუშათა რაოდენობით 300-დან 400 კაცამდე, პროდუქციის შესანახი ბაზები, საწყობები და ა.შ.

1. ობიექტის პერსონალის მუშაობის რეჟიმის მიხედვით:

ა) ობიექტები, რომელთა პერსონალი მუშაობს ერთ ცვლაში.

ბ) ორ ცვლაში მომუშავე ობიექტები.

გ) 24- საათიან რეჟიმში მომუშავე ობიექტები.

3. ობიექტის რაიონში განლაგების მიხედვით:

ა) ობიექტები, რომლებიც განლაგებულია ძირითადი სამრეწველო, საწარმოო და დასაცავი ზონის მიღმა.

ბ) ობიექტები, რომლებიც განლაგებულია ცალკე მდგომ შენობებში ან უკავიათ სხვა შენობის ნაწილი.

4. ობიექტის ტექნიკური გამაგრების მიხედვით[9,10]:

ა) ძალიან კარგად გამაგრებული ობიექტები, რომლებსაც პრაქტიკულად არა აქვთ სუსტი ადგილები;

ბ) კარგად გამაგრებული ობიექტები, რომლებსაც აქვთ სუსტი ადგილების გარკვეული რაოდენობა, მაგრამ ისინი ცნობილია დაცვის

სამსახურისათვის და აკონტროლებენ დაცვის თანამშრომლები.

გ) სუსტად გამაგრებული ობიექტები, რომლებსაც ბევრი სუსტი წერტილი აქვთ, რომელთა ნაწილს დაცვის სამსახური ვერ აკონტროლებს.

5. დაცვის ტიპის მიხედვით:

განსაკუთრებით მნიშვნელოვანი ობიექტი - ობიექტი, რომლის მნიშვნელობაც განისაზღვრება სახელმწიფო ხელისუფლების ან ადგილობრივი ორგანოებით, რათა განისაზღვროს სახელმწიფო ინტერესების დაცვის ზომები ბოროტმოქმედთა ხელყოფის ან ზარალის მიყენების შემთხვევაში, ასევე შემუშავდეს კომპლექსური ღონისძიებები საგანგაშო სიტუაციის დროს.

სასიცოცხლო ობიექტი - ცხოვრებისეულად მნიშვნელოვანი მატერიალურ, ფინანსურ საშუალებათა და მომსახურებათა ერთობლიობა, რომლების დაჯგუფებულია ფუნქციონალური დანიშნულებით და გამოიყენება მოსახლეობის სასიცოცხლოდ აუცილებელი მოთხოვნილებების დასაკმაყოფილებლად.

გაზრდილი საფრთხის ობიექტი - ეს არის ობიექტი, სადაც აწარმოებენ, გადაამუშავებენ, ინახავენ და გადააქვთ რადიოაქტიური, ფეთქებად და ცეცხლსაშიში, სახიფათო ქიმიური და ბიოლოგიური ნივთიერებები, რომლებიც ქმნიან საგანგაშო სიტუაციის შექმნის რეალურ საფრთხეს[11,12].

1.2 უსაფრთხოების კომპლექსური სისტემები და მათი ანალიზი

თითოეული ჯგუფის ობიექტს უნდა შეესაბამებოდეს გარკვეული დაცვის კლასი და უსაფრთხოების უზრუნველყოფის ტექნიკური საშუალებები, შემდგომი დამატებითი ანალიზის შედეგად დაპროექტდება დაცვის სისტემა რეკომენდირებული მოწყობილობების სახეობებით და ელემენტების კლასიფიკაციით[21,22,23,].

უსაფრთხოების კომპლექსური სისტემის სტრუქტურა განიხილავს ობიექტის დაცვას ოთხი განუყოფელი ქვესისტემის მეშვეობით: დამცავი და

საგანგაშო სიგნალიზაციის სისტემები, სახანძრო სიგნალიზაციის სისტემები, შესვლის ნებართვისა და წვდომის სისტემები და ტელე-ვიდეო თვალთვალისა და კონტროლის სისტემები, მათ შეიძლება დაემატოს სხვადასხვა დამხმარე მოწყობილობები, მაგალითად, კვების, განათების, შეტყობინების და სხვა, რომლებიც ხელს უწყობენ მთლიანი სისტემის ფუნქციონირებას.

თუ გავითვალისწინებთ დაცვის კომპლექსური სისტემის მუშაობისათვის მისი თითოეული ელემენტის მნიშვნელობას, შეიძლება გამოიყოს მოწყობილობათა სამი ჯგუფი, რომელთა გარეშეც შეუძლებელია სისტემის ფუნქციონირება: საფრთხეთა აღმომჩენი მოწყობილობები, ინფორმაციის შეკრებისა და გადამუშავების სისტემები და აგრეთვე ის საშუალებები, რომლებიც ასე თუ ისე დაკავშირებულნი არიან სისტემის მდგომარეობის შესახებ კავშირის არხებით ინფორმაციის გადაცემასთან.

განვიხილოთ ცოტა უფრო დაწვრილებით ამ სისტემების შემადგენლობა და თავისებურებები.

საფრთხეთა აღმომჩენი მოწყობილობები (სამ)- მისი ფუნქციონირების საფუძველს წარმოადგენს მგრძნობიარე ელემენტის ფიზიკური მოქმედების პრინციპი.

მგრძნობიარე ელემენტი-პირველადი გარდაქმნელია, რომელიც რეაგირებს მასზე პირდაპირი ან ირიბი ზემოქმედებისას და მიმღებია გარე სამყაროს მდგომარეობის ცვლილების.

აღმოჩენის საშუალებები-ეს მოწყობილობაა, რომლის დანიშნულებაა მოცემული პარამეტრების მქონე სიგნალების ავტომატური ფორმირება, რომელიც წარმოიქმნება ობიექტზე შეჭრის შედეგად ან მგრძნობიარე ზონის დარღვევის შედეგად.

დეტექტორი-მოწყობილობა, განგაშის შესახებ განაცხადების ფორმირების შესახებ ან განგაშის სიგნალის ინიცირების შემთხვევაში.

მართვის ინფორმაციის შეკრებისა და დამუშავების სისტემა (მიშდს)

ინფორმაცია სამ-დან მიეწოდება მიშდს-ს, ამოცანის სირთულის

მიხედვით, მისი რეალიზაცია შეიძლება იყოს სხვადასხვა. უმარტივეს შემთხვევაში ეს სისტემა შეიძლება წარმოადგენდეს რელეს, რომელიც ამოქმედდება სიგნალების შედეგად და მართავს ხმოვანი და სინათლის საშუალებებით. ზოგად შემთხვევაში კი მიშდს-ი წარმოადგენს აპარატურულ-პროგრამულ საშუალებათა ერთობლიობას, რომლის დანიშნულებაა სამ-დან მიწოდებული ინფორმაციის შეკრება, დამუშავება, რეგისტრაცია, გადაცემა და ოპერატორისათვის მიწოდება, დისტანციურად მართვადი მოწყობილობების სამართავად (ვიდეოკამერები, განათება) ასევე სხვა დისტანციურად მართვადი მოწყობილობებისათვის[21,22,23].

შეტყობინებების გადაცემის სისტემა (შგს)

ობიექტზე არასაშტატო სიტუაციის დროს აუცილებელი ვიზუალური და აკუსტიკური ინფორმაცია კავშირის არხებით გადაეცემა საავარიო სამსახურებს, ობიექტის მფლობელებს და ა.შ. არხების სახით და სამსახურეობრივი და საგანგაშო შეტყობინებების გადასაცემად იყენებენ სპეციალურ გატარებულ მავთულს.

ზოგად შემთხვევაში შეტყობინებების გადაცემის არხი ეს არის ერთდროულად მოქმედი მოწყობილობებისა და კავშირის ტექნიკურ საშუალებათა ერთობლიობა, რომლებიც უზრუნველყოფენ ინფორმაციის გადაცემას მიმდევრობით ჯაჭვში: დამაბოლოებელი მოწყობილობა-კავშირის არხი-რეტრანსლიატორი-კავშირის არხი-ცენტრალიზებული დაკვირვების არხი.

შეტყობინების ინსტრუმენტები (ში)

განგაშის შეტყობინების ინსტრუმენტები-ტექნიკური საშუალებებია, რომელთა დანიშნულებაა შუქით ან ხმოვანი შეტყობინებით მოსახლეობისათვის საფრთხის წარმოქმნის შესახებ, ამ მხრივ გავრცელებულ საშუალებებს მიეკუთვნება განგაშის საყვირი, ზარი, მკვეთრი ნათება, სააბონენტო სატელეფონო კავშირი, რადიოკავშირი, ტელეფაქსები, მობილური ტელეფონები, პეიჯერები და ა.შ.

შეტყობინებათა საშუალებების კომპლექსი აყალიბებს

შეტყობინებათა სისტემას, რომელიც კავშირის სისტემასთან ერთად წყვეტს ოპერატიული მართვისა და პერსონალის მოქმედებათა კოორდინაციის ამოცანებს საშიშროების შემთხვევაში.

კავშირისა და შეტყობინების სისტემები ასრულებენ შემდეგ ფუნქციებს;

- ობიექტის მდგომარეობის შესახებ სწორი ინფორმაციის შეუზღუდავი გადაცემა დაცვის სამსახურებისათვის, საკონტროლო ზონების შესახებ არასაშტატო სიტუაციების ან საფრთხის დროს;
- საავარიო სიტუაციის შეტყობინება იმ პირთათვის, რომლების იმყოფებიან დაცულ ობიექტზე;
- გარშემომყოფებისა და პოლიციის ყურადღების გამახვილება შეღწევის ან ქურდობის მცდელობისას, ხანძრის ან სხვა შემთხვევაში;
- განკარგულებათა დროული და ოპერატიული გაცემა პერსონალის მოქმედების შესახებ ობიექტზე მდგომარეობის შესახებ;

არასაშტატო სიტუაციების დროს ხალხის გადაადგილების კოორდინაცია და მართვა შეტყობინების სისტემით მიიღწევა ისეთი ქმედებებით, როგორიცაა:

- ❖ ევაკუაციის აუცილებლობის შესახებ სიტყვიერი ინფორმაციის გადაცემა და ამ მიზნით მოძრაობის მიმართულების მითითება;
- ❖ სპეციალური ტექსტების გადაცემა ხალხის დინამიკის მართვისათვის და მათი უსაფრთხოებისათვის;
- ❖ ევაკუაციის რეკომენდირებულ მიმართულებებზე ან ავარიულ გასასვლელებზე შუქის მაჩვენებლების ჩართვა [25,26];

საშიშროების უკუქმედებისა და ლიკვიდაციის საშუალებები (სულს)

ობიექტის უსაფრთხოების უზრუნველყოფისათვის უსაფრთხოების სამსახურის ძირითად ამოცანას წარმოადგენს მატერიალურ და სხვა ფასეულობათა დაცვა. ისინი იყოფიან ორ ჯგუფად:

- პასიურ, რომლებიც აფრთხილებენ პოტენციური ან წარმოქმნილი საშიშროების შესახებ;
- აქტიური, რომლებიც უშუალოდ ეწინააღმდეგებიან წარმოქმნილ

საშიშროებას, ხელს უშლიან მის შემდგომ განვითარებას; მათ შეიძლება მივაკუთვნოთ:

- ვენტილაციის, კვამლმოცილების და ცეცხლმაქრ საშუალებათა ავტომატიზებული საშუალებები, რომლებიც უზრუნველყოფენ სახანძრო დაცვის მოსვლამდე ხანძრის ლოკალიზებას ან ჩაქრობას;
- დამრღვევის მოქმედებათა ბლოკირების საშუალებები (შუქები ან რადიომიმღებები, მოწყობილობები, რომლებიც ბლოკავენ კარების ჩამკეტებს ან მანქანათა ამა თუ იმ მოწყობილობებს;
- ბოროტმოქმედზე ზემოქმედების საშუალებები (ცრემლსადენი გაზი და ა.შ.)

ობიექტის ეფექტური დაცვისათვის აუცილებელია, რომ მითითებული მოქმედებები ჩატარდეს ძალიან მოკლე ვადაში სპეციალური სამსახურების მოსვლამდე, რათა მინიმუმამდე იქნას დაყვანილი შესაძლო ზარალი.

1.3 ობიექტის დაცვის სისტემის აგების ზოგადი პრინციპები

განვიხილოთ ობიექტის დაცვის სისტემის აგების ზოგადი პრინციპები:

1. ობიექტზე მიღებული ადმინისტრაციული და ორგანიზაციული ზომები ადეკვატური უნდა იყოს შესაძლო საფრთხეების;
2. ზონალური აგება ანუ ზონალური პრინციპი. დაცვის სისტემა უნდა ითვალისწინებდეს შეზღუდული შეღწევისა და დაცული ზონის არსებობას, რომელიც უზრუნველყოფს „ეშელონისებურ“ დაცვას დასაცავ ობიექტზე.
3. თანაბრად დაცული უნდა იყოს დაცვის მოთხოვნილი დონე ყველა ტიპის დამრღვევისათვის;
4. დაცვის სისტემა არ უნდა ქმნიდეს წინააღმდეგობებს ობიექტის ფუნქციონირებისათვის და უნდა ადაპტირდეს მუშაობის ტექნოლოგიურ თავისებურებებთან, მათ შორის საგანგებო სიტუაციების დროს;

დაცვის სისტემის დანიშნულება და ტიპი დამოკიდებულია იმ

გადამწოდების ტიპზე, რომლებიც გამოყენებულია მოცემულ სისტემაში, გადამწოდები შეიძლება რეაგირებდნენ შემდეგ ქმედებებზე:

- წყლის გამოჟონვა;
- ტემპერატურის ცვლილება;
- ვიბრაციის, ხმაურისა და კვამლის წარმოქმნა;
- მოძრავი ობიექტის გამოჩენა;
- კარისა და ფანჯრის გაღება.

მაგრამ ყველა გადამწოდის წინაშე ერთი და იგივე ამოცანა დგას: დროულად გააგზავნოს სიგნალი მართვის ბლოკზე რაიმე ცვლილების აღმოჩენის შემთხვევაში, გარდა მოვლენების სახეობებისა ისინი განსხვავდებიან სიგნალის გადაცემის სახეობების მიხედვითაც: კაბელით და უკაბელოდ. კაბელურ დაცვით სისტემებში გადამწოდები და მართვის ბლოკები ერთმანეთს კაბელით უკავშირდება, ხოლო უკაბელო სისტემებში ისინი ერთმანეთს რადიოსიგნალებით უკავშირდებიან, თუმცა მისი ღირებულება ძალიან დიდია[1,3].

ინფორმაციაზე რეაგირების მიხედვით სისტემები იყოფიან ცენტრალიზებულ და ავტონომიურ სისტემებად. პირველები მიერთებულია ცენტრალური მართვის პულტთან, ხოლო მეორე შემთხვევაში გადამწოდის ამუშავებისას ჩაირთვება განგაში, რომელიც იპყრობს ხალხის ყურადღებას. მოცემულ რაიონში დაკვირვების პუნქტის არ არსებობის შემთხვევაში ან დაცვისათვის დიდი გადასახადის გადახდის გამო, შესაძლებელია ისეთი სისტემის დაყენება, როდესაც განგაშის სიგნალი მიეწოდება მობილური ტელეფონის დაფიქსირებულ ნომერზე.

ნებისმიერ დაცვის სისტემაში მიმდინარეობს ავტომატიზაციის პროცესი, როგორებიც შეიძლება იყოს შეღწევის მცდელობები, განგაშის შესახებ შეტყობინებები და ა.შ. და არსებობს სრულად ავტომატიზებული სისტემები, რომლებსაც ეწოდება ინტელექტუალური დაცვის სისტემები, რომლებსაც ძირითადად იყენებენ მოძრავი ობიექტების დაცვის უზრუნველყოფისათვის. მათ შესახებ შეიძლება ითქვას, რომ ისინი

აღიარებულნი არიან უნივერსალურ და საიმედო სისტემებად.

დაცვის სისტემების აგების პრინციპების დაცვა უზრუნველყოფს ობიექტების ეფექტურ დაცვას, ეწინააღმდეგება არასაშტატო სიტუაციებს და ხელს უწყობს საფრთხეების გამოვლენას სხვადასხვა დარღვევის მოდელების დროს.

დაცვის სისტემის ნორმალური ფუნქციონირებისათვის აუცილებელია რამდენიმე პირობის შესრულება;

1. არც ერთი ქვესისტემა არ უნდა უშლიდეს ხელს მთლიანი სისტემის ფუნქციონირებას;
2. ერთობლივად მოქმედი სისტემების ფუნქციები უნდა ავსებდეს ერთმანეთს და არ უნდა ახდენდნენ ხელისშემშლელ გავლენას თავიანთი შემადგენელი ნაწილების მუშაობისუნარიანობაზე.
3. ერთდროულად მოქმედ სისტემებში უზრუნველყოფილი უნდა იყოს ალგორითმული თავსებადობა და ყველა სამსახურეობრივი თუ საგანგაშო სიგნალების რეგისტრაცია.
4. ერთ-ერთი ქვესისტემის მწყობრიდან გამოსვლა არ უნდა იწვევდეს მთლიანი სისტემის მოშლას.
5. დაცვის სისტემა უნდა იმართებოდეს როგორც ცენტრალიზებულად, ასევე დეცენტრალიზებულად პერსონალის დონეების კონტროლის გათვალისწინებით.
6. დაცვის სისტემა უნდა ინარჩუნებდეს გამართულ მდგომარეობას გარე სამყაროს ფაქტორების ზემოქმედების შემდეგაც უნდა შეეძლოს მუშაობისუნარიანობის აღდგენა ამ ფაქტორების შეყვეტის შემდეგ.
7. დაცვის სისტემა არ უნდა გამოდიოდეს მწყობრიდან ობიექტზე ელექტროენერგიის გათიშვის შემთხვევაშიც და უნდა ინარჩუნებდეს მუშაობისუნარიანობას სხვა ძირითადი წყაროს დაზიანების დროსაც, არ უნდა იძლეოდეს მცდარ სიგნალებს ძირითადიდან სარეზერვო კვებაზე გადართვის მომენტში.
8. ყველა მოვლენა, რომელიც მოხდება სისტემაში უნდა ექვემდებარებოდეს

პროტოკოლირებას.

9. სისტემა უნდა აკონტროლებდეს, ტესტავდეს და იცავდეს თავის თავს მართვაში არასანქცირებული შეღწევის შემთხვევაში.
10. სისტემა არ უნდა უქმნიდეს საფრთხეს ობიექტის უსაფრთხოების უზრუნველყოფას[25,26,].

1.4 დაცვის ინტეგრირებული კომპლექსური სისტემები

დაცვის სიტემების აგების დროს არა საკმარისია მარტო ფუნქციონალურად დამოუკიდებელი ქვესისტემების შემქნა, არამედ აუცილებელია ინტეგრირებული კომპლექსური სისტემების გამოყენება.

ინტეგრირების მიზანს შეადგენს:

ა) მცდარი გადაწყვეტილებების მიღების რისკების შემცირება და ობიექტზე არასაშტატო სიტუაციის შექმნისას რეაქციის დროის შემცირება;

ბ) ახალი ფუნქციების მიღება, რომელთა მიზანია დაცვის სისტემების ქვესისტემების ოპერატიული ურთიერთკავშირის უზრუნველყოფა და ამასთან სისტემის შემადგენელი ნაწილების სრული მოცულობით შენარჩუნება;

გ) ამ ფუნქციების რეალიზებისათვის საშუალებათა ეკონომიკა;

დ) ობიექტის დაცვისათვის ყველა მიმართულებით მაქსიმალური ავტომატიზაციის დონე;

ერთი სისტემის ფარგლებში შესაძლებელია მოწყობილობათა ინტეგრაციის რამდენიმე იერარქიული საფეხური:

- **ინტეგრაცია საპროექტო დონეზე** -გულისხმობს საშუალებათა გაერთიანებას კონკრეტული სისტემისათვის პროექტირების ეტაპზე, ეს არის ინტეგრაციის ყველაზე დაბალი დონე, მისი გამოყენების ნაკლოვანებებია „ადამიანური ფაქტორი“, აპარატურათა სახესხვაობები, მომსახურების სირთულე, ავტომატიზაციის არარსებობა და ა.შ.
- **ინტეგრაცია აპარატურულ დონეზე**- გულისხმობს გაერთიანებას უპირატესად აპარატურული უზრუნველყოფის დახმარებით ყოველი სისტემისათვის მართვის კომპიუტერებისა და პროგრამული

უზრუნველყოფის გამოყენების გარეშე, ასეთი გაერთიანების კლასიკური მაგალითია სისტემების გაერთიანება სარელეო კონტაქტების დახმარებით. მისი უპირატესობაა გამოყენებული აპარატურის სიმარტივე და საიმედოობა, დაბალი ღირებულება და სხვადასხვა მწარმოებლების მიერ შექმნილი მოწყობილობების გაერთიანების შესაძლებლობა.

- **ინტეგრაცია პროგრამულ დონეზე-** (პროგრამულ-აპარატურულ დონეზე პროგრამული მარდაჭერის პრიორიტეტით)- გულისხმობს ერთიანი პროგრამული უზრუნველყოფის ქვეშ სხვადასხვა მწარმოებლების მიერ შექმნილი ქვესისტემების გაერთიანებას, ასეთი სისტემის აგება მიმდინარეობს ორი გზით: პირველი გზა მდგომარეობს სპეციალური პროგრამული უზრუნველყოფის გამოყენებაში, ხოლო მეორე ითვალისწინებს პროგრამული გარსის გამოყენებას ინტეგრირებადი პროგრამული მხარდაჭერის მაგიერ[25,26].
- **ინტეგრაცია პროგრამულ-აპარატურულ დონეზე-** გულისხმობს მაქსიმალური ხარისხის ურთიერთკავშირს სისტემის ყველა ელემენტს შორის, მიუხედავად იმისა, თუ რა ფუნქციები აკისრიათ მათ, რითაც მიიღწევა მუშაობის სიმარტივე და ხარჯების შემცირება სისტემის მონტაჟისა და აწყობის დროს.

ინტეგრირებული დაცვის სიტემები წარმოადგენენ მრავალფუნქციონალურ ნაკეთობას, ფუნქციონალური დანიშნულების მიხედვით ის შეიძლება დავყოთ:

- ✓ **უმაღლესი დონე**-გულისხმობს ინტეგრირებული და სხვა ინფორმაციული სისტემების ურთიერთკავშირს, ეს ერთგვარი „კლიენტ-სერვერის“ კომპიუტერული ქსელია ქსელური ოპერაციული სისტემის გამოყენებით, ეს დონე უზრუნველყოფს კავშირს სერვერსა და ოპერატორების მუშა სადგურებს შორის პროგრამული უზრუნველყოფის საშუალებით, მოითხოვება მაღალი საიმედობა და დაცვა არასანქცირებული წვდომისაგან.

- ✓ **პირველი დონე-** გულისხმობს გარკვეული ქვესისტემების ინფორმაციულ ურთიერთკავშირს, თითოეული ქვესისტემა ავტომატურად ასრულებს გარკვეულ მოქმედებას სხვა სისტემიდან მოსული სიგნალის ზემოქმედების შედეგად.
- ✓ **მეორე დონე** -წარმოადგენს ინფორმაციის შეკრებისა და გადაცემის ლოკალური სისტემების ინტეგრაციას, აქ შესაძლებელია ვერტიკალური (ინტეგრაციისა კონტროლერებსა და ქვესისტემების კომპიუტერებს შორის კავშირი) და ჰორიზონტალური (ერთი ტიპის კონტროლერებისა და თითოეული ქვესისტემის კავშირი) ინტერგრაციის კავშირი.

1.5 დამცავი დეტექტორები და მათი მოქმედების პრინციპები

დაცვის სისტემების თითოეულ ელემენტს აქვს განსაკუთრებული მნიშვნელობა სისტემის ფუნქციონირებისათვის, განვიხილოთ მათგან სამი უმთავრესი ჯგუფი, რომლებიც ითვლებიან ძირითადად:

- ❖ დაცვისა და განგაშის სისტემები (დგს)
- ❖ სახანძრო სიგნალიზაციის სისტემები (სსს)
- ❖ დაცვის სატელევიზიო სისტემები (დსს)

დაცვისა და განგაშის სისტემები შეიცავს შემდეგ ძირითად ელემენტებს:

- დეტექტორები
- საგანგაშო სიგნალიზაციის საშუალებები-ღილაკები, სატერფულები, დეტექტორები
- ინფორმაციის შეკრების, დამუშავების, წარმოდგენის და მართვის საშუალებები.

სახანძრო სიგნალიზაციის სისტემები შეიცავენ შემდეგ ძირითად ელემენტებს:

- სახანძრო დეტექტორები (სითბური, კვამლის, ალის, გაზის და ხელის);
- ინფორმაციის შეკრების, დამუშავების, წარმოდგენის და მართვის საშუალებები.

ობიექტის აღჭურვა სახანძრო სიგნალიზაციის ტექნიკური

საშუალებებით და ხანძარსაწინააღმდეგო დაცვის ინვენტარით მკაცრად უნდა რეგულირდებოდეს შესაბამისი ნორმატიული დოკუმენტებით, აგრეთვე დაიშვება ისეთი ტექნიკური საშუალებების გამოყენება, რომლებსაც გააჩნიათ სტანდარტებთან შესაბამისობის სერტიფიკატი, დაყენებული სისტემები უნდა უზრუნველყოფდეს სადღეღამისო განუწყვეტელ მუშაობას.

დგს და სსს აგების იდეოლოგიის მიხედვით ძალიან ახლოსაა ერთმანეთთან და მცირე ობიექტებზე, როგორც წესი შერწყმულია ერთმანეთთან ერთიანი კონტროლის ბლოკის ან საკონტროლო პანელის ბაზაზე, ამასთან რეალიზებულია დამცავ-სახანძრო სიგნალიზაცია, რომლის ძირითადი ამოცანაა დასაცავ ობიექტზე ხანძრის ან არასანქცირებული შეღწევის შედეგად მიღებული ინფორმაციის დამუშავება და გადაცემა, ეს ინფორმაცია მიეწოდება პერსონალს შემდგომი რეაგირებისათვის [30,31].

თითოეული ასეთი სისტემა შეიცავს დეტექტორებს, რომლებიც აკონტროლებენ გარე სამყაროს სხვადასხვა ფიზიკურ პარამეტრებს, საფრთხეების გამოვლენისა და სიგნალების ფორმირების მიხედვით დეტექტორები იყოფიან უმისამართო, მისამართიან და მისამართიან-ანალოგურ დეტექტორებად.

უმისამართო სისტემებში დეტექტორებს აქვთ მგრძნობელობის ფიქსირებული ზღვარი, თანაც დეტექტორების ჯგუფი ირთვება სისტემის საერთო შლეიფში, და ერთ-ერთ მათგანის ამოქმედებისას ყალიბდება განგაშის განზოგადებული სიგნალი.

მისამართიანი სისტემები განსხვავდებიან ინფორმაციის განაცხადში განმცხადებლის მისამართით, რაც საშუალებას იძლევა განისაზღვროს ხანძრის ზონა დეტექტორის განლაგების სიზუსტით.

მისამართიან-ანალოგური სისტემები არიან ყველაზე ინფორმატიული და განვითარებული, მათში გამოიყენება „ინტელექტუალური“ დეტექტორები, რომლებიც გადასცემენ კონტროლირებადი პარამეტრის მიმდინარე მნიშვნელობას შლეიფში მათ

მისამართთან ერთად. მონიტორინგის ასეთი მეთოდი გამოიყენება საგანგაშო სიტუაციების ადრეული აღმოჩენისათვის, გარდა ამისა ეს სისტემები საშუალებას იძლევიან სისტემის მუშაობის შეუწყვეტლივ ცვალონ დეტექტორების ფიქსირებული მგრძნობელობის ზღვარი პროგრამულ დონეზე და შეუსაბამონ ისინი ობიექტის ექსპლოატაციის პირობებს.

დეტექტორების თითოეულ ტიპს აქვს ძირითადი მახასიათებლების თავისი ჩამონათვალი, რომელიც შეესაბამებიან სტანდარტებს. ამავე დროს ერთი და იმავე ტიპის დეტექტორებსაც კი აქვთ კონსტრუქციული განსხვავებები ძირითად ნაწილებში, საიმედობაში, დიზაინში, რაც თქმა უნდა მიიღება მხედველობაში ამა თუ იმ ფირმის ან მწარმოებლის მიერ შექმნილი დეტექტორების ამორჩევისას.

ობიექტზე შეღწევის ან ხანძრის შემთხვევაში ინფორმაციული სიგნალების ჩამოყალიბების პრინციპის მიხედვით დეტექტორები იყოფა ორ ჯგუფად:

- **აქტიური,** რომლებიც ახდენენ დასაცავ ზონაში სიგნალის გენერირებას და რეაგირებენ მისი პარამეტრების ცვლილებაზე;
- **პასიური,** რომლებიც რეაგირებენ გარემომცველი სამყაროს პარამეტრების ცვლილებაზე, რაც გამოწვეულია ხანძრის ან სხვა პირის შეღწევით;

გამოყენების სფეროს მიხედვით დეტექტორები იყოფა დამცავ, სახანძრო-დამცავ და სახანძრო დეტექტორებად.

დამცავი დეტექტორები კლასიფიცირდებიან ფუნქციონალური დანიშნულების შემდეგი ნიშნების მიხედვით:

1. მათი მოქმედებაში მოყვანის მეთოდის მიხედვით- ავტომატურ და ხელის დეტექტორებად;

2. ექსპლოატაციის პირობების მიხედვით-გამთბარ შენობებში დასაყენებელი, გაუთბობელ შენობებში დასაყენებელი, ღია ობიექტებზე და მოედნებზე დასაყენებელი;

3. ავტომატური დეტექტორის მიერ კონტროლირებადი ზონის მიხედვით:
   — წერტილოვანი დეტექტორი-აკონტროლებს ობიექტზე შეღწევას დაყენების წერტილში;
   — ხაზოვანი დეტექტორი-აკონტროლებს წრფის ან მრუდის გასწვრივ ტერიტორიას;
   — ზედაპირული დეტექტორი-აკონტროლებს ზონას სამი განზომილების მიხედვით: სიგრძე, სიგანე და სიღრმე;
4. ფიზიკური პრინციპების მიხედვით, რომლებიც შეადგენს აღმოჩენის საფუძველს: მექანიკური (ელექტროკონტაქტური, მაგნიტოკონტაქტური, დარტყმით-კონტაქტური), ელექტრომაგნიტური უკონტაქტო, პიეზოელექტრული, ტევადური, აკუსტიკური (ინფრაბგერითი, ულტრაბგერითი, ბგერითი), ვიბრაციული, ოპტიკურ-ელექტრონული (აქტიური, პასიური, რადიოტალღური, ელექტროსტატიკური, რადიოსხივური (მიკროტალღური), კომბინირებული [30].
5. დეტექტორების მიერ აღმოსაჩენი ზონების რაოდენობის მიხედვით-ერთზონიანი და მრავალზონიანი.
6. მოქმედების სიშორის მიხედვით-ულტრაბგერითი, ოპტიკურ-ელექტრონული და რადიოსხივური, დახურული შენობებისათვის განიხილავენ:
   - მცირე მანძილზე მოქმედების-12 მ-მდე;
   - საშუალო მანძილზე მოქმედების-12 მ-დან 30 მ-მდე;
   - დიდ მანძილზე მოქმედების-30 მ -ის ზევით (გარდა ულტრაბგერითებისა);

   7. მოქმედების სიშორის მიხედვით არსებობენ ოპტიკურ-ელექტრონული და რადიოსხივური დეტექტორები, ღია მოედნებისა და პერიმეტრებისათვის ისინი იყოფა:
   - მცირე მანძილზე მოქმედების -50 მ-მდე;
   - საშუალო მანძილზე მოქმედების-50-მ-დან 200 მ-მდე;
   - დიდ მანძილზე მოქმედების-200 მ-ზე ზევით;

8. კონსტრუქტორული შესრულების მიხედვით ულტრაბგერითი, ოპტიკურ-ელექტრონული და რადიოსხივური დეტექტორები იყოფიან:
   - ✓ ერთპოზიციური -ერთი ან მეტი გადამცემი და მიმღები შეთავსებულია ერთ ბლოკში;
   - ✓ ორპოზიციური - გადამცემი და მიმღები შესრულებულია ცალკეული ბლოკების სახით;
   - ✓ მრავალპოზიციური- ორზე მეტი ბლოკი (ერთი გადამცემი, ორი ან მეტი მიმღები; ერთი მიმღები, ორი ან მეტი გადამცემი)
9. კვების წყაროს ხასიათის მიხედვით:
   - ❖ დენის არ მომხმარებელი;
   - ❖ სიგნალიზაციის შლეიფიდან მკვებავი;
   - ❖ კვების გარე ავტონომიური წყაროდან მკვებავი;
   - ❖ ცვლადი დენის ქსელიდან ძაბვით 220 ვ.

სახანძრო დეტექტორები კლასიფიცირდება შემდეგი ფუქციონალური ნიშნების მიხედვით:

1. მოქმედებაში მოყვანის მეთოდის მიხედვით-ავტომატური და ხელის;
2. ინფორმაციის გაცვლის ხასიათის მიხედვით-ზღვრული და ანალოგური
3. ხანძრის საკონტროლო ნიშნის მიხედვით ავტომატური სახანძრო დეტექტორები არსებობენ:
   - — სითბური, რომლებიც რეაგირებენ ტემპერატურის მომატებაზე;
   - — კვამლის, რეაგირებენ კვამლის წარმოქმნაზე;
   - — ალის;
   - — გაზის;
   - — კომბინირებული;
   - — ხანძრის სხვა ნიშნის;
4. ხანძრის თვისებაზე რეაქციის ხასიათის მიხედვით ზღვრული სითბური დეტექტორები იყოფა მაქსიმალურ, დიფერენციალურ და მაქსიმალურ-დიფერენციალურ დეტექტორებად [31].

განვიხილოთ დაცვის დეტექტორების ზოგიერთი ფუნქციონალური

თავისებურებები, რომლებიც აქტიურად გამოიყენება პრაქტიკაში:

წერტილოვანი ელექტროკონტაქტური დეტექტორი-გამოსცემს განგაშის სიგნალს ელექტრო კონტაქტის გაღება-ჩაკეტვის დროს, ეს დაცვის დეტექტორების ყველაზე მარტივი სახეობაა, რომელიც წარმოადგენს წვრილ ლითონის გამტარს, რომელიც სპეციალურადაა დამაგრებული საგანზე ან კონსტრუქციაზე.

მაგნიტოკონტაქტური დეტექტორები - აყალიბებენ სიგნალს მაგნიტური კონტაქტის გაღებისას, გამოიყენება გაღების ბლოკირებისათვის სხვადასხვა სამშენებლო კონსტრუქციებში.

დარტყმით-კონტაქტური დეტექტორები - რეაგირებენ და გამოსცემენ განგაშის სიგნალს ობიექტზე დარტყმითი ზემოქმედების დროს, ძირითადში გამოიყენება შემინული კონსტრუქციების ბლოკირებისათვის.

პიეზოელექტრული დეტექტორები - გამოსცემენ განგაშის სიგნალს დრეკადი ტალღის ზემოქმედების დროს, გამოიყენება სამშენებლო კონსტრუქციების და ცალკეული საგნების ბლოკირებისათვის.

ოპტიკურ-ელექტრონული აქტიური დეტექტორები -სიგნალს აყალიბებენ ხანძრის ან ობიექტზე შეღწევის დროს არეკვლილი ნაკადის ცვლილებისას ან შეწყვეტისას, რაც შეიძლება გამოწვეული იყოს დამრღვევის მოძრაობით აღმოჩენის ზონაში, ძირითადად გამოიყენება შიგა და გარე პერიმეტრების, ფანჯრების, ვიტრინების დასაცავად.

ოპტიკურ-ელექტრონული ინფრაწითელი პასიური დეტექტორი - რეაგირებს ინფრაწითელი გამოსხივების დონის ცვლილებაზე, რაც გამოწვეულია ადამიანის გადაადგილებით აღმოსაჩენ ზონაში, გამოიყენება ნებისმიერი კონფიგურაციის შენობების დაცვისათვის.

ტევადური დეტექტორები - რეაგირებენ მგრძნობიარე ელემენტის ტევადობის შეცვლაზე, რაც განპირობებულია ობიექტზე შეჭრით. ძირითადად გამოიყენება კარადების, სეიფების ბლოკირებისათვის.

კომბინირებული დეტექტორები - საშუალებას იძლევიან გამოვლენილ იქნას დამრღვევი ორი ან მეტი სხვადასხვა მოქმედების

ფიზიკური პრინციპის მიხედვით, ისინი შეიცავენ სხვადასხვა ტიპის არხებს, მაგრამ იცავენ ერთ და იმავე ზონას. თითოეული არხი ასრულებს მუშაობის თავის ფიზიკურ პრინციპს და შესაბამისად აქვს თავისი ფაქტორების ნაკრები, სხვადასხვა არხების არსებობა ამცირებს მცდარი რეაგირების ალბათობას.

1.6 შესვლის მართვისა და კონტროლის სისტემების აგების პრინციპები.

დაცვის ობიექტზე თანამშრომელთა და შემსვლელთა ნაკადი უნდა კონტროლდებოდეს საკონტროლო-გამშვები რეჟიმის მეშვეობით, რომელიც რეალიზდება პროგრამულ-ტექნიკური საშუალებებითა და ორგანიზაციულ-ადმინისტრაციული ღონისძიებებით, რომელთა ერთობლიობა შეადგენს შესვლის მართვისა და კონტროლის სისტემას, რომლებიც განსხვავდებიან სხვადასხვა ნიშან-თვისებების მიხედვით, კერძოდ:

1. მართვის მეთოდის მიხედვით:
   - ავტონომიური-ერთი ან რამდენიმე მოწყობილობის მართვისათვის ცენტრალურ მოწყობილობაზე ინფორმაციის გადაცემის გარეშე;
   - ცენტრალიზებული-ინფორმაციის გამცვლელი მოწყობილობის მართვისათვის, ცენტრალურ პულტთან ცენტრალური მოწყობილობის მხრიდან;
   - უნივერსალური ანუ განაწილებული, რომლებიც ითავსებენ თავის თავში როგორც ავტონომიურ, ისე ქსელურ სისტემებს, რომლებიც მუშაობენ ცენტრალური მოწყობილობის ხელმძრვანელობით;
2. იდენტიფიკაციის დონეების მიხედვით:
   - ერთდონიანი (იდენტიფიკაცია ხდება ერთი ნიშნის მიხედვით);
   - მრავალდონიანი (რამდენიმე ნიშნის მიხედვით);
3. საკონტროლო წერტილების რაოდენობის მიხედვით:
   - მცირე მოცულობა (არა უმეტეს 84 წერტილისა);
   - საშუალო მოცულობა (84-დან 256 წერტილამდე);
   - დიდი მოცულობა (256 ზე მეტი წერტილი);

წვდომის იდენტიფიკაციის მოწყობილობები აითვლიან და შიფრავენ ინფორმაციას, რომლებიც ჩაწერილია სხვადასხვა ტიპის იდენტიფიკატორებზე, როგორებიცაა მაგნიტური ბარათები, ოპტიკური შტრიხ-კოდური ბარათები, ელექტროკონტაქტური კვანძ-გასაღებები, ელექტრონული რადიოსიხშირული უკონტაქტო ბარათები, უკონტაქტო სმარტ-ბარათები და ასე შემდეგ. ასევე ხშირად გამოიყენება ბიომეტრული ტექნოლოგიები, რომელიც გულისხმობს პიროვნების იდენტიფიკაციას ცალკეული სპეციფიკური ბიომეტრული ნიშნების მიხედვით.

მთავარი ამოცანა, რომელიც დგას შესვლისა და ნებართვის სისტემების წინაშე ეს არის წვდომის რეჟიმის უზრუნველყოფა და ინფორმაციის მიღება, დამუშავება და გადაცემა, რომელიც წარმოებს მთვლელებისაგან, ამ ფუნქციის შესრულებას მნიშვნელოვნად უწყობს ხელს აპარატურული საშუალებები-კონტროლერები, რომლებიც წარმოადგენენ მოწყობილობას, გამოყენებადს მთვლელებისაგან მიღებული ინფორმაციის დამუშავებაში, ისინი იყოფიან სამ ჯგუფად:

ავტონომიური კონტროლერები - მთლიანად დასრულებული მოწყობილობაა, რომელიც გამოიყენება გასვლის ერთი წერტილის მომსახურებისათვის, ისინი კონსტრუქტორულად შეიძლება შეერწყას მთვლელებს ან ჩამონტაჟდეს ელექტრულ საკეტში,

ქსელური კონტროლერი - კონტროლერი, რომელსაც კომპიუტერი მართავს, ამ დროს გადაწყვეტილების მიღების ფუნქციები მთლიანად კომპიუტერის პასუხისმგებლობის ქვეშაა, ისინი გამოიყენებიან ნებისმიერი სირთულის სისტემების მართვისათვის.

კომბინირებული კონტროლერები - შეითავსებენ თავის თავში ქსელური და ავტონოლიური კონტროლერების ფუნქციებს, კომპიუტერთან კავშირის არსებობის დროს ისინი მუშაობენ როგორც ქსელური მოწყობილობები, კავშირის არ არსებობის შემთხვევაში კი-როგორც ავტონომიურები [30,31,32].

კონტროლერების შესაძლებლობები უფრო ფართოდ ჩანს

განაწილებული ქსელის პირობებში, რომელიც საშუალებას იძლევა საიმედოდ იქნას დაცული ინფორმაციის დამუშავების პროცესი უარყოფითი ზემოქმედებისაგან და ცენტრალური პერსონალური კომპიუტერის მწყობრიდან გამოსვლის შემთხვევისაგან.

თავი 2.

სამრეწველო ობიექტების დაცვის ვიდეო დაკვირვების სისტემები.

2.1 დაცვის ვიდეო დაკვირვების სისტემების მიმოხილვა.

სამრეწველო ობიექტების დაცვისა და უსაფრთხოების დონის ამაღლებისათვის გამოიყენება მაღალი დონის ტექნიკური საშუალებები, მათ მიეკუთვნება სახანძრო სისტემები, შესვლის ნებართვისა და წვდომის სისტემები, სატელევიზიო დაკვირვების სისტემები. ჩამოთვლილი სისტემები მუშაობენ როგორც ცალკე, ასევე კომპლექსში, მაგალითად ვიდეო დაკვირვების სისტემები გამოიყენებიან არა მარტო დიდი რაოდენობის ობიექტებზე, არამედ ცალკე აღებულ ოფისში ან სახლში. ამიტომ დაცვის ამა თუ იმ სისტემის ამორჩევისას დიდი ყურადღება ექცევა იმ ამოცანებს, რომელიც დგას კონკრეტულ შემთხვევაში [33,34,19].

ერთ ერთ ყველაზე მეტად გავრცელებულ დაცვის ტექნიკურ საშუალებას მიეკუთვნება დაცვის ვიდეო დაკვირვების სისტემები, რომელიც აქტიურად გამოიყენება სახელმწიფო და კომერციული ობიექტების ძალიან ფართო წრეების უსაფრთხოების სისტემებში. მისი მთავარი მომხიბლავი თავისებურებაა ის, რომ ის არა მარტო აფიქსირებს ობიექტის დაცვის რეჟიმის დარღვევას, არამედ საშუალებას გვაძლევს ვიზუალურად გავაკონტროლოთ ვითარება. სწორად დაპროექტებული ვიდეო დაკვირვების სისტემის მიზანია საკონტროლო ზონებში დროის რეალურ მასშტაბში სიტუაციის შეფასების შესაძლებლობა, არასაშტატო სიტუაციაში რეაქციის დროის შემცირება და წარმოქმნილი საფრთხის პირობებში ყველაზე მიზანშეწონილი ზომების მიღების უზრუნველყოფა.

უცხოურ პრაქტიკაში დაცვის ვიდეო დაკვირვების ხშირად უწოდებენ „ჩაკეტილ ვიდეოაპარატურას“ (Closed Circuit Video), ეს მიუთითებს მის განსხვავებაზე სამაუწყებლო ტელევიზიისაგან, რომლის საშუალებითაც შესაძლებელია მრავალფეროვანი პროგრამების მიღება. დაცვის ვიდეო

დაკვირვების სისტემებში კი მონიტორის ეკრანზე მიიღება ერთი ან რამდენიმე კამერის გარკვეული გამოსახულებები. ოპერატორის გარდა ვერავინ ვერ აკვირდება ამ გამოსახულებებს, სწორედ ამიტომ უწოდებენ ამ სისტემებს ჩაკეტილს.

დაცვის ვიდეო დაკვირვების სისტემები-ეს ჩაკეტილი ტიპის ვიდეო დაკვირვების სისტემაა, რომლის დანიშნულებაა დასაცავი ობიექტიდან ვიდეო გამოსახულების მიღება კრიმინალსაწინააღმდეგო დაცვისათვის.

დაცვის ვიდეო დაკვირვების სისტემების გამოყენება მნიშვნელოვნად ამაღლებს დაცვის ეფექტურობას მთლიანობაში, ამცირებს მომსახურე პერსონალის რაოდენობასა და ობიექტის უსაფრთხოებისათვის დანახარჯებს, უზრუნველყოფს ობიექტის სადღეღამისო ვიდეოკონტროლს, ქმნის ვიდეოარქივებს, განსაზღვრავს დარღვევის ხასიათს, დარღვევის ადგილს, დამრღვევის მოძრაობის მიმართულებას, იღებს აუცილებელ ზომებს, ამაღლებს არა მარტო ადმინისტრაციის, არამედ უსაფრთხოების სამსახურების მუშაობის კომფორტულობას, ამიტომ ამ სისტემების გამოყენება ან მათი დამატება სხვა სისტემებზე დაცვის სიგნალიზაციის კომპლექსურ სისტემებში უკვე არის აუცილებელი. დაცვის ვიდეო დაკვირვების სისტემები, რომლებიც ინტეგრირებულია უსაფრთხოებისა და დაცვის სისტემებში, აიგება ციფრული და კომპიუტერული ტექნოლოგიების, ასევე ვიდეოინფორმაციის საფუძველზე სპეციალიზებული ციფრული მოწყობილობების საფუძველზე

2.2 დაცვის ვიდეო დაკვირვების სისტემების ფუნქციები

დაცვის ვიდეო დაკვირვების სისტემების გამოყენება უზრუნველყოფს შემდეგი ფუნქციების შესრულებას:

- საკონტროლო ზონის პირდაპირი ვიდეო დაკვირვება ოპერატორის მიერ, დანიშნულების მიხედვით დაკვირვების ობიექტების აღმოჩენა და იდენტიფიკაცია, მათ შორის ხალხი, სატრანსპორტო საშუალებები, ქონება, ობიექტების ინფრასტრუქტურის ელემენტები;
- დასაცავი ზონების მდგომარეობის შესახებ ვიზუალური ინფორმაციის

გადაცემა ობიექტის პერიმეტრის, დაცვის პუნქტისა და გადაადგილების შესახებ განგაშის ვიდეოვერიფიკაციისათვის;

- დასაცავი ობიექტის მდგომარეობის ანალიზისათვის ვიდეოინფორმაციის არქივის შექმნა საგანგაშო სიტუაციების შეფასებისათვის, ასევე დამრღვევის იდენტიფიცირებისა და სხვა ამოცანების შესასრულებლად.

პირდაპირი ვიდეო დაკვირვება უნდა ხორციელდებოდეს უწყვეტ რეჟიმში ვიდეოგამოსახულების მიღებით ცალკეული ოპერატორების ვიდეომონიტორზე (ვიდეომონიტორებზე), არა უმეტეს ოთხი ვიდეოკამერის გამოსახულებისა ერთ მონიტორზე-ერთი ოპერატორის უწყვეტი დაკვირვების პირობებში. პრაქტიკაში პირდაპირი ვიდეოდაკვირვება წარმოებს პერიოდულად წარმოქმნილ საფრთხეზე პასუხის ნიშნად ობიექტის მდგომარეობის შესამოწმებლად. არსებობს ვიდეოინფორმაციის დათვალიერების ოთხი ძირითადი შესაძლებლობა:

1. **ლოკალური დაკვირვება-** გამოიყენება მცირე ობიექტების (საცალო ვაჭრობის, ბანკების ან მცირე ბიზნესის საწარმოები) ტერიტორიის მონიტორინგისათვის ვიდეოჩამწერი მოწყობილობის გამოსასვლელიდან ან სერვერიდან;
2. **დაშორებული დაკვირვება პერსონალური კომპიუტერის საშუალებით** - პირდაპირი ან ჩაწერილი ვიდეოგამოსახულების დათვალიერებისათვის გამოიყენება პერსონალური კომპიუტერები სპეციალური ვებ-ბროუზერებით ან პროგრამებით;
3. **მობილური დაკვირვება**- საშუალებას აძლევს მცველს, რომელიც იმყოფება ობიექტის ტერიტორიაზე, ელვისებურად შეამოწმოს რას აღწერს ვიდეო დაკვირვება. მობილურ დაკვირვებას აქვს დიდი პოტენციალი ოპერატიული და სწრაფი რეაგირების ჯგუფების შეთანხმებული მუშაობის კუთხით;
4. **ვიდეოკედელი** - ეს იდეალური გადაწყვეტაა დიდი სტაციონალური ცენტრებისათვის, რომლებიც ფლობენ დაკვირვების ასობით და

ათასობით კამერას. ვიდეოკედელი ქმნის ძალიან დიდ ეკრანს, რომელიც აკვირდება ხალხის ჯგუფებს, ეს განსაკუთრებით საჭიროა საგანგებო სიტუაციების დროს, ვიდეოკედელს აქვს საშუალება გადაერთოს კამერებს შორის, ასევე შეუძლია ავტომატურად მოახდინოს იმ კამერების გამოსახულებათა დემონსტრირება, სადაც ადგილი ჰქონდა განგაშს [1930,31].

განგაშის ვერიფიკაციისას ვიდეოდაკვირვება უნდა გამოიტანებოდეს მონიტორზე განგაშის სიგნალის მიღებისთანავე, დაცვის სიგნალიზაციის დეტექტორებიდან, რომლებიც ლოგიკურად არიან დაკავშირებული კონკრეტულ ვიდეოკამერასთან. ვიდეოკამერები შეიძლება ჩაირთოს ასევე მოძრაობის ვიდეოდეტექტორის სიგნალის მიხედვით.

არქივში ვიდეოინფორმაციის ჩაწერის ავტომატური ჩაწერა ხორციელდება უწყვეტად, ცხრილის მიხედვით პერიოდულად, დეტექტორების ამოქმედებისთანავე. არქივაციის ტექნიკური საშუალებები უნდა უზრუნველყოფდეს ვიდეოინფორმაციის საკმარისი რაოდენობის შენახვას იმ დროის განმავლობაში, რომელიც განისაზღვრება ობიექტის დაცვის რეჟიმის პირობებით.

2.3 ვიდეო დაკვირვების სისტემის კომპონენტები და მათი პარამეტრები

დაცვის სატელევიზიო სისტემების ტიპიურ შემადგენლობაში შედის ვიდეოკამერები, რომელთა რაოდენობა განისაზღვრება ვიდეოსისტემაზე დაკისრებული ამოცანების მიხედვით, ვიდეოსიგნალის გადაცემის არხებით, ასევე ვიდეოინფორმაციის შენახვისა და დამუშავების, გამოსახვის საშუალებებით.

დაცვის ვიდეო დაკვირვების სისტემების ძირითად აპარატურულ-ტექნიკურ და პროგრამულ საშუალებებს ფუნქციონალურად ყოფენ:

- ვიდეოსიგნალების წყაროებად (ვიდეოკამერები ობიექტივებით);
- ვიდეო სიგნალების ანალოგურ-ციფრული გარდაქმნის მოწყობილობებად;
- ვიდეოსიგნალის გადაცემისა და კომუტაციის საშუალებებად;

- ვიდეოგამოსახულების გამომტანი მოწყობილობებად;
- ციფრული დაცვის ვიდეო დაკვირვების სისტემებისათვის ვიდეომონაცემების მიღებისა და დამუშავების საშუალებებად;

დამატებით ამ სისტემის შემადგენლობაში შეიძლება შედიოდეს: კვების ბლოკები, კომუტაციის მოწყობილობები, სხვადასხვა არხებით ვიდეოსიგნალების გადაცემის აპარატურა, ვიდეოკამერების დამაგრებისა და ბრუნვის მოწყობილობები, ვიდეოკამერების ფარები, განათებისა და ინფრაწითელი მინათების საშუალებები, ასევე სხვა მოწყობილობები, რომლებიც აუცილებელია სისტემის ნორმალური მუშაობისათვის [34,33,32].

კონსტრუქციულად დაცვის ვიდეო დაკვირვების სისტემები უნდა იგებოდეს მოდულური პრინციპით და უზრუნველყოფდეს ექსპლოატაციის პირობებში შემდეგი ფუნქციების შესრულებას:

- ერთნარი ტიპის ტექნიკური დეტალების სრულ ურთიერთშეცვლას;
- რემონტის, ექსპლოატაციისა და ტექნიკური მომსახურების მოხერხებულობას;
- მართვის ელემენტებზე არასანქცირებული წვდომის გამორიცხვას;
- ექსპლოატაციის პროცესში საჭირო კვანძებზე და ბლოკებზე სანქცირებულ წვდომას;

დაცვის ვიდეო დაკვირვების სისტემების ერთ-ერთ მთავარ კომპონენტს წარმოადგენს ვიდეოსიგნალის წყარო-ვიდეოკამერები, ისინი ოპტიკურ-ელექტრონული მოწყობილობებია, რომლებიც დასაკვირვებელი ობიექტის ოპტიკურ გამოსახულებას გარდაქმნიან გარკვეული სტანდარტის ელექტრულ ვიდეოსიგნალად.

ვიდეოკამერა წარმოადგენს ელექტრონულ დაფას, რომელზეც განლაგებულია მგრძნობიარე ელემენტი და ობიექტივი. კონსტრუქციული შესრულების, ტექნიკური მახასიათებლების და ექსპლოატაციის პირობების მიხედვით ისინი იყოფიან კორპუსიან და უკორპუსო, შავ-თეთრ და ფერად გამოსახულებიანი, ჩვეულებრივი და მომატებული მგრძნობელობის, ჩვეულებრივი და მაღალი გარჩევადობის, შიგა და გარე დაკვირვების,

ფარული დაკვირვების ვიდეოკამერებად [1].

ყველაზე ეფექტურად ისინი უნდა განლაგდებოდნენ კრიტიკულ ზონებში, მათი განლაგებისას გამოიყენება ორი ძირითადი პრინციპი:

- გადასვლის წერტილებზე (კარები, კორიდორები, გასასვლელები) დაკვირვება;
- ყველაზე ფასეულზე დაკვირვება.

გადასვლის წერტილებად ითვლება ის ზონები, რომელთა საშუალებითაც ხალხი და ტრანსპორტი უნდა მოხვდეს ობიექტზე, ამ წერტილებში კამერების განლაგება ეკონომიურად გამართლებულია იმათ დასადგენად, ვინც ხვდება დასაცავ ობიექტზე.

ფასეულია სპეციფიური ობიექტები, რომლებიც ითხოვენ მაღალი უსაფრთხოების უზრუნველყოფას და მათი მნიშვნელობა განსაზღვრულია კონკრეტული დამკვეთის მიერ.

ვიდეოკამერის გამოსახულების ხარისხი განპირობებულია მთელი რიგი მაჩვენებლებით, მაგრამ უმეტეს შემთხვევაში კონკრეტული სისტემის კამერის ამორჩევისათვის ორიენტაცია აღებულია შემდეგი პარამეტრები:

ოპტიკური ფორმატი - სენსორის ფოტომგრძნობელობის ზომა დიუმებში დიაგონალზე (1 დიუმი შეესაბამება 25,4 სმ). ძირითადი ფორმატებია: 1/4“, 1/3“, 1/2“, 2/3“ და 1“. რაც უფრო მეტია ოპტიკური ფორმატი, მით უფრო ნაკლებია გამოსახულების გეომეტრული დამახინჯება.

გარჩევადობის უნარიანობა - კამერის პარამეტრია, რომელიც განსაზღვრავს ვიდეოკამერის შესაძლებლობას, გადმოსცეს გამოსავალზე გამოსახულების უმცირესი დეტალები მაღალი ხარისხით.

განათებულობის მუშა დიაპაზონი - ვიდეოკამერის ხედვის არეში განათებულობის არეა მინიმალურიდან მაქსიმალურამდე, რომელშიც გარჩევადობის უნარის შეფარდება ვიდეოკამერის სიგნალთან არაა მოცემულზე ნაკლები.

ზღვრული მგრძნობელობა - ფოტომგრძნობიარე ფართობზე

მინიმალური განათებულობაა, რომელზეც ვიდეოკამერა ინარჩუნებს მუშაობისუნარიანობას.

დაცვის სატელევიზიო სისტემების მთავარი ელემენტია ობიექტივი, მის ამორჩევაზეა დამოკიდებული კამერის ხედვის კუთხე, მგრძნობელობა და მთელი სისტემის გარჩევადობა [31,33].

დიაფრაგმის რეგულირების მეთოდის მიხედვით ობიექტივები იყოფა სამ ჯგუფად: ფიქსირებულ, ხელის და ავტომატურ დიაფრაგმიან ობიექტივებად. ყველაზე მარტივია ფიქსირებულ დიაფრაგმიანი ობიექტივები, რომლებიც დაყენებულია ვიდეოკამერებზე, ფოკუსირება სრულდება ხელით.

ავტოდიაფრაგმიან ობიექტივებს იყენებენ გარე დაკვირვებისათვის, მისი მექანიზმი წარმოადგენს უარყოფით ელექტრო-მექანიკურ უკავშირს სიგნალის დაყოვნებისათვის წინასწარ მონიშნულ დონეზე.

ვარიფოკალური ობიექტივი-ერთიანი ოპტიკური სისტემაა, რომელთა კომპონენტებს აქვთ ერთმანეთის მიმართ გადაადგილების უნარი, ამ დროს იცვლება ფოკუსური მანძილი, მაგრამ შენარჩუნებულია გამოსახულების ხარისხი, იგი იძლევა მასშტაბირების ანუ გამოსახულების ზომის გადიდების საშუალებას, ისე რომ არ შეიცვალოს კამერის განლაგება.

2.4 ინფორმაციის გადაცემის საშუალებები ვიდეო დაკვირვების სისტემებში.

ტექნიკის განვითარების თანამედროვე საშუალებები და მიდგომები საშუალებას იძლევა შეიქმნას ყველაზე მრავალფეროვანი რთული განშტოებადი სისტემები დაცვისა და ვიდეოდაკვირვებისათვის. მთავარი ამოცანა, რომელიც გადიჭრება ასეთი სისტემების მიერ - სიგნალის გადაცემაა წყაროდან მიმღებამდე, ამ პრობლემის გადაწყვეტის რამდენიმე საშუალება არსებობს, რომლებსაც თავისი პლიუსები და მინუსები გააჩნია.

დაცვის ვიდეო დაკვირვების სისტემებში აუცილებელია ინფორმაციის გადაცემა მოხდეს ვიდეოკამერიდან იმ მოწყობილობებში, რომლებიც დაყენებულია დაცვის ადგილებში- ვიდეომონიტორებისთვის, ვიდეორეგისტრატორებისათვის და ვიდეოკავირვების სხვა

სისტემებისადმი. გარდა ვიდეოსიგნალისა, შესაძლებელია აუდიოსიგნალის გადაცემაც, ამასთან მანძილი, რომელზეც ხდება სიგნალის გადაცემა, შეიძლება რამდენიმე ათეული მეტრიდან რამდენიმე ათეულ კილომეტრამდე. ბოლო პერიოდში დაცვის ვიდეო დაკვირვების სისტემებში გამოიყენება ვიდეოსიგნალის გადაცემის შემდეგი მეთოდები: კოაქსიალური კაბელით, კაბელით „დახვეული წყვილი“ და ოპტიკურ-ბოჭკოვანი კაბელით. მანძილზე დამოკიდებულების მიხედვით იყენებენ სხვადასხვა ტექნოლოგიებს და ვიდეოსიგნალის გადაცემის საშუალებებს [2].

ყველაზე მეტად გავრცელებულია ვიდეოსიგნალის გადაცემა კოაქსიალური კაბელით, ეს საიმედო და იაფი საშუალებაა, მაგრამ აქვს თავისი ნაკლოვანებები, 300 მ-ის მეტ მანძილზე გადაცემისას სიგნალის ხარისხი უარესდება, ეცემა სიგნალის დონე, შეიძლება წარმოიქმნას სიხშირული დამახინჯებები, რასაც მივყავართ გამოსახულების სიმკვეთრის დაცემამდე, ეს რომ თავიდან ავიცილოთ, საჭიროა ყოველ 250-300 მ-ში დავაყენოთ სიგნალის გამაძლიერებლები, რაც საჭიროებს კვების მიყვანას დაყენების ადგილზე, რაც ამცირებს დამოკიდებულებას სიგნალი/ხმაური, ეს ასევე აისახება ვიდეოსიგნალის ხარისხზე.

1,5 კმ მანძილამდე სიგნალის გადაცემისას იყენებენ „დახვეული წყვილის“ ტექნოლოგიას, ამ დროს საჭირო არ არის სიგნალის გამაძლიერებლების დაყენება, მდგრადია სხვადასხვა ხმაურის და სხვა ხელისშემშლელი პირობების მიმართ, სისტემის შემადგენლობაში შედის გადამცემი, დახვეული წყვილი და მიმღები, იგი საშუალებას გვაძლევს გადავცეთ ვიდეო, აუდიო მართვის და სატელეფონო სიგნალები, ასეთი კაბელის გაშვება უფრო იაფია, ვიდრე კოაქსიალური ან ოპტიკურბოჭკოვანი კაბელების გაჭიმვა.

მიუხედავად იმისა, რომ ოპტიკურ-ბოჭკოვანი კაბელები საკმაოდ ძვირია, დიდ მანძილებზე სიგნალების გადაცემის შემთხვევაში მისი გამოყენება უფრო იაფია, ვიდრე კოაქსიალური კაბელების სისტემის გამოყენება, რომელიც დაკომპლექტებულია ვიდეოსიგნალის გამაძლიერებლებით და

სხვა მოწყობილობებით.

უკანასკნელი წლების ერთ-ერთ ყველაზე თავბრუდამხვევ ტექნოლოგიურ ნამუშევარს წარმოადგენს თანამგზავრული ნავიგაციის სფეროში არსებული მიღწევები, ამ წლების განმავლობაში თანამგზავრულმა ნავიგაციამ გადალახა გზა მეცნიერული ფაქტიდან სწრაფად განვითარებად ტექნოლოგიამდე მთელ მსოფლიოში, რომლის დროსაც იოლად და საიმედოდ განისაზღვრება ობიექტის პოზიცია რეალურ დროში [25,24,23].

2.5 გამოსახულებათა სახეები, მათი მიღების ტექნიკური საშუალებები და პარამეტრები.

აუცილებელია, რომ დაცვის ვიდეო დაკვირვების სისტემები იძლეოდნენ ისეთი ხარისხის გამოსახულებას, რომელიც შეესაბამება მის წინაშე დასმულ ამოცანებს, თუ აუცილებელია იდენტიფიცირება, მაშინ უხარისხო გამოსახულებებმა შეიძლება ეჭვქვეშ დააყენოს მთელი სისტემის მუშაობის მიზანშეწონილობა, ამიტომაც ასეთი სისტემების დაყენებისას ატარებენ შემდეგ ფარდობით გაზომვებს:

- ✓ მოცემულ უბანზე ვიდეო დაკვირვების დაფარვის ზონის შემოწმება;
- ✓ დეტალების გარჩევადობის სპეციალური მოთხოვნებისა და მასშტაბის შემოწმება;
- ✓ ოპერატორის მიერ თავისი ამოცანის შესრულების ხარისხისა და სისწრაფის კომპლექსური შემოწმება;
- ✓ ჩანაწერის კომპლექსური შემოწმება;

ობიექტის განათებულობა ძლიერ გავლენას ახდენს გარჩევადობაზე, ამიტომაც ძალიან დაბალი განათებულობის მქონე ობიექტებზე ირჩევენ მაღალი მგრძნობელობის და გარჩევადობის პარამეტრის მქონე კამერებს, მათ ასევე უნდა ჰქონდეთ სიგნალის გაძლიერების ავტომატური სისტემა, რომელიც უზრუნველყოფს კამერის მუშაობას მცირე განათების შემთხვევაშიც [1].

არასაკმარისი განათების პირობებში ფარული ვიდეოდაკვირვებისათვის იყენებენ სპეციალიზებულ კამერებს, რომელთა

მგრძნობელობის მაჩვენებელი აღემატება ჩვეულებრივ ნახევარგამტარულ კამერებს 100 ან 1000 ჯერ, რაც მიიღწევა გამოსხივების გამაძლიერებლის დახმარებით.

მონოქრომულ და ფერად კამერებს აქვთ თავისი უპირატესობები და ნაკლოვანებები, ფერადი კამერები მეტად ინფორმატიულები არიან, მაგრამ ნაკლები მგრძნობელობისაა, რაც ზღუდავს მათ გამოყენებას ნაკლები განათებულობის პირობებში. მათი მატრიცები მგრძნობიარეა ინფრაწითელი გამოსხივების მიმართ, რაც დამატებითი პარამეტრია მგრძნობელობისადმი, მაგრამ ამ დროს მახინჯდება მუქი ფერები გამოსახულებაზე, ეს პრობლემა მოხსნილია ფერადი კამერების კლასზე „დღე/ღამე“, რომლებიც კარგი განათების პირობებში მუშაობენ ფერად რეჟიმში, ხოლო განათების შემცირებისას გადაერთვება მონოქრომულ რეჟიმში [2].

კამერების ერთ-ერთი სახეობაა ბრუნვადი ვიდეოკამერები, რომელსაც PTZ-კამერებსაც უწოდებენ (Pan, Tilt, Zoom), ასეთი კამერების რეალიზაციის ორი გზა არსებობს:

- ✓ როგორც სტატიკური ვიდეოკამერა, რომელიც დაყენებულია ბრუნვად მოწყობილობაზე;
- ✓ როგორც სიჩქარიანი ბრუნვადი ვიდეოკამერა, რომელიც შესრულებულია სფეროს ფორმით;

ბრუნვადი ვიდეოკამერები- ფუნქციონალურად დასრულებული კვანძია, რომელიც შედგება ვიდეოკამერისაგან, ბრუნვადი მოწყობილობის, კვების ბლოკის და სიგნალების მიმღები მოწყობილობისაგან.

ობიექტივისა და ბრუნვადი მოწყობილობის დისტანციური მართვა ვიდეოკამერას აძლევს ორიენტირების საშუალებას როგორც აზიმუტის, ისევე ხედვის კუთხის მიმართ [25,26].

ბრუნვადი კამერის მართვა შეიძლება ინტეგრირდეს ვიდეოჩაწერის სისტემაში.

მობრუნებადი კამერის ძირითადი ფუნქციები და შესაძლებლობებია:

- ჰორიზონტალურ სიბრტყეში მობრუნება 360 ^{0}, ხოლო ვერტიკალურ სიბრტყეში 180^0-ით;
- X12…X36 ჯერადი ოპტიკური და X10…X25 ჯერადი ციფრული გადიდება.
- 4...256 გადაყენების წერტილი-კამერის დაკვირვების წერტილები წინასწარ გათვლილი პარამეტრებით და ვერტიკალური და ჰორიზონტალური კუთხეებით, ასევე ობიექტივის ფოკუსით.
- 1...32 დაყენების წერტილის თანმიმდევრული დათვალიერება ვიდეოკამერის მიერ;
- მოცემული დაკვირვების სექტორის ავტომატური სკანირება;
- „ავტოთვალთვალი“-რეჟიმი, როდესაც ვიდეოკამერა ავტომატურად „იჭერს“ კადრში ყველაზე დიდ ობიექტს, ამავდროულად ის აახლოვებს მოძრავ ობიექტს ინარჩუნებს რა მას კადრის ცენტრში.

ბრუნვადი ვიდეოკამერების უპირატესობაა ის, რომ ის აკონტროლებს დიდ ტერიტორიებს, თანმიმდევრობით მოიცავს მის სხვადასხვა ნაწილებს, თავისი ინფორმატიულობით ერთი ასეთი კამერა აღემატება ტერიტორიაზე განლაგებულ რამდენიმე კამერას, მათ ნაკლოვანებებს მიეკუთვნება:

- კამერის ინფორმატიულობა იმით განისაზღვრება, რამდენად კარგად აირჩია ოპერატორმა მიმართულება და ხედვის კუთხე საჭირო მომენტში;
- წარუმატებელი მოქმედების შედეგად დამრღვევის გაშვების შესაძლებლობა;
- ძალიან მაღალი ნერვულ-ფსიქოლოგიური დატვირთვა ვიდეოდაკვირვების ოპერატორებზე.

PTZ-ვიდეოკამერები ავტომატურად ფოკუსირდება ობიექტზე და უთვალთვალებს მას, ადიდებს გამოსახულებას უკეთ დანახვის მიზნით, როდესაც სათვალთვალო ობიექტი გადის მხედველობის არიდან, ის ეძებს სხვა ობიექტს, თუ მის მხედველობის არეში ხვდება ერთდროულად რამდენიმე ობიექტი, მაშინ თვალთვალის სისტემა ირევა, ამიტომ ასეთი კამერების გამოყენება ოპერატორის გარეშე მიზანშეწონილია მხოლოდ

მცირედ დატვირთული გარემოსთვის. ისინი უფრო ხშირად გამოიყენებიან გაშლილი ტერიტორიებისათვის, პერიმეტრის დაცვისათვის და ა.შ [3].

თანამედროვე პირობებში სწრაფი ტემპებით ვითარდება ვიდეოსიგნალის ციფრული დამუშავების მეთოდები. ასეთ სისტემებში ანალოგური სიგნალი გაივლის რა ანალოგურ-ციფრულ გარდამქმნელს, მუშავდება მიკროპროცესორში და მიეწოდება ციფრულ მონიტორზე., ეს საშუალებას იძლევა მნიშვნელოვნად ამაღლდეს გამოსახულების ხარისხი და გარჩევადობა.

თვალთვალის ვიდეო დაცვითი სისტემები ვითარდება შემდეგი ოთხი მიმართულებით:

- სალაპარაკო პანელში ჩაშენებული ფარული ვიდეო დაკვირვების კამერები;
- ვიდეო „თვალი“ კარებში;
- ფარული დაკვირვების მინიატურული კამერა;
- გარეთ გამოტანილი დაკვირვების ფარული კამერა;

ფარული ვიდეო დაკვირვების კამერები და ვიდეო „თვალი“ მონტაჟდება კარებში ან სალაპარაკო პანელში. ობიექტზე დაკვირვების ხარისხის ამაღლების მიზნით მათ გააჩნიათ მცირე ფოკუსური მანძილი და ხედვის კუთხე 160 გრადუსამდე, დღე-ღამის ბნელ დროს იყენებენ ინფრაწითელი დანათების მოწყობილობებს [2].

ციფრული სატელევიზიო სისტემების განვითარების ერთ-ერთი მთავარი მიმართულებაა ვიდეოდაკვირვების სისტემები IP-კამერების ბაზაზე, რომელსაც ხშირად უწოდებენ ქსელური ვიდეოდაკვირვების სისტემებს, ისინი იყენებენ ვიდეო და აუდიო სიგნალების გადაცემისათვის სადენიან ან უსადენო ქსელს. ქსელური ვიდეოდაკვირვების სისტემა, საშუალებას იძლევა ქსელის ნებისმიერი წერტილიდან დაათვალიეროს და ჩაწეროს ვიდეო, არა აქვს მნიშვნელობა ეს ქსელი ლოკალურია, გლობალურია თუ ინტერნეტია.

IP-ვიდეოდაკვირვების აქტიური დანერგვა განპირობებულია მთელი

რიგი მიზეზებით:

- IP-ინდუსტრიის მიღწევების გამოყენების შესაძლებლობით;
- ციფრული სახით ინფორმაციის გადაცემის ან შენახვისას არ აქვს ადგილი ინფორმაციის დამახინჯებას;
- დიდი ვიდეოსისტემებისათვის ეკონომიკური ეფექტურობით;
- ვიდეოანალიზის შესაძლებლობის გამო ახალი ფუნქციების რეალიზებით;

ქსელური ვიდეოდაკვირვების სისტემების საბაზო კომპონენტს წარმოადგენს ქსელური კამერები, ვიდეოკოდერები და პროგრამული უზრუნველყოფა, ვიდეოს მართვისათვის, დანარჩენი კომპონენტები, მათ შორის ქსელი, შენახვის სისტემები, სერვერი წარმოადგენს სტრანდარტულ მოწყობილობებს [28, 25,26].

ქსელური ვიდეოკოდერის საშუალებით ანალოგური ვიდეოკამერების მიერთებით მომხმარებელი იღებს იმ უპირატესობას, რომ აღარ არის საჭირო ვიდეოგამოსახულების მისაღებად უკვე არსებული ანალოგური მოწყობილობების (ვიდეოკამერები, კოაქსიალური კაბელი) შეცვლა.

IP-კამერების ქვეშ იგულისხმება ციფრული ვიოდეოკამერა, რომელიც იძლევა ინფორმაციას ვიდეონაკადის სახით ციფრულ ფორმატში, მათ შეუძლიათ ინფორმაციის მოცემა როგორც შეკუმშული, ისე გაშლილი სახითაც, ამისათვის ისინი იყენებენ TCP, UDR და სხვა ტიპის პროტოკოლებს.

იმის გამო, რომ ასეთ კამერებს არ სჭირდებათ ანალოგური სიგნალის გადაცემა, მათში გამოყენებულია მეგაფიქსელური გარჩევადობა, სტანდარტულია 640X480, მაგრამ არსერბობენ მეგაფიქსელური გარჩევადობის კამერებიც 1280X1024, 1600X1200 და უფრო მაღალიც.

ქსელური ვიდეოდაკვირვების სისტემები ფლობენ ფუნქციონალურ უპირატესობებს ანალოგურ სისტემებთან შედარებით:

- გამოსახულების მაღალი ხარისხის მიღწევა და მკვეთრი დაფიქსირების

საშუალება, შედეგად ადვილია მოვლენის მონაწილეთა იდენტიფიცირება, ხოლო კამერებში მეგაფიქსელური ტექნოლოგიების გამოყენება იძლევა გამოსახულების უკეთეს ხარისხს და მაღალ გარჩევადობას, ვიდრე ანალოგურ კამერებში.

- ქსელურ სისტემებში გამოსახულების მაღალი ხარისხის მიღწევა უფრო ადვილია, ვიდრე ანალოგურში, ანალოგურ სისტემებში მიმდინარეობს რამდენიმე ანალოგურ-ციფრული გარდაქმნა, ხოლო ყოველი გარდაქმნისას გამოსახულების ხარისხი უარესდება, უარყოფითად მოქმედებს გამოსახულების ხარისხზე გადაცემის სიშორეც, რაც მეტია გადაცემის მანძილი, მით უფრო სუსტია სიგნალი, ხოლო ციფრულ სატელევიზიო სისტემებში გამოსახულება ერთხელ ციფრულდება და რჩება ამ ფორმით, ასეთი სახით ის ადვილად ინახება და მისდამი წვდომაც უფრო ადვილია.
- ხშირად ჩაწერილი ვიდეოინფორმაციის დიდი მოცულობის გამო, შეუძლებელია ხარისხიანი ვიდეოანალიზის გაკეთება, ხოლო ქსელური კამერები ჩაშენებული ინტელექტუალური და ანალიტიკური ფუნქციებით ადვილად უმკლავდებიან ამ პრობლემას, ამცირებენ არასაჭირო ჩაწერების რაოდენობას და იყენებენ წინასწარ განსაზღვრულ მოვლენებს. ასეთი შესაძლებლობები არ გააჩნიათ ანალოგურ სისტემებს [2,3].

შეიძლება განვაზოგადოთ და ჩამოვაყალიბოთ ქსელური კამერების უპირატესობები ანალოგურთან შედარებით;

- მასშტაბირებადი განაწილებული სისტემების აგების შესაძლებლობა;
- ვიდეოკამერის მუშაობისათვის საჭირო პარამეტრების ფართო დიაპაზონი:
- არ არის „მიბმული“ ანალოგურ სტანდარტებზე, ამიტომ შესაძლებელია IP-კამერების დანერგვა მაღალი გარჩევადობით;
- ასეთი კამერები შეიძლება ვარეგულიროთ მოცილებულად, მივცეთ საშუალება რამდენიმე ავტომატიზებულ მომხმარებელს დაათვალიეროს

გამოსახულება რეალური დროის რეჟიმში და ჩაიწეროს ვიდეოგამოსახულებები მსოფლიოს ნებისმიერი წერტილიდან.

- აუდიო და ვიდეონაკადის ერთდოულად გადაცემის შესაძლებლობა ქსელში პარალელურ რეჟიმში;
- ნაკადების შეკუმშულ რეჟიმში გადაცემის შესაძლებლობა, რაც იძლევა ვიდეომატარებლებზე ადგილის ეკონომიის საშუალებას, თანაც ამ დროს არ არის საჭირო მაღალმწარმოებლური ვიდეორეგისტრატორი.

მაგრამ IP-კამერებს აქვთ ნაკლოვანებებიც ანალოგურთან შედარებით;

- IP-კამერების ფასი გაცილებით მაღალია, ვიდრე ანალოგურების, მაგრამ თუ განვიხილავთ ობიექტის მოწყობილობას დაკვირვების სისტემებთან ერთად მაშინ ფასები თავსებადია ერთმანეთთან;
- IP-კამერების მგრძნობელობა გაცილებით დაბალია, ვიდრე ანალოგურის;
- ვიდეონაკადის დეკომპრესიის აუცილებლობა კომპიტერულ პლატფორმაზე;
- კომპიუტერული ქსელის „გატეხვის“ შესაძლებლობა;
- აპარატურული „ჩამოკიდების“ შესაძლებლობა.

დაცვის ვიდეო დაკვირვების სისტემების ერთ-ერთი ძირითადი ფუნქციაა-ვიდეოჩაწერა, რომელიც შეიძლება რეალიზებული იქნას ვიდეოჩაწერის მოწყობილობებით-ციფრული ვიდეორეგისტრატორებით ან პროგრამული მეთოდით პერსონალური კომპიუტერების ბაზაზე შესაბამისი პროგრამული უზრუნველყოფით [2,3,26].

ვიდეორეგისტრატორი - მოწყობილობაა, რომელიც გამოიყენება ვიდეოინფორმაციის ჩასაწერად, აღსაქმნელად და შესანახად, თითოეული ვიდეოკამერისათვის შეიძლება ინდივიდუალურად შემუშავდეს პარამეტრების განლაგება ჩაწერის რეჟიმისათვის.

ჩანაწერის დათვალიერებისას ვიდეორეგისტრატორი:

- არეგულირებს დათვალიერების სისწრაფეს, მათ შორის პირდაპირი და უკუ ნახვისას;

- ასახავს არა ერთი, არამედ რამდენიმე კამერის გამოსახულებებს, ან ასახავს ერთი კამერის გამოსახულებას მაქსიმალური გარჩევადობით;
- ეძებს ჩანაწერებს ბეჭდვის შესაძლებლობით დროის მიხედვით და თითოეული კამერის მიხედვით.

ვიდეორეგისტრატორების ძირითადი პარამეტრებია:

ვიდეოარხი - ტექნიკურ საშუალებათა ერთობლიობა, ვიდეო გამოსახულების გადასაცემად ერთი ვიდეოკამერიდან ვიდეომონიტორის ეკრანზე, ძირითადად გამოიყენება 4,8,16 ვიდეოარხიანი ვიდეორეგისტრატორები, იშვიათად 24 ან 32 არხით.

გარჩევადობის უნარი - მითითებულია ფიქსელებში ჰორიზონტალურად და ვერტიკალურად, უფრო ხშირად გამოიყენება 352X288, 704X288, 704X576 ფიქსელი.

ჩაწერის სიჩქარე - ეს იმ კადრების რაოდენობაა, რომელსაც რეგისტრატორი ამუშავებს 1 წამის განმავლობაში. ვიდეოდაკვირვების სისტემებში კადრული სიჩქარე არ უმდა აჭარბებდეს 25 კადრს წამში.

ციფრული ვიდეორეგისტრატორები უნდა უზრუნველყოფდეს ვიდეოარქივის წარმოებას და მის შენახვას 15 დღე-ღამის განმავლობაში, ამავე დროს გამოსახულების ხარისხი არ უნდა გაუარესდეს 10%-ზე მეტად [2].

ერთი ვიდეოარხით 1 წანის განმავლობაში გარჩევადობით 704X576-ზე 25 კადრი/წმ სიჩქარით ჩაწერისას მოცულობა 30 მბაიტია, ძნელია არაა დაითვალო არქივის მოცულობა ერთი საათის ან ერთი დღე-ღამის განმავლობაში, ვიდეოჩაწერის მოცულობის შესამცირებლად იყენებენ შესაკუმშ ალგორითმებს (კომპრესიებს), რომლების ამცირებენ ფაილის მოცულობას იმ გრაფიკული ელემენტების მოცილებით, რომლებსაც ადამიანის თვალი ვერ აღიქვამს, ვიდეოსიგნალის კოდირების ალგორითმები გამოიყენება ციფრული წარმოდგენისთვის, ასევე ვიდეოინფორმაციის შეკუმშვის, შენახვისა და გადაცემისათვის.

ნაკადურ ალგორითმებში ვიდეოსიგნალის კომპრესია ხორციელდება

იმის გათვალისწინებით, რომ გვერდით მდგომი კადრები თითქმის არ განსხვავდება ერთმანეთისაგან, აირჩევა და კოდირდება კარგი ხარისხის ერთი საყრდენი კადრი, შემდეგ მიმდინარეობს საყრდენსა და მიმდინარე კადრს შორის განსხვავების კოდირება, მნიშვნელოვანი განსხვავების არსებობის შემთხვევაში აირჩევა სხვა საყრდენი კადრი და პროცესი მეორდება, ალგორითმი ითვალისწინებს ობიექტის არსებობას და გამოსახულებას, მათ მდებარეობას და კადრების მიმდინარეობის დინამიკას, ამ დროს არა მარტო ძნელდება შეკუმშვის ალგორითმი, არამედ მნინელოვნად იზრდება კომპრესიის ხარისხი და შესაბამისად, ძლიერად იკუმშება ნაკადური ვიდეო [3].

ვიდეორეგისტრატორები ფლობენ მრავალამოცანიან ფუნქციას, ანუ უნარი აქვთ ერთდროულად შეასრულონ რამდენიმე ამოცანა: ვიდეოჩაწერა, მულტისურათის ასახვა, ვიდეოარქივის აღბეჭდვა, გარე მატარებლებზე ვიდეოარქივის კოპირება, კომპიუტერულ ქსელში ტრანსლირება და მართვა. გათვალისწინებულია მრავალამოცანის შემდეგი რეჟიმები:

- სიმპლექსი-ერთი ოპერაციის შესრულება (იწყება არქივის დათვალიერება, წყდება ჩაწერა).
- დუპლექსი- არქივის დათვალიერება ჩაწერის შეწყვეტის გარეშე;
- ტრიპლექსი- ერთდროულად სამი ოპერაციის შესრულება (მაგალითად ტრანსლაცია, არქივის დათვალიერება და ქსელში მუშაობა).
- პენტაპლექსი- ხუთი ან მეტი ოპერაციის შესრულება ერთდროულად.

ადამიანური ფაქტორის შემცირებისა და დაცვის ვიდეო დაკვირვების სისტემების ეფექტურობის ამაღლების მიზნით იქმნება ვიდეოდაკვირვების ინტელექტუალური სისტემები, რომელშიც ვიდეორეგისტრატორის ან სერვერის მიერ რეალიზდება ვიდეოანალიტიკის ფუნქციები, ნაკადების უმეტესობა გადაეცემა ვიდეოკამერებით, და ვიდეორეგისტრატორებში მიმდინარეობს დეკომპრესია და ანალიზი, ინტელექტუალური სისტემების ფუნქციონალობა იყოფა ორ ჯგუფად:

- ვიდეოდაკვირვების ობიექტების ამოცნობა და კლასიფიკაცია:

- ვიდეოდაკვირვების ობიექტის სავალი გზის დაკვირვება.

ვიდეოანალიზის შესაძლებლობები გამოიყენება ობიექტების დაცვისა და კონტროლის სხვადასხვა ამოცანების გადასაწყვეტად:

- ❖ ობიექტების ქცევაზე ვიდეოდაკვირვებისათვის;
- ❖ ვიდეოდაკვირვების ობიექტების დასათვლელად;
- ❖ ობიექტის მოძრაობის გზის დასადგენად.

ვიდეოანალიზის გამოყენების ერთ-ერთი გამოყენების გზაა ვიდეოდაკვირვების ობიექტების დათვლა, ობიექტზე შემსვლელი და გამომსვლელი ადამიანების განსაზღვრის ალგორითმი გვაძლევს ამომწურავ ინფორმაციას ობიექტის დაცვის მუშაობის ოპტიმიზაციისათვის.

არასანქცირებული შესვლის გარკვევა ვიდეოანალიზის საშუალებით იძლევა გავერკვეთ სიტუაციაში, როდესაც ერთი ადამიანი ბარათით აღებს კარს, ხოლო შედის რამდენიმე [2].

ობიექტის გარკვეულ ნაწილებში შესაძლებელია ადამიანთა რაოდენობის დათვლა სისტემურად, ამავე დროს სისტემა აგზავნის შეტყობინებას დიდი რაოდენობის შესახებ, როცა იქნება კრიტიკულთან მიახლოებული სიტუაციასთან მაშინ, როცა ვინმე ხელს უშლის თავისუფალ შესვლას.

2.6 თანამგზავრული ნავიგაციური სისტემები.

უკანასკნელი წლების ერთ-ერთ ყველაზე თავბრუდამხვევ ტექნოლოგიურ ნამუშევარს წარმოადგენს თანამგზავრული ნავიგაციის სფეროში არსებული მიღწევები, ამ წლების განმავლობაში თანამგზავრულმა ნავიგაციამ გადალახა გზა მეცნიერული ფაქტიდან სწრაფად განვითარებად ტექნოლოგიამდე მთელ მსოფლიოში, რომლის დროსაც იოლად და საიმედოდ განისაზღვრება ობიექტის პოზიცია რეალურ დროში [33,34,20].

ყველა თანამგზავრული ნავიგაციური სისტემები იყენებენ კოორდინატის განსაზღვრის ზოგად პრინციპებს:

- თანამგზავრები ცნობილი პოზიციიდან გადმოსცემენ სიგნალს;
- რადიოტალღების გავრცელების დროზე დაფუძნებული მიმღების

პოზიცია გამოითვლება.

რას გულისხმობენ პოზიციონირების ტერმინის ქვეშ? ეს არის დაკვირვების ობიექტების სივრცული პარამეტრების განსაზღვრის შესაძლო მეთოდების რეალიზაცია, ასეთ პარამეტრებად შეიძლება ჩაითვალოს მიმღების კოორდინატები, მისი გაადგილების სიჩქარის ვექტორი, პოზიციონირების ზუსტი დრო და ა.შ. ეს პარამეტრები წარმოადგენენ ე.წ. მომხმარებლის ვექტორს, შესაბამისად ობიექტის ადგილმდებარეობის, მისი სიჩქარის, სივრცული ვექტორის განსაზღვრა, დროის ფიქსაცია წარმოადგენენ პოზიციონირების კერძო შემთხვევას.

თანამგზავრული სისტემები იყენებენ თანამგზავრებს როგორც დროის სიგნალების გადამცემებს, ისინი ისეა განლაგებული, რომ მათ გააჩნიათ 4-მდე ატომური საათი, რომლებიც თანამდეროვე პირობებში წარმოადგენენ ყველაზე ზუსტ ინსტრუმენტს, ცდომილება 1 წამი ყოველ 30 000-1 000 000 წელში, იმისათვის, რომ ისინი გახადონ უფრო ზუსტი, ახდენენ მათ კორექციას ან სინქრონიზაცის დედამიწის რამდენიმე მართვად წერტილში. სიგნალები გადმოიცემა სინათლის სიჩქარით და შესაბამისად სჭირდებათ დაახლოებით 67,3 მ/წმ დედამიწის ზედაპირის მისაღწევად. თუ შევადარებთ თანამგზავრიდან სიგნალის მიღების დროს გაგზავნის დროსთან, შეიძლება განვსაზღვროთ ამ სიგნალის ტრანზიტის დრო. რუკაზე პოზიციის განსაზღვრისათვის საჭიროა სამგანზომილებიანი სივრცე და არა სიბრტყე, რადგან გამოთვლებისათვის აუცილებელია მესამე განზომილების გამოყენება. შესაბამისად პოზიციონირების ამოცანის წარმატებით გადაწყვეტისათვის აუცილებელია სიშორის გაზომვა, ანუ მანძილისა მიმღებსა და გადამცემს შორის. თუ ვიცით მხოლოდ მანძილი სამ გადამცემამდე, რომლებიც ერთ სიბრტყეში არიან განლაგებული, შესაძლებელია პოზიციონირების ამოცანის ცალსახად გადაწყვეტა. აშკარაა, რომ სიშორის გაზომვის შემთხვევაში მიმღები ანტენის მოქმედების მიმართულება ვერ ახდენს პოზიციონირების სიზუსტეზე გავლენას, მაგრამ გადამწყვეტი მნიშვნელობა აქვს მიმღების სინქრონიზაციის შკალების

სიზუსტეს დროში, ასვე ცდომილების სიზუსტეს, რომელიც წარმოიშვება სიგნალის გავრცელების დროის გაზომვის შემთხვევაში [19,20].

შეიქმნა სისტემა, რომელიც იყენებს თანამგზავრების სიგნალების გაყოფის ახალი მეთოდი-სიგნალის ფსევდოშემთხვევითი კოდური გაყოფა, ამ შემთხვევაში ყველა თანამგზავრი ასხივებს ერთ სიხშირეზე, რომელიც მოდელირდება ზეგრძელი ფსევდოშემთხვევითი კოდით, რომელიც თითოეული თანამგზავრისთვის ინდივიდუალურია, ასეთი სიგნალის სპექტრი ძალიან ჰგავს შემთხვევითი ხმაურის სპექტრს გაუსის ნორმალური განაწილების კანონით, საიდანაც სიგნალმა მიიღო სახელწოდება „ხმაურისმაგვარი“.

ფსევდოშემთხვევითი კოდის გამოყენება მნიშვნელოვნად აუმჯობესებს ხმაურის იმუნიტეტს და საშუალებას იძლევა სიგნალის საშუალებით გადაეცეს ინფორმაცია თანამგზავრების მდგომარეობის შესახებ, მათი დახმარებით ძალიან იოლად წყდება წვდომის შეზღუდვის ამოცანა, ზოგად შემთხვევაში კოდები შეიძლება იყოს როგორც გახსნილი საერთო სარგებლობისათვის, ასევე საიდუმლო. სამოქალაქო მომხმარებლებისათვის ნებადართულია ღია კოდები, ამიტომ საკმარისია დედამიწის სამეთაურო პუნქტიდან გაიცეს ბრძანება, რომ მუშაობისუნარიანი გახდება მხოლოდ სამხედრო მოწყობილობები, ხოლო სამოქალაქო მიმღებები მიღებული სიზუსტით შეწყვეტენ ფუნქციონირებას.

თანამგზავრული ნავიგაციის სისტემების უპირატესობა შემდეგში მდგომარეობს; პირველ რიგში ჭეშმარიტ გლობალურობას სანავიგაციო სერვისს ანიჭებს მხოლოდ თანამგზავრების გამოყენება, რადგანაც ნებისმიერ სხვა სისტემას ექნება ლოკალური ხასიათი, დედამიწისეული სადგურები შეიძლება განლაგდეს ან თავის ან მეგობრული ქვეყნის ტერიტორიაზე, საზღვაო სივრცეები საერთოდ არ ექვემდებარება დაფარვას; მეორე, იმ სადგურის გამოყენება, რომელიც დგას მიწის ზედაპირზე, ვერ ახერხებენ აუცილებელი სიზუსტით განისაზღვროს ობიექტის სიმაღლე, გარდა ამისა, თანამგზავრების გამოყენება, რომლებიც ასხივებენ

მაღალსიხშირულ სიგნალს, ეხმარება მომხმარებლის მოწყობილობას გახდეს მობილური. მობილურობა მაღლდება იმის გამო, რომ მაქსიმალურად შესაძლო ფუნქციონალური დატვირთვა გადატანილია თანამგზავრებზე და მიწიერ სადგურებზე, ხოლო მობილურმა მიმღებმა მოწყობილობამ უნდა მოახდინოს წინასწარ მომზადებული ინფორმაციის საბოლოო დამუშავება.

ამრიგად, დაცვის ვიდეო დაკვირვების სისტემების გამოყენება მნიშვნელოვნად უწყობს ხელს ობიექტის დაცვის ეფექტურობის ამაღლებას, უზრუნველყოფს სადღეღამისო ავტომატური ვიდოკონტროლის ორგანიზებას, ქმნის ვიდეოარქივებს, დარღვევის სიგნალის მიღების შემთხვევაში, დანამდვილებით დაადასტუროს შეღწევის ფაქტი, განსაზღვროს დარღვევის ხასიათი და მიიღოს აუცილებელი ზომები, უზრუნველყოს როგორც ადმინისტრაციის, ისევე ობიექტის უსაფრთხოების სამსახურის მუშაობის კომფორტულობა.

თავი 3. დაცვის ინტელექტუალური სისტემის პარამეტრების მართვის სიმულაციური მოდელი.

3.1 იდენტიფიკაციის და აუტენტიფიკაციის მეთოდები.

ნებისმიერი ინფორმაციული სისტემების დაცვის საფუძველს წარმოადგენს იდენტიფიკაცია და აუტენტიფიკაცია, რადგანაც ინფორმაციის დაცვის ყველა მექანიზმი გათვლილია სახელდებული სუბიექტებისა და ავტომატიზებული სისტემის ობიექტებთან მუშაობაზე. ამ სუბიექტების რანგში შეიძლება ვიხილოთ როგორც მომხმარებლები, ასევე პროცესები, ხოლო ობიექტებს წარმოადგენენ ინფორმაცია ან სისტემის სხვა საინფორმაციო რესურსები [27,28].

სუბიექტებისა და ობიექტებისათვის პირადი იდენტიფიკატორის წვდომის მინიჭება და მისი შედარება მოცემულ ჩამონათვალთან არის იდენტიფიკაცია, იგი უზრუნველყოფს შემდეგი ფუნქციების შესრულებას:

- ✓ ნამდვილობის დადგენასა და სუბიექტის უფლებამოსილების განსაზღვრა სისტემისადმი წვდომის დროს;
- ✓ დადგენილი უფლებამოსილებების კონტროლი მუშაობის სეანსის დროს;
- ✓ მოქმედებათა რეგისტრაცია და ა.შ,

აუტენტიფიკაცია (ნამდვილობის დადგენით) ეწოდება სუბიექტის მიერ წარმოდგენილი იდენტიფიკატორის სინამდვილის შემოწმებას ანუ ეს არის სუბიექტის შემოწმება მის ნამდვილობაზე [1].

თუ აუტენტიფიკაციის პროცესში სუბიექტის ნამდვილობა დადგენილია, მაშინ ინფორმაციის დაცვის სისტემამ უნდა განსაზღვროს მისი უფლებათა ჩამონათვალი, ეს აუცილებელია შემდგომი კონტროლისა და უფლებამოსილებათა გამიჯვნისათვის რესურსებთან წვდომის დროს.

სისტემის კონტროლირებადი კომპონენტის მიხედვით აუტენტიფიკაციის მეთოდები შეიძლება დავყოთ საკონტაქტო პარტნიორებისა და მონაცემთა წყაროს აუტენტიფიკაციად. პირველ შემთხვევაში აუტენტიფიკაცია გამოიყენება სეანსის დროს დამყარებული

შეერთების დროს, იგი ემსახურება ისეთი საფრთხეების თავიდან აცილებას, როგორიცაა შენიღბვა ან კავშირის წინა სეანსის გამეორება. მონაცემთა წყაროს აუტენტიფიკაცია კი მონაცემთა წყაროს ნამდვილობის დადასტურებაა.

მიმართულების მიხედვით აუტენტიფიკაცია არის ერთმხრივი (როდესაც მომხმარებელი ადასტურებს თავის ნამდვილობას სისტემაში შესვლისას) და ორმხრივი.

ჩვეულებრივ აუტენტიფიკაციის მეთოდები განსხვავდებიან გამოყენებული საშუალებების მიხედვით, მათ შორის მითითებული მეთოდები დაყოფილია ოთხ ჯგუფად:

1. სახით ცნობაზე დამყარებული იმ პირების მიმართ, ვისაც აქვს წვდომა სისტემის რესურსებზე;
2. უნიკალური საგნის გამოყენებაზე დამყარებული, როგორიცაა ჟეტონი, ელექტრონული ბარათი და ა.შ.
3. ადამიანის ბიომეტრული პარამეტრების გაზომვაზე დამყარებული- ცოცხალი ორგანიზმის ფიზიოლოგიურ და ყოველდღიურ ატრიბუტებზე.
4. დამყარებული იმ ინფორმაციაზე, რომელიც ასოცირდება მომხმარებელთან.

განვიხილოთ ეს ჯგუფები:

1. ყველაზე მარტივ და გავრცელებულ აუტენტიფიკაციის მეთოდს წარმოადგენს აუტენტიფიკაცია, რომელიც დამყარებულია პაროლებზე- სუბიექტების საიდუმლო იდენტიფიკატორებზე. ბოლო დროს ძალიან ფართოდ გამოიყენება ე.წ. ელექტრონული უსაფრთხოების სისტემები, რომლებსაც თავის არსენალში გააჩნიათ იდენტიფიკაციის ისეთი საშუალებები, როგორიცაა პაროლი, პლასტიკური ბარათი, გასაღები და ა.შ. ასეთი სისტემების გამოყენებაში განსხვავებული მიდგომებია კერძო ობიექტებისა და მსხვილი სახელმწიფო ობიექტების მიხედვით, სწორედ აქედან გამომდინარეობს აპარატურის საიმედობისადმი განსაკუთრებით

მაღალი მოთხოვნები, საყოველთაოდ ცნობილია რომ სისტემის საიმედობა მით უფრო დაბალია, რაც მეტი ელემენტი შედის მის შემადგენლობაში, ამიტომ საიმედობის ამაღლების ერთ-ერთი გზაა სხვადასხვა მოწყობილობათა რიცხვის მინიმუმამდე დაყვანა, ყველაზე რთული სისტემაც კი უნდა შედგებოდეს რამდენიმე ფუნქციონალურად დამოუკიდებელი ნაწილისაგან, რომლებიც მარტივია გამოყენებაში და ექსპლოატაციაში, მეორეს მხრივ არ ღირს ეკონომია გავწიოთ სისტემის აგების სტადიაზე და ვიყიდოთ უცნობი ფირმების იაფფასიანი აპარატურა, ამ სტადიაზე უფრო სჯობია აპარატურის სიჭარბე ტექნიკური და ფუნქციონალური მახასიათებლების მიხედვით, თანამედროვე დაცვის სისტემების უმრავლესობას აქვს მოდულური სტრუქტურა, რომელიც იძლევა მისი გაფართოების საშუალებას ელემენტებისა და ბლოკების დამატების გზით. მესამე და არანაკლებ მნიშვნელოვან განსხვავებას წარმოადგენს მაღალი ესთეტიკური მოთხოვნები და სამონტაჟე სამუშაობის შესრულების ხარისხი, ამ მოთხოვნების შესრულებაც გაადვილებულია სისტემის ელემენტების რიცხვის მინიმუმამდე შემცირებით [27,28,29].

3.2 აუტენტიფიკაციის საპაროლო სისტემები.

დღესდღეობით საკმაოდ ფართოდაა გავრცელებული აუტენტიფიკაციის საპაროლო სისტემები, რომლებიც საშუალებას იძლევიან ცალკეული მომხმარებლები განასხვავონ იმ უნიკალური ინფორმაციით, რომელიც ცნობილია მხოლოდ მათთვის. ეს შეიძლება იყოს სააღრიცხვო ჩანაწერის სახელი ან სპეციალურად გენერირებადი უნიკალური რიცხვითი იდენტიფიკატორები.

მომხმარებლის პაროლი-ეს არის საიდუმლო ინფორმაცია, რომელიც მხოლოდ მისთვისაა ცნობილი აუტენტიფიკაციის გავლისათვის. სისტემის რეალიზაციის მიხედვით პაროლი შეიძლება იყოს ერთჯერადი ან მრავალჯერადი. სხვა თანაბარ პირობებში ერთჯერადი პაროლების მქონე სისტემები უფრო საიმედოა, მათში გამორიცხულია იმის რისკი, რომ ვინმემ შეიძლება ისარგებლოს სხვისი პაროლით უნებართვოდ, პაროლი მოქმედია

მხოლოდ ერთ სესიაზე და თუ ლეგალურმა მომხმარებელმა უკვე ისარგებლა, დამრღვევს არ შეუძლია იგი ხელმეორედ გამოიყენოს, მაგრამ სისტემები მრავალჯერადი პაროლით მარტივად რეალიზებადია და შენახვაც იაფია, ამიტომ ისინი უფრო გავრცელებულია.

პაროლების სისტემა-პროგრამული ან პროგრამულ-აპარატურული კომპლექსია, რომელიც ასრულებს კომპიუტერული სისტემის მომხმარებლების იდენტიფიკაციისა და აუტენტიფიკაციის ფუნქციას პაროლების შემოწმების გზით, როგორც წესი იგი თავის თავში აერთიანებს მომხმარებლისა და ადმინისტრატორის ინტერფეისს, სააღრიცხვო ჩანაწერების ბაზას, უსაფრთხოების ქვესისტემებთან შესაბამისობის მოდულებს და ა.შ.

განვიხილოთ პაროლების სისტემის ადმინისტრირების ზოგიერთი რეკომენდაციები, რომლებიც გამოიყენება მრავალჯერადი პაროლების შემთხვევაში:

1. სისტემაში გამოყენებული პაროლებისათვის მინიმალური სიგრძის მინიჭება, ეს ართულებს პაროლების გამოცნობის სისტემას, რეკომენდირებულია 6-8 სიმბოლო.
2. პაროლის შემადგენლობაში სიმბოლოთა სხვადასხვა ჯგუფის არსებობა-დიდი და პატარა ასოები, ციფრები, სპეციალური სიმბოლოები, ეს ართულებს მათ გამოცნობას.
3. ადმინისტრატორის მიერ სისტემაში გამოყენებული პაროლების პერიოდული შემოწმება შეტევების იმიტაციის გზით.
4. პაროლების სიცოცხლის მაქსიმალური და მინიმალური სიცოცხლისუნარიანობის დადგენა და ძველი პაროლების იძულებითი შეცვლის მექანიზმის გამოყენება. ამ ზომის გამოყენებისას, მხედველობაში უნდა მივიღოთ ის გარემოება, რომ ადმინისტრატორისაგან შეიძლება საჭირო გახდეს დამატებითი ახსნა-განმარტებები მომხმარებლებისათვის, რას ითხოვს მათგან სისტემა [27,28,35,36].

5. წარუმატებელი შესვლის მცდელობების რაოდენობების შეზღუდვა, ეს დაიცავს სისტემას კლავიატურაზე აკრების გზით პაროლების გამოცნობის მრავალჯერადი მცდელობებისაგან, მაგრამ არსებობს იმის საფრთხეც, რომ ლეგალურ მომხმარებლებს შეცდომით შეყვანილი პაროლის გამო დაებლოკოს საკუთარი სააღრიცხვო ჩანაწერები.
6. პაროლების ისტორიის ჟურნალის შემოღება, რათა მომხმარებლებმა პაროლების იძულებითი ცვლილების გამო კვლავ არ გამოიყენონ ძველი, უკვე კომპრომეტირებული პაროლები.

მომხმარებლის-სუბიექტის მიერ შეყვანილ პაროლს აუტენტიფიკაციის ქვესისტემა ადარებს თავის პაროლს, რომელიც შენახულია მონაცემთა ბაზაში დაშიფრული სახით, დამთხვევის შემთხვევაში სისტემა ნებას რთავს სუბიექტს ავტომატიზებული სისტემის წვდომაში. პაროლთა მეთოდები შეიძლება დავყოთ პაროლების ცვალებადობის ხარისხის მიხედვით:

- მეთოდები, რომლებიც იყენებენ მუდმივ (მრავალჯერ გამოყენებად) პაროლებს;
- მეთოდები, რომლებიც იყენებენ ერთჯერად (დინამიურად ცვლად) პაროლებს;

უმრავლეს ავტომატურ სისტემებში გამოიყენება მრავალჯერადი პაროლები, ამ შემთხვევაში მომხმარებლის პაროლი იცვლება სეანსიდან სეანსამდე ადმინისტრატორის მიერ დადგენილი ხანგრძლივობის მიხედვით. ეს ამარტივებს ადმინისტრირების პროცედურას, მაგრამ ადიდებს პაროლის გატეხვის საფრთხეს. ცნობილია პაროლების გატეხვის მრავალი მეთოდი დაწყებული ზურგის მხრიდან თვალთვალით და დამთავრებული სეანსის მიტაცება-დაჭერით. პაროლის გახსნის ალბათობა იმატებს იმ შემთხვევაშიც, თუ იგი ატარებს აზრობრივ დატვირთვას (დაბადების წელი, საყვარელი ავტომობილის მარკა), არის მცირე სიგრძის, აკრებილია ერთი რეგისტრით, არა აქვს არსებობის ვადა განსაზღვრული და ა.შ. მნიშვნელობა აქვს აგრეთვე იმასაც, პაროლის შეყვანა ხდება დიალოგურ

რეჟიმში თუ მიმართვა ხდება პროგრამიდან.

უფრო საიმედოა ერთჯერადი ან დინამიურად ცვალებადი პაროლების გამოყენება.

ცნობილია პაროლური დაცვის სხვადასხვა მეთოდები, რომლებიც ეფუძნება ერთჯერად პაროლებს:

- მარტივი პაროლების სქემების მოდიფიკაციის მეთოდები;
- მეთოდი „მოთხოვნა-პასუხი“;
- ფუნქციონალური მეთოდები;

პირველ შემთხვევაში მომხმარებელს მიეწოდება პაროლების სია, აუტენტიფიკაციის დროს სისტემა მოითხოვს მომხმარებლისაგან პაროლს, რომლის ნომერიც სიაში განისაზღვრება შემთხვევითი კანონით, პაროლის სიგრძე და საწყისი სიმბოლოს რიგითი ნომერი განისაზღვრება ასევე შემთხვევითი კანონით.

„მოთხოვნა-პასუხი“ მეთოდის გამოყენების დროს სისტემა ეკითხება მომხმარებელს ზოგადი ხასიათის კითხვებს.

ფუნქციონალური მეთოდები ეფუძნება პაროლების გარდაქმნის სპეციალურ ფუნქციას f(x). იგი საშუალებას იძლევა პაროლები შეიცვალოს დროში გარკვეული ფორმულის მიხედვით, მაგრამ მითითებული ფუნქცია უნდა აკმაყოფილებდეს შემდეგ მოთხოვნებს:

- მოცემული x პაროლისათვის იოლად უნდა გამოითვალოს ახალი პაროლი y=f(x);
- თუ ვიცით x და y, ძალიან რთულია ან შესაძლებელია განისაზღვროს ფუნქცია f(x);

ფუნქციონალური მეთოდის ყველაზე ცნობილ მაგალითებს წარმოადგენს: ფუნქციონალური გარდაქმნისა და „ხელის ჩამორთმევის“ მეთოდები.

ფუნქციონალური გარდაქმნის მეთოდის იდეა მდგომარეობს თვითონ f(x) ფუნქციის პერიოდულ ცვლილებაში, რომელიც მიიღწევა ფუნქციონალურ გამოსახულებაში დინამიურად ცვალებადი პარამეტრების

არსებობით, მაგალითად თარიღისა და დროის ფუნქციის არსებობით. მომხმარებელს მიეწოდება საწყისი პაროლი, საკუთრივ ფუნქცია და პაროლის შეცვლის პერიოდულობა, რთული არაა დავინახოთ, რომ მომხმარებლის პაროლები მოცემულ n პერიოდებში იქნება x, f(x) f(f(x)), …f(x)n-1.

„ხელის ჩამორთმევის“ მეთოდი მდგომარეობს შემდეგში: პაროლების გარდაქმნის ფუნქცია ცნობილია მხოლოდ მომხმარებლისათვის და დაცვის სისტემისათვის. ავტომატიზებულ სისტემაში შესვლისას აურენტიფიკაციის ქვესისტემა ახდენს x პარამეტრის თანმიმდევრობის შემთხვევით გენერირებას, რომელიც გადაეცემა მომხმარებელს. იგი გამოთვლის y=f(x) ფუნქციის შედეგს და აბრუნებს მას სისტემაში, სისტემა თავის გამოთვლილ შედეგთან ადარებს მას და დამთხვევის შემთხვევაში მომხმარებლის ნამდვილობა ითვლება დამტკიცებულად.

ამ მეთოდის უპირატესობა იმაში მდგომარეობს, რომ რაიმე ინფორმაციის გადაცემა, რომელიც შეიძლება გამოიყენოს ბოროტმოქმედმა, დაყვანილია მინიმუმამდე[35,36].

რიგ შემთხვევებში ხშირად მომხმარებელს შეიძლება მოუწიოს დაშორებულ ავტომატიზებულ სისტემებში მოქმედი მომხმარებლის ნამდვილობის შემოწმება და სწორედ ამ დროს ყველაზე მისაღებია „ხელის ჩამორთმევის“ მეთოდის გამოყენება, რადგანაც ინფორმაციების გაცვლაში მონაწილე არც ერთი პირი არ მიიღებს არანაირ კონფიდენციალურ ინფორმაციას.

აუცილებელია აღინიშნოს რომ ერთჯერად პაროლებზე დამყარებული აუტენტიფიკაციის მეთოდები, ვერ უზრუნველყოფენ ასევე აბსოლუტურ დაცვას, მაგალითად თუ ბოროტმოქმედს ექნება საშუალება მიუერთდეს ქსელს და გაშიფროს გადაცემული პაკეტები, მაშინ მას შეუძლია გააგზავნოს ისინი როგორც საკუთარი.

იდენტიფიკაციის და აუტენტიფიკაციის თანამედროვე პროგრამულ-აპარატურული საშუალებები საიდენტიფიკაციო ნიშან-თვისებების

მიხედვით შეიძლება დავყოთ ელექტრონულ, ბიომეტრულ და კომბინირებულ საშუალებებად. ცალკე ჯგუფად შეიძლება გამოვყოთ ელექტრონულ საშუალებებში შემავალი ერთჯერადი პაროლების სისტემა.

3.3 იდენტიფიკაციის და აუტენტიფიკაციის ელექტრონული საშუალებები

ელექტრონული იდენტიფიკაციის სისტემებში საიდენტიფიკაციო ნიშნები წარმოდგენილია კოდის სახით, რომელიც ინახება იდენტიფიკატორის დაცულ მეხსიერებაში და განსაკუთრებული გამონაკლისების გარდა არ ტოვებს მას. ამ შემთხვევაში იდენტიფიკატორებს წარმოადგენენ:

- საკონტაქტო სმარტ-ბარათები;
- უკონტაქტო სმარტ-ბარათები;
- უსბ-გასაღებები

კომბინირებულ სისტემებში ხშირად გამოიყენება როგორც ერთი, ისე მეორე კლასის კუთვნილი ნიშან-თვისებები.

იდენტიფიკაციისა და აუტენტიფიკაციის ელექტრონული სისტემების შემადგენლობაში შედის კონტაქტური და უკონტაქტო სმარტ-ბარათები და უსბ-გასაღებები.

უსბ-გასაღებები მუშაობენ კომპიუტერის უსბ-პორტებთან და დამზადებულია გასაღებ-ჯაჭვის სახით-ეს არის მონაცემების შენახვისა და აუტენტიფიკაციის პერსონალური საშუალება. უსბ-გასაღებები შეიძლება დამზადებული იყოს სტანდარტული სმარტ-ბარათების სახითაც[26,27,28].

სმარტ-ბარათებს უნდა ჰქონდეთ კომპიუტერთან შეერთებისას სმარტ-ბარათების წამკითხველი მოწყობილობა, იგი შეიძლება გამოიყენებოდეს როგორც ვიზუალური იდენტიფიკაციის საშუალება, მასზე შეიძლება ინახებოდეს მფლობელის შესახებ ინფორმაცია და ფოტოგრაფია სამსახურეობრივი გამოყენებისათვის. სმარტ-ბარათები შეიძლება დამზადდეს თეთრი პლასტმასისაგან შემდგომი დაბეჭდვის მიზნით, წინასწარი ანაბეჭდით, ასევე დაწებებული მაგნიტური ზოლით ამოტვიფრული სიმბოლოებით.

უსბ-გასაღებები პირდაპირ უერთდება კომპიუტერს და ითავსებს სმარტ-ბარათისა და წამკითხველი მოწყობილობის ფუნქციებს.

თუ შევადარებთ ამ ორ ტექნოლოგიას, აშკარაა რომ ერთ-ერთის ამორჩევა დამოკიდებულია უსაფრთხოების იმ ტექნოლოგიაზე, რომელიც მიღებულია კომპანიაში. მაგალითად, თუ დაგეგმილია ავტომატური გაშვების რეჟიმის შემოღება და ამ დროს საშვებზე უნდა იყოს ფოტოსურათი, მფლობელის სახელი და სხვა ინფორმაცია, მაშინ უმჯობესია სმარტ-ბარათების გამოყენება, მაგრამ უნდა გავითვალისწინოთ, რომ ასევე დაგვჭირდება ამ ბარათების წამკითხველი მოწყობილობის შეძენაც.

თუ შესვლის რეჟიმი უკვე შემოღებულია და საჭიროა მხოლოდ დამატებითი კონტროლის ან რომელიმე შენობაში შესვლის ზომების გამკაცრება, შესაძლებელია უსბ-გასაღებების გამოყენება ჩაშენებული რადიოჭდეებით.

მათი გამოყენების ძირითადი სფეროებია:

- მომხმარებელთა ორფაქტორიანი აუტენტიფიკაცია სერვერებთან, მონაცემთა ბაზებთან, დანართებთან ვებ-საიტების დანაყოფებთან წვდომისას;
- საიდუმლო ინფორმაციის უსაფრთხო შენახვა, მათ მიეკუთვნება: პაროლები, შიფრები ციფრული სერტიფიკატებისათვის;
- ელექტრონული ფოსტის დაცვა;
- კომპიუტერების დაცვა არასანქცირებული შესვლისაგან;
- მონაცემთა გადაცემის არხებისა და ქსელების დაცვა;

მრავალფაქტორული აუტენტიფიკაციის გამოყენების დროს მომხმარებელს აქვს მთელი რიგი უპირატესობები: კერძოდ, მას უნდა ახსოვდეს გასაღების მხოლოს ერთი პაროლი, ნაცვლად დანართების პაროლებისა, ასევე დროს აღარ არის საჭირო პაროლების რეგულარული შეცვლა, უსბ-გასაღების დაკარგვის შემთხვევაშიც კი არაფერია საშიში-იმისათვის რომ ამ გასაღების მპოვნელმა ისარგებლოს, მან უნდა იცოდეს მისი პაროლი, ყველაფერი ეს მნიშვნელოვნად ამაღლებს ორგანიზაციის

უსაფრთხოების დონეს.

უკონტაქტო სმარტ-ბარათები ფართოდ გამოიყენება სხვადასხვა დამატებებში როგორც აუტენტიფიკაციისათვის (ელექტრონული შესვლის რეჟიმი, კარების ელექტრონული გასაღებები) ასევე სხვადასხვა სახის სატრანსპორტო, საიდენტიფიკაციო, გამოთვლითი და სხვა ტიპის დამატებებისათვის.

უკონტაქტო სმარტ-ბარათების მთავარი თვისება, რომლითაც იგი განსხვავდება სხვა ბარათებისაგან იმაში მდგომარეობს, რომ მას არ აქვს მექანიკური კონტაქტი იმ მოწყობილობასთან, რომელიც ახორციელებს მონაცემების დამუშავებას ბარათიდან. უკონტაქტო სმარტ-ბარათებში გამოყენებული სისტემის ტექნიკური ელემენტების ფიზიკური საიმედობა განისაზღვრება მიკროსქემების საიმედობით. ეს გარემოება მნიშვნელოვნად ამცირებს საექსპლოატაციო დანახარჯებს იმ ანალოგიურ სისტემებთან შედარებით, რომლებიც შიგა კონტაქტიან სმარტ-ბარათებს იყენებენ.

უკონტაქტო სმარტ-ბარათებთან მუშაობისას ოპერაციების თანმიმდევრობა განსაზღვრულია პროგრამის დამატებებში, ბარათის მიტანით წამკითხველთან ხდება ტრანზაქცია, ანუ მონაცემების გაცვლა წამკითხველსა და ბარათს შორის. ტრანზაქციის განხორციელებისას მაქსიმალური დაცილება ბარათსა და წამკითხველს შორის არ უნდა აღემატებოდეს 10 სანტიმეტრს, ამ დროს ბარათი შეიძლება არც ამოიღო საფულედან, ერთის მხრივ ეს მომხმარებელს საშუალებას აძლევს მოხერხებულად და სწრაფად განახორციელოს ტრანზაქცია, მეორეს მხრივ ანტენის ხედვის არეში მოხვედრილი ბარათი ჩართულია ინფორმაციის გაცვლაში მიუხედავად იმისა უნდა ეს მომხმარებელს თუ არა[27,28].

ბარათებთან მუშაობის ტიპიური თანმიმდევრობა შეიცავს შემდეგ თანმიმდევრობას:

- ბარათის დაჭერა (ამოირჩევა ხედვის არეში მყოფი პირველი წამკითხველი), აუცილებლობის შემთხვევაში ჩაირთვება ანტიკოლიზიური ალგორითმი (ეს ალგორითმი პროგრამას მიუთითებს

ბარათის უნიკალურ სერიულ ნომერს, რომელიც ჩაშენებულია ბარათის მიკროსქემაში);

- მოცემული სერიული ნომრის ბარათის ამორჩევას მასთან შემდგომი მუშაობისას;

ბრძანებათა მითითებული თანმიმდევრობა სრულდება 3 წამის განმავლობაში ანუ ელვისებურად.

ამის შემდეგ ხდება ბარათის მეხსიერების არის აუტენტიფიკაცია, თუ ბარათმა და მომხმარებელმა იცნეს ერთმანეთი, მასინ მეხსიერების მოცემული არე გაიხსნება მონაცემთა გაცვლისათვის და წვდომის პირობების მიხედვით შეიძლება შესრულდეს წაკითხვისა და ჩაწერის ბრძანებები, ასევე ელექტრონული საფულეს სპეციალიზებული ბრძანებები. მეხსიერების 16 ბაიტის წაკითხვა ხდება2,5 წამში, საფულის ბალანსის წაკითხვა და შეცვლა-9-10 წამში, ანუ მთლიანი ტრანზაქცია სრულდება 16 წამში.

3.4 კომბინირებული სისტემები.

კომბინირებული სისტემების გამოყენება მნიშვნელოვნად ზრდის საიდენტიფიკაციო ნიშნების რაოდენობას და მაღლებს უსაფრთხოებას.

დღესდღეობით არსებობს შემდეგი ტიპის საიდენტიფიკაციო სისტემები:

- კონტაქტური სმარტ-ბარატებისა და უსბ-გასაღებების ბაზაზე არსებული სისტემები;
- ჰიბრიდული სმარტ-ბარათების ბაზაზე არსებული სისტემები;
- ბიოელექტრონული სისტემები;

უსბ-გასაღების კორპუსში ჩაშენებულია ანტენა და მიკროსქემა უკონტაქტო ინტერფეისისათვის, იგი უზრუნველყოფს შენობაში წვდომის მართვას კომპიუტერთან, იყენებს რა ერთ იდენტიფიკატორს, გამოყენების ეს სქემა გამორიცხავს იმის შესაძლებლობას, როცა თანამშრომლის მიერ სამუშაო ადგილის დატოვებისას, კომპიუტერში ჩარჩენილი გასაღებით იმუშაოს სხვამ სხვისი იდენტიფიკატორით.

იდენტიფიკაციისათვის კომბინირებულ სისტემებში ხშირად გამოიყენება ერთდროულად რამდენიმე საიდენტიფიკაციო ნიშანი, ასეთი ინტეგრაცია საშუალებას იძლევა ბოროტმოქმედის წინ წარმოიქმნას დამატებითი წინააღმდეგობები, რომელსაც ის ვერ გადალახავს და თუ მაინც შეძლებს, მნიშვნელოვანი სიძნელეებით. კომბინირებული სისტემების დამუშავება მიმდინარეობს ორი ძირითადი მიმართულებით:

- ერთი კლასის სისტემების ფარგლებში იდენტიფიკატორების ინტეგრაცია;
- სხვადასხვა კლასის სისტემების ინტეგრაცია;

პირველ შემთხვევაში კომპიუტერების დაცვისათვის გამოიყენება სისტემები, რომლებიც ეფუძნება უკონტაქტო სმარტ-ბარათებისა და უსბ-გასაღებების გამოყენებას, ასევე ჰიბრიდული სმარტ-ბარათების გამოყენებას. მეორე შემთხვევაში კი წარმატებით შეათავსებენ ბიომეტრულ და ელექტრონულ იდენტიფიკაციას და აუტენტიფიკაციას.

დღესდღეობით არსებობს რამდენიმე თანამედროვე ტექნოლოგია, მათ შორის რადიოსიხშირული იდენტიფიკაცია, რომელიც ყველაზე პოპულარულია უკონტაქტო იდენტიფიკაციებს შორის, რადიოსიხშირული გამოცნობა ხორციელდება ობიექტზე დამაგრებული ე.წ. RFID-ჭდეებით, რომლებიც შეიცავენ იდენტიფიკაციის და სხვა ინფორმაციებს.

RFID-ტექნოლოგიების უპირატესობის გარდა, კომბინირებული უსბ-გასაღებები და სმარტ-ბარათები იყენებენ ერთიანი „ელექტრონული საშვის“ მექანიზმს შენობაში და ინფორმაციული რესურსების წვდომის კონტროლისათვის, რაც საშუალებას იძლევა:

- შემცირდეს ხარჯები;
- დაცული იქნას ინვესტიციები აპარატურის გაუმჯობესებისათვის, ტექნოლოგიების გაერთიანების მიზნით;
- შემცირდეს ადამიანური ფაქტორის გავლენა ორგანიზაციის ინფორმაციულ უსაფრთხოებაზე, თანამშრომელს არ შეეძლება დატოვოს შენობა, თუ მას დატოვებული აქვს კომბინირებული ბარათი სამუშაო

ადგილზე;

- მოხდეს ოფისის თანამშრომლების სამუშაო დროის ავტომატიზება;
- მოხდეს თანდათანობითი ცვლილება და ეტაპობრივი დანერგვა ახალი ტექნოლოგიების;

ჰიბრიდული სმარტ-ბარათები შეიცავენ ორგვარ მეხსიერების ბარათებს: ერთი უზრუნველყოფს კონტაქტურ ინტერფეისს, მეორე უკონტაქტოს, რის გამოც ისინი გადაჭრიან ორ ამოცანას: შენობაში შესვლისა და კომპიუტერთან წვდომის კონტროლს, ასეთი ტიპის ბარათებზე დამატებით შეიძლება დატანილ იქნას კომპანიის ლოგოტიპი, თანამშრომლის ფოტო ან მაგნიტური ზოლი, რაც საშუალებას იძლევა ჩვეულებრივი საშვები შეიცვალოს ასეთი ბარათებით და გადასვლა მოხდეს ერთიან ელექტრონულ სისტემაზე[127,35].

3.5 ბიომეტრული სისტემის აუტენტიფიკაცია და მისი ეტაპები.

ბიომეტრია-ეს არის ადამიანის პიროვნების დადასტურებისა და ავტომატური აუტენტიფიკაციის მეთოდების ერთობლიობა, რომელიც დამყარებულია ფიზიოლოგიურ და ყოფა-ცხოვრებით თავისებურებებზე. ბიომეტრულ სისტემებში იდენტიფიკაციურია ადამიანის ინდივიდუალური მახასიათებლები, რომლებსაც მოცემულ შემთხვევაში ეწოდებათ ბიომეტრული ნიშნები. ყველა ბიომეტრული სისტემა მუშაობს პრაქტიკულად ერთი და იმავე სქემით. პირველ რიგში სისტემა იმახსოვრებს ბიომეტრული მახასიათებლების ნიმუშებს, ამას ეწოდება ჩაწერის პროცესი, ამ დროს ზოგიერთი ბიომეტრული სისტემა ითხოვს რამდენიმე ნიმუშის ჩაწერას, რათა შედგენილ იქნას ბიომეტრული პარამეტრების უფრო ზუსტი სურათი.

იდენტიფიკაცია მიმდინარეობს მიღებული ბიომეტრული ნიშან-თვისებების შედარებით ბაზაში არსებულ შაბლონებთან. იმ მახასიათებლებისაგან დამოკიდებულებით, რომლებიც ამ დროს გამოიყენებიან, ბიომეტრული სისტემები იყოფა სტატიკურ და დინამიკურ სისტემებად [24,22,23].

ნებისმიერი ბიომეტრული სისტემის აუტენტიფიკაცია შეიცავს ოთხ ეტაპს: ჩაწერა-ფიზიკური ან ყოფა-ცხოვრებითი სახე დამახსოვრდება სისტემის მიერ; გამოყოფა-უნიკალური ინფორმაცია გამოიტანება ნიმუშიდან და იქმნება ახალი ნიმუში; შედარება-როდესაც მიღებული ნიმუში შეედარება წარმოდგენილს; დამთხვევა/არდამთხვევა-სისტემას გამოაქვს გადაწყვეტილება.

ბიომეტრიის გამოყენება აუტენტიფიკაციისათვის ძალიან ბევრ უნიკალურ საშუალებას უხსნის გზას, იგი ახდენს თქვენს იდენტიფიცირებას თქვენივე დახმარებით, სმარტ-ბარათები, მაგნიტურ ზოლიანი ბარათები და სხვა მსგავსი საშუალებები შეიძლება დაიკარგოს, მოიპარონ ან მოახდინონ მათი კოპირება ან უბრალოდ დაგრჩეთ სახლში, თანაც მუდმივად განვითარებადი ელექტრონული ბიზნესის პირობებში ინფორმაციებთან მუშაობის პროცესში აუცილებელია ადამიანის მიერ მრავალი შიფრებისა და საიდენტიფიკაციო ნომრების დამახსოვრება კომპიუტერისა და ბანკის ანგარიშებისათვის-ეს ძალიან რთულია, ბიომეტრია კი გთავაზობთ სწრაფ, მოხერხებულ ზუსტ და საიმედო მეთოდს და არც თუ ისე ძვირ საშუალებას გამოყენებაში. თუმცა არ არსებობს ერთადერთი ბიომეტრული ტექნოლოგია, რომელიც მიესადაგება ყველა საჭიროებას[6].

სტატიკური ბიომეტრია დამყარებულია იმ მონაცემებზე, რომლებიც მიღებულია ადამიანის ანატომიური მახასიათებლების გაზომვის შედეგად (თითების ანაბეჭდები, თვალის ბროლის მოხაზულობა და ა.შ.), ხოლო დინამიკური-ადამიანის მოქმედების ანალიზზე (ხმა, ხელმოწერის პარამეტრები, მისი დინამიკა).

ბიომეტრული სისტემები ძალიან ფართოდ არ გამოიყენებიან რამდენიმე მიზეზის გამო:

- ასეთი სისტემების ძალიან მაღალი ღირებულება;
- ასეთი სისტემის აწყობის სირთულე;

ბიომეტრული იდენტიფიკაციის დროს მონაცემთა ბაზაში ინახება

ციფრული კოდი, რომელიც ასოცირებულია კონკრეტულ ადამიანთან, ხოლო სკანერი ან სხვა მოწყობილობა, რომელიც გამოყენებულია იდენტიფიკაციისათვის, კითხულობს კონკრეტულ ბიოლოგიურ პარამეტრს, შემდეგ იგი მუშავდება გარკვეული ალგორითმით და შეედარება იმ კოდს, რომელიც ინახება მონაცემთა ბაზაში.

ბიომეტრული სკანერების უპირატესობაა ის, რომ ისინი არ არიან დამოკიდებული მომხმარებელზე და მომხმარებელს არ შეუძლია გადასცეს სხვას თავისი ბიოლოგიური იდენტიფიკატორი, პაროლისაგან განსხვავებით, ხოლო ადამიანის თითის მოხაზულობის გაყალბება პრაქტიკულად შეუძლებელია. ყველა ბიომეტრული ტექნოლოგია დაიყვანება ორ ჯგუფზე:

- სტატიკური მეთოდები, რომელიც დამყარებულია ადამიანის ფიზიოლოგიურ მახასიათებლებზე, ანუ იმ უნიკალურ თვისებებზე, რაც მას ახასიათებს დაბადებიდან და განუყოფელია მისგან, მას მიეკუთვნება ხელისგულის ფორმა, თითების ანაბეჭდები, თვალის გუგა, სახის ფორმა, ხელის მტევანზე ვენების განლაგება და ა.შ.
- დინამიური მეთოდები, რომლებიც დამყარებულია ადამიანის დინამიურ მახასიათებლებზე, განსაკუთრებულ, ადამიანის ქვეცნობიერ მოქმედებებზე, რაიმე მოქმედების პროცესში.

ადამიანის იდეალური ბიომეტრული მახასიათებლები უნდა იყოს უნივერსალური, უნიკალური, სტაბილური და კრებადი. უნივერსალობა ნიშნავს ბიომეტრული მახასიათებლების არსებობას ყოველი ადამიანისათვის. უნიკალურობაა-არ არსებობს ორი ადამიანი, რომელთაც აქვთ ერთნაირი ბიომეტრული პარამეტრები, სტაბილურობა-ამ მახასიათებლების დამოუკიდებლობა დროისაგან, კრებადობა- თითოეული ინდივიდისაგან ბიომეტრული პარამეტრების მიღების შესაძლებლობა.. რეალური ბიომეტრული მახასითებლები არა იდეალურია და ეს ზღუდავს მათ გამოყენებას, საექსპერტო შეფასების შედეგად დადგენილია, რომ არც ერთი ზემოთ ჩამოთვლილი მახასიათებლებიდან (თითების ანაბეჭდები,

ხელის გეომეტრია, ხელმოწერა, ხმის თავისებურება, ტუჩებისა და ყურების ფორმები, სიარულის მანერა) არ აკმაყოფილებს იდეალურობის მოთხოვნებს.

3.6 ამოცნობა თითის ანაბეჭდებით.

თითის ანაბეჭდების ამოცნობა არის იდენტიფიკაციის უპირატესად ადაპტური მეთოდი და გამოიყენება მრავალმხრივ, მათ შორის იმ ობიექტებშიც, სადაც ტრადიციულად გამოიყენება გასაღებები, დაშვების რუკები და პაროლები. ეს ტექნოლოგია უკვე გამოიყენება გასვლის კონტროლისათვის, ინსტრუმენტების გაცემის ავტომატებში, სასაწყობე შენობებში, ქსელური მომსახურების გაწევისას და სხვა მრავალ შემთხვევაში [35,37] .

თითის ანაბეჭდი-ეს პიროვნების უნიკალური იდენტიფიკატორია, რადგან თითების ანაბეჭდები განსხვავდება ერთმანეთისაგან, ეს საკმაოდ საიმედო მეთოდია, იგი უზრუნველყოფს დაცულობის მაღალ ხარისხს, მისი დაკარგვა ან მოპარვა შეუძლებელია, იგი ასევე ძალიან პრაქტიკულია, და ამცირებს იმ ხარჯებს, რომელიც საჭიროა შესვლის კონტროლისათვის.

ეს ყველაზე გავრცელებული სტატიკური მეთოდია ბიომეტრულ იდენტიფიკაციაში, რომლის საფუძველსაც შეადგენს თითებზე ნაოჭების მოხაზულობის უნიკალურობა თითოეული ადამიანისათვის, თითების ანაბეჭდების გამოსახულება, რომელიც მიღებულია სპეციალური სკანერით, გარდაიქმნება ციფრულ კოდად და შეედარება ადრე შეყვანილ შაბლონს (ეტალონს) ან შაბლონთა ნაკრებს (აუტენტიფიკაციის დროს). მოცემული მომენტისათვის არსებობს ანაბეჭდების სამი ტიპის სკანერი:

1. ოპტიკური
2. ნახევარგამტარული
3. ალტრაბგერითი

ყველა ეს საშუალება მუშაობს სხვადასხვა პრინციპით, მაგრამ შედეგად ღებულობენ დაახლოებით ერთსა და იმავე შედეგს, რომელიც გარკვეული მათემატიკური ალგორითმების შესაბამისად გარდაიქმნებიან საკონტროლო

ჯამის ფორმად.

ამ ტექნოლოგიის შესაძლო სირთულე შეიძლება იყოს:

- ჟელატინის ან ლატექსის ბაზაზე მულაჟის შექმნა, ასეთს შეუძლია იმუშაოს მარტივ სკანერებზეც.
- გამოსავალი: მრავალფაქტორიანი სკანერის გამოყენება, რომელიც აფიქსირებს ტემპერატურას და ოფლიანობას.
- სიგნალის მიტაცება, თუ სკანერი ძირითად სისტემას უკავშირდება გამტარი ინტერფეისით;
- გამოსავალი: სიგნალების გადაცემისას კრიპტოგრაფიის მეთოდების გამოყენება.
- კონდენსაცია (თბილი ჰაერის ნაკადის მიმართვა სკანერზე და შედეგად უკანასკნელი ანაბეჭდის აღდგენა).
- გამოსავალი: პრობლემა არსებობს მხოლოდ იაფი ოპტიკური სკანერებისათვის.

დღევანდელ პირობებში ამოცნობა თითის ანაბეჭდებით სრულდება ძალიან სწრაფად, ტექნოლოგია იმდენად სრულყოფილია, რომ იდენტიფიკაციის დრო იზომება წამის მეასედი ნაწილებთ, განსაკუთრებით ეფექტურია ელექტრო წამკითხველები, რომლებიც საოცრად სწრაფად ახდენენ ანაბეჭდების იდენტიფიცირებას.

ტექნოლოგიის საიმედოობა ძალიან მაღალ დონეზეა- პრაქტიკულად ყველა ანაბეჭდი შეიძლება იყოს ამოცნობილი, მიუხედავად ასეთი მაღალი საიმედობისა, როცა ამოცნობის ხარისხი უტოლდება თითქმის 100%-ს, უახლოეს წლებში მაინც არ არის იმის იმედი, რომ ნებისმიერი ანაბეჭდი იქნება ამოცნობილი. მაგალითად, იმ ხალხისათვის, რომლებიც მუშაობენ გარკვეულ სფეროებში, მაგალითად ქიმიურ წარმოებაში და კანი განიცდის მავნე ნივთიერებების ზემოქმედებას, დაზიანების ხარისხი შეიძლება გახდეს ამოცნობის ხელის შემშლელი ფაქტორი, ერთჯერადი დაზიანებისასთითის ანაბეჭდების აღდგენა შეიძლება და ეს არ მოქმედებს ამოცნობის სიზუსტეზე.

3.7 ამოცნობა ხელის ფორმით.

მოცემული სტატიკური მეთოდი დამყარებულია ხელის მტევნის გეომეტრიის ამოცნობაზე, რომელიც ასევე წარმოადგენს ადამიანის უნიკალურ ბიომეტრიულ მახასიათებელს, სპეციალური მოწყობილობის მიხედვით, რომელიც იძლევა ხელის მტევნის სამგანზომილებიან გამოსახულებას (ზოგიერთი სკანერები ახდენენ რამდენიმე თითის ფორმის სკანირებას), ტარდება გაზომვები, რომლებიც საჭიროა უნიკალური ციფრული მწკრივის მისაღებად, რომლითაც ხდება ადამიანის იდენტიფიცირება [35, 36,37,38].

მსგავსი ბიომეტრული სისტემები ყურადღებას ამახვილებენ ადამიანის ხელისგულზე ხუთ ძირითად ხაზზე და ჩვიდმეტ სხვა გეომეტრიულ პარამეტრზე.

ძირითადი ნიშნებია: ხელისგულის სიფართე, ხელისგულში ჩახაზული წრეწირის რადიუსის სიგრძე, თითების სიგრძე და ხელის მტევნის სიმაღლე. ეს არის საწყისი პარამეტრები და ისინი განისაზღვრება პირველ რიგში. ამ მეთოდის მინუსი არის ის, რომ არ არის საიმედობის მაღალი სტანდარტი, რადგან ანაბეჭდების ნიმუშები შეიძლება დამზადდეს ძალიან იოლად სხვების მიერაც.

მეორე, უფრო თანამედროვე და სიხშირული მეთოდი დამყარებულია ფალანგის ნახვევების გეომეტრიაზე და სისხლგამტარი არხების განლაგებაზე. უნდა აღინიშნოს, რომ ვენების სურათიც ისეთივე უნიკალურია, როგორც თითების ანაბეჭდები. თვითონ მეთოდი გულისხმობს ხელის ზურგის ინფრაწითელ სკანირებას, მის შედეგი არ არის დამოკიდებული დაბინძურებაზე ან კანის დაზიანებებზე, თანც ეს ძალიან სწრაფი საშუალებაა, ხოლო შემდგომი იდენტიფიკაცია ვითარდება ჩვეულებრივი სქემის მიხედვით: მიღებული ნიმუშის გარდაქმნა ციფრულ ფორმატში-შედარება ეტალონთან-გადაწყვეტილება დაშვებაზე.

და ბოლოს, მესამე საშუალება ხელის გეომეტრიისათვის-3D-სკანირება, იგი იყენებს ჩვეულებრივ პარამეტრებს. მაგრამ აქვს დაცულობის

და საიმედობის ძალიან მარალი ხარისხი ხელის სამგანზომილებიანი სკანირების, მიღებული ინფორმაციის შემდგომი გასაშუალების და ხელის 3D-გამოსახულების კომპიუტერული მოდელირების გამო.

3.8 თვალის ირისის გარსის მოხაზულობით ამოცნობა.

ამოცნობის მოცემული მეთოდი დამყარებულია თვალის ირისის ნახატის უნიკალურობაზე, ამ მეთოდის რეალიზაციისათვის აუცილებელია კამერა, რომელიც საშუალებას იძლევა მივიღოთ თვალის ირისის გამოსახულება მაღალი გარჩევადობით და სპეციალური პროგრამული უზრუნველყოფა, რომელიც მიღებული გამოსახულებიდან გამოყოფს თვალის ირისის გამოსახულებას, რის მიხედვითაც აიგება ადამიანის იდენტიფიცირებისათვის საჭირო ციფრული კოდი [35, 36,37,38].

გამოსახულების პირველადი დამუშავების დრო თანამედროვე სისტემებში 300-500 მწმ-ია, შედარების სიჩქარე 50000-150000 შედარება წამში, შედარების ეს სისწრაფე არ ზღუდავს მის გამოყენებას დიდ ორგანიზაციებში შესვლის ნებართვების გამოყენებისას. მისი უპირატესობაა ალგორითმის სტატიკური საიმედობა, გამოსახულების დაფიქსირება შეიძლება რამდენიმე სანტიმეტრიდან რამდენიმე მეტრამდე, თანაც ადამიანის ფიზიკური კონტაქტი მოწყობილობასთან არ ხდება, თვალის ირისი დაცულია დაცულია დაზიანებისაგან და რა თქმა უნდა არ შეიცვლება დროის მიხედვით. მეთოდის ნაკლია სისტემის ფასი, აპარატურა, რომელიც საჭიროა ამ მეთოდისათვის, ძალიან ძვირია.

3.9 ამოცნობა სახის ფორმის მიხედვით

ამოცნობის ამ სტატიკური მეთოდის მიხედვით აიგება ადამიანის სახის ფორმის ორ ან სამგანზომილებიანი გამოსახულება, კამერისა და სპეციალიზებული პროგრამული უზრუნველყოფის მიხედვით სახეზე გამოიყოფა წარბების, თვალის, ცხვირის და ტუჩების კონტურები, გამოითვლება მანძილები მათ შორის და სხვა პარამეტრები-გამოყენებული ალგორითმის მიხედვით. ამ მონაცემების მიხედვით შეიქმნება სახე,

რომელიც გარდაიქმნება შედარებისათვის საჭირო ციფრულ ფორმად. თანაც რაოდენობა, ხარისხი და მრავალფეროვნება შეიძლება იცვლებოდეს იმ ალგორითმებისა და სისტემის ფუნქციის მიხედვით, რომლითაც რეალიზებულია მოცემული მეთოდი [35, 36,37,38].

ეს მეთოდი ფართოდ გამოიყენება კრიმინალისტიკაში, რაც განაპირობებს მის განვითარებას, არსებობს მეთოდის კომპიუტერული ინტერპრეტაციები, რითაც ის გახდა ბევრად უფრო საიმედო.

თანამედროვე პირობებში უფრო ხშირად გამოიყენება სახის ამოცნობა 3D მეთოდით, ეს ძალიან რთულია, მაგრამ მიუხედავად ამისა, არსებობს უამრავი მეთოდი, რომლებიც იყენებენ სხვადასხვანაირ სკანერებსა და ბაზებს.

3.10 ამოცნობა ნაწერის მიხედვით

როგორც წესი ადამიანის ამოცნობის ამ დინამიური მეთოდის მიხედვით გამოიყენება მისი ნაწერი ან კოდური სიტყვის წერის მანერა.

იდენტიფიკაციის ციფრული კოდი ყალიბდება ნაწერის დინამიური მახასიათებლების მიხედვთ, ანუ იდენტიფიკაციისათვის აიგება მწკრივი, რომელშიც შედის ინფორმაციია ნაწერის გრაფიკული პარამეტრების შესახებ, დროებითი მახასიათებლებისა და რეჟიმის დინამიკის შესახებ.

ამ მეთოდისათვის არსებობს ამოცნობის ორი ძირითადი მიმართულება_ამოცნობა სტატიკური (ე.წ. მკვდარი) ნაწერით და მისი დინამიური მახასიათებლების ანალიზი.

თუ გვაქვს გრაფიკული პლანშეტი, შეგვიძლია მივიღოთ ნაწერის ორ ან სამგანზომილებიანი გამოსახულება, დღესდღეობით არ არსებობს არც ორ და არც სამგანზომილებიანი ნაწერების ამოცნობის უნივერსალური მიდგომა, ამიტომ „მკვდარი“ ნაწერის ამოცნობის ამოცანა არ არის გადაჭრილი სრულფასოვნად [37,38].

3.11 ამოცნობა სახის ფორმის მიხედვით

ამოცნობის ამ სტატიკური მეთოდის მიხედვით აიგება ადამიანის სახის ფორმის ორ ან სამგანზომილებიანი გამოსახულება, კამერისა და სპეციალიზებული პროგრამული უზრუნველყოფის მიხედვით სახეზე გამოიყოფა წარბების, თვალის, ცხვირის და ტუჩების კონტურები, გამოითვლება მანძილები მათ შორის და სხვა პარამეტრები-გამოყენებული ალგორითმის მიხედვით. ამ მონაცემების მიხედვით შეიქმნება სახე, რომელიც გარდაიქმნება შედარებისათვის საჭირო ციფრულ ფორმად. თანაც რაოდენობა, ხარისხი და მრავალფეროვნება შეიძლება იცვლებოდეს იმ ალგორითმებისა და სისტემის ფუნქციის მიხედვით, რომლითაც რეალიზებულია მოცემული მეთოდი.

ეს მეთოდი ფართოდ გამოიყენება კრიმინალისტიკაში, რაც განაპირობებს მის განვითარებას, არსებობს მეთოდის კომპიუტერული ინტერპრეტაციები, რითაც ის გახდა ბევრად უფრო საიმედო [35, 36,37,38].

თანამედროვე პირობებში უფრო ხშირად გამოიყენება სახის ამოცნობა 3D მეთოდით, ეს ძალიან რთულია, მაგრამ მიუხედავად ამისა, არსებობს უამრავი მეთოდი, რომლებიც იყენებენ სხვადასხვანაირ სკანერებსა და ბაზებს.

3.12 ამოცნობა კლავიატურაზე აკრების მიხედვით

ეს მეთოდი ზემოთ აღწერილის ანალოგიურია, მხოლოდ ხელმოწერის მაგიერ გამოიყენება რაიმე კოდური სიტყვა, ხოლო მოწყობილობებიდან აუცილებელია მხოლოდ სტანდარტული კლავიატურა. ძირითადი მახასიათებელი, რომლიდანაც მოიცემა იდენტიფიკაციის მწკრივი არის კოდური სიტყვის აკრების დინამიკა.

თანამედროვე კვლევების მიხედვით კლავიატურაზე ბეჭდვა ხასიათდება გარკვეული სტაბილურობით, რის გამოც ცალსახად შეიძლება ამოვიცნოთ პიროვნება, გამოიყოფა მომხმარებლის შემდეგი

მახასიათებლები:

- აკრების პროცესში შეცდომების რაოდენობა;
- კლავიშებზე დაჭერებს შორის ინტერვალი;
- აკრების სიჩქარე;
- კლავიშზე დაჭერის დრო;
- არითმულობა აკრებისას;

კომპიუტერის კლავიატურაზე დარტყმების დინამიკა აანალიზებს ბეჭდვის მეთოდს ამა თუ იმ ფრაზისას. არსებობს ამ ტიპის ორი მეთოდი, პირველი დამყარებულია მომხმარებლის აუტენტიფიკაციაზე გამოსათვლელ რესურსებზე წვდომის მიღების მცდელობაზე, ხოლო მეორე ახორციელებს მონიტორინგს უკვე წვდომის მიღების შემდეგ და ბლოკავს სისტემის მუშაობას იმ შემთხვევაში, თუ მუშაობს არა ის ადამიანი, ვინაც მიიღო წვდომა. კლავიატურაზე მუშაობის რიტმი წარმოადგენს მომხმარებლის საკმარისად ინდივიდუალურ მახასიათებელს და სრულად გამოყენებადია იდენტიფიკაციისა და აუტენტიფიკაციისათვის, რიტმის გაზომვისათვის ფასდება დროის ინტერვალები ან დარტყმებს შორის, ან იმ სიმბოლოების ბეჭდვისას, რომლებიც განლაგებული არიან გარკვეული მიმდევრობით, ან იმ მომენტებს შორის დროის ინტერვალი კლავიშზე დარტყმისა და აშვების მომენტს შორის, მართალია მეორე მეთოდი უფრო ეფექტურია, მაგრამ ყველაზე კარგი შედეგი მიიღწევა მათი ერთობლივი გამოყენებისას [35.38].

3.13 ამოცნობა ხმისა და მეტყველების თავისებურებათა მიხედვით

ამ ბოლო დროს ამ უძველესი ტექნოლოგიის განვითარება დაჩქარებულია, რადგანაც განიხილება მისი ფართო გამოყენება ინტელექტუალური შენობების აგებაში, არსებობს ხმის იდენტიფიკაციის მიხედვით კოდების აგების მრავალი მეთოდი, რაც განპირობებულია ხმის სიხშირული და სტატისტიკური მახასიათებლების შერწყმით. მაგრამ უნდა გავითვალისწინოთ, რომ სტატისტიკური მახასიათებლებით იდენტიფიკაცია უფრო სანდოა, რადგანაც არ არის დამოკიდებული

იდენტიფიცირების ობიექტის ფსიქოემოციურ მდგომარეობაზე.

ამ ტიპის აუტენტიფიკაციის ძირითადი პრობლემებია:

1. ხმის შეცვლა (ემოცია, ჯანმრთელობის მდგომარეობა)
2. ხმაური მიკროფონში ან კავშირის ხაზებში.
3. ბოროტმოქმედის მიერ კონფიდენციალური ინფორმაციის მიტაცება

ხმის მიხედვით იდენტიფიკაციის დროს მთავარია იმ პარამეტრების არჩევა, რომლებიც უკეთესად აღწერენ ხმის ინდივიდუალობას, მათ ინდივიდუალურობის ნიშნები ეწოდება. ეს ნიშნები, ხმის თავისებურობების მონაცემების გარდა, უნდა შეიცავდნენ სხვა მონაცემებსაც. მაგალითად, ისინი ადვილად გაზომვადი ან ხმაურზე ნაკლებად დამოკიდებულნი უნდა იყვნენ. ასევე ისინი უნდა იყვნენ სტაბილური დროში და ეწინააღმდეგებოდნენ იმიტაციას [35, 36,37,38].

3.14 დნმ-ის ანალიზზე აგებული ტექნოლოგიები

იმ ტექნოლოგიების სპექტრი, რომლებიც შეიძლება გამოიყენებოდეს უსაფრთხოების სისტემებში მუდმივად ფართოვდება, მთელი რიგი ბიომეტრული ტექნოლოგიებისა დამუშავების სტადიაშია, მათგან ზოგიერთი ითვლება მეტად პერსპექტიულად, მაგალითად:

1. სახის თერმოგრამები, გამოსხივების ინფრაწითელ დიაპაზონში.
2. დნმ-ის მახასიათებლები
3. კლავიატურული ნაწერი
4. კანის სტრუქტურის ანალიზი
5. ხელისგულების ანაბეჭდების ანალიზი
6. ყურის ნიჟარების ანაბეჭდების ანალიზი
7. ადამიანის სიარულის მანერის ანალიზი
8. ადამიანის ინდივიდუალური სუნის ანალიზი
9. კანის დამარილების დონის მიხედვით ამოცნობა
10. ვენების განლაგების მიხედვით ამოცნობა.

თერმოგრამის აგებისა და ანალიზის ტექნოლოგია წარმოადგენს ბიომეტრიაში უკანასკნელ მიღწევას, როგორც აღმოჩნდა ინფრაწითელი

კამერების გამოყენებამ მოგვცა სახის კანის ქვეშ არსებული ობიექტების უნიკალური სურათი, ძვლის, ცხიმის და სისხლგამტარი არხების სხვადასხვა სიმკვრივე ინდივიდუალურია და განსაზღვრავს მომხმარებლის თერმოგრაფიულ სურათს. სახის თერმოგრამა უნიკალურია და დამაჯერებლად არჩევს თუნდაც ძალიან მსგავს ტყუპებსაც კი ერთმანეთისაგან, მათი დამატებითი თვისებებისაგან შეიძლება გამოვყოთ მისი ინვარიანტულობა და დამოკიდებულება ნებისმიერ კოსმეტიკურ ან კოსმეტოლოგიურ ცვლილებებთან, მათ შორის პლასტიკურ ქირურგიასთან და მაკიაჟის გამოყენებასთან.

დნმ-ის ანალიზზე აგებული ტექნოლოგიები არის ყველაზე ხანგრძლივი, მაგრამ ამავე დროს ყველაზე პერსპექტიული და საიმედო იდენტიფიკაციების მეთოდებისგან. ის დამყარებულია იმაზე, რომ ადამიანის დნმ-ში არსებობს პოლიმორფული ქრომოსომები, მათი კომბინაციების განსაზღვრა რამდენიმე პოლიმორფული ქრომოსომისათვის საშუალებას იძლევა კონკრეტულ ადამიანზე მივიღოთ გენური სურათი, რომელიც დამახასიათებელია მხოლოდ ამ კონკრეტული ადამიანისათვის. ამ მეთოდის სიზუსტე დამოკიდებულია გაანალიზებული ადამიანების ხასიათსა და რაოდენობაზე და დღესდღეობით მიღწეულია შედეგი 1 მილიონ ადამიანზე ერთი შეცდომა [37,38].

მიუხედავად ამისა, ზემოთ აღწერილ ბიომეტრულ მეთოდებს აქვთ ნაკლოვანებებიც, რომელთაგან შეიძლება აღინიშნოს შემდეგი:

პირველ რიგში ბიომეტრული სკანერების ნაკლოვანებები, რა თქმა უნდა ისინი მრავალია ან ისევე როგორც სკანერთა ტიპები, მაგრამ მათ აერთიანებთ ის, რომ ისინი არსებობენ. მაგალითად თითების ანაბეჭდების სკანერები შეიძლება იყოს ოპტიკური და ელექტრონული. ოპტიკური სკანერები უზრუნველყოფენ უფრო ხარისხიან გამოსახულებას, მაგრამ მალე ჭუჭყიანდებიან და აქვთ დიდი მოთხოვნები ხელის სისუფთავესთან, ელექტრონულები-უფრო ნაკლებად საიმედო და ხარისხიანია, მაგრამ შეუძლიათ ჭუჭყიანი ხელების ამოცნობაც კი. ამიტომაც შეიძლება

დავასკვნათ, რომ თითოეული კონკრეტული შემთხვევისათვის ბიომეტრული ტექნოლოგია შეიძლება შეირჩეს სხვადასხვანაირად.

მეორეც, ეს უაღრესად რთულად დასალაგებელი მოწყობილობაა, სადაც თითოეული შემთხვევისათვის დადგენილი უნდა იყოს შეცდომის ზღვრული მნიშვნელობა, როგორიცაა მცდარი მტყუნებების პროცენტი, სისტემაში დაურეგისტრირებელი ადამიანის დაშვების ალბათობა. მგრძნობელობის ბარიერი წარმოადგენს წარმოადგენს იდენტიფიცირების თავისებურ საზღვარს. თუ ადამიანს აქვს რომელიმე მახასიათებლისათვის ზომაზე მეტი მსგავსება, დაშვებული იქნება სისტემაში ან პირიქით. ბარიერი ადმინისტრატორმა შეიძლება შეცვალოს თავისი შეხედულების მიხედვით, რაც წარმოადგენს მისთვის ძალიან მაღალ მოთხოვნას, რადგანაც მოსახერხებლობასა და საიმედობას შორის ბალანსის დაცვა მოითხოვს დიდ ძალისხმევას.

მესამეც, ბიომეტრული სისტემების დანერგვისას შეიძლება წარმოიშვას წინააღმდეგობა კომპანიის თანამშრომლების მხრიდან, რაც გამოწვეული შეიძლება იყოს მათი პრეტენზიებით სამუშაო დროის გაკონტროლების გამო, მით უმეტეს რომ თანამშრომელთა სამუშაო დროის კონტროლის სისტემები ისედაც არსებობენ.

მაგრამ ბიომეტრული კამერების გამოყენება შეუძლებელია ფიზიკური ნაკლის მქონე ადამიანების იდენტიფიკაციისათვის. მაგალითად თვალის ბადურის სკანირება შეუძლებელია იმ ადამიანებისათვის, ვინც ატარებს სათვალეებს ან კონტაქტურ ლინზებს, ხოლო ართრიტით დაავადებულ ადამიანებს უჭირთ თანაბრად გააჩერონ თითი სკანერზე ანაბეჭდის ასაღებად[8].

კიდევ ერთი პრობლემაა სიმაღლე, სახის სკანირება შეიძლება გაძნელდეს, თუ ადამიანის სიმარლე 1,55 მ-ზე დაბალია ან 2,1 მ-ზე მაღალია, ბოროტმოქმედებს ადვილად შეუძლიათ მოატყუონ ბიომეტრული სისტემები, ზოგიერთები ცვლიან თავის თავიანთი თითების ანაბეჭდებს ან წვავენ მათ მჟავით, არის აგრეთვე უნებური შემთხვევები, მაგალითად

ხალხი დასახიჩრებული ხელებით.

ამრიგად, შეიძლება ითქვას, რომ მიუხედავად იმისა, რომ ბიომეტრული ტექნოლოგიები გამოიყენება უკვე 20 წელია, მაინც ძალიან დიდი ყურადღება ექცევა მის სრულყოფასა და განვითარებას, მთელი რიგი კვლევებისა და დაკვირვებების მიხედვით ევროპაი გამოყოფენ სამ სფეროს, სადაც ისინი სასურველია გრძნობდნენ თავს უფრო დაცულად:

1. გადაადგილება ტრანსპორტით, მოგზაურობა
2. ფინანსური ოპერაციები
3. პერსონალური მონაცემები.

ბიომეტრული მონაცემების დაცვა წარმოადგენს ძალიან მნიშვნელოვან პრობლემას და იგი ძალიან ხშირად განიხილება ყველაზე მაღალ დონეზე აქტიური ტექნოლოგიური სამუშაოები მიმდინარეობს როგორც ბიომეტრული მონაცემების ანალიზის სრულყოფის მიზნით, ასევე მათი წაკითხვისა და დამუშავების კუთხით.

ყველა ეს საშუალება მიმართულია იქეთ, რომ შენობებისა და ოფისების უსაფრთხოების სისტემები იყოს მაქსიმალურად საიმედო, ამიტომ აუცილებელია იგი იყოს აწყობილი თანამედროვე ტექნოლოგიებით.

დაცვის სისტემების ტექნოლოგიების განვითარების ტენდენციებმა საფუძველი დაუდო არსებული უსაფრთხოების სისტემების გარდაქმნას სხვადასხვა მოწყობილობათა სერიოზულ კომპლექსებად, რომლებიც იქმნება სპეციალურად სამრეწველო ობიექტების დაცვისათვის, მაგრამ მიზნობრივ ჯგუფებში შედიან აგრეთვე სხვა ობიექტებიც, მაგალითად კომერციული უძრავი ქონება, ოფისები, ქალაქგარე სახლები, კოტეჯები. დაცვის სისტემებს საჭიროებენ აგრეთვე სავაჭრო დაწესებულებები და ეს მათი ფუნქციონირების მთავარი პირობაა. უსაფრთხოებაზე ზრუნვა სარგებლობს დიდი მოთხოვნილებით და დაცვის სისტემების სხვდასხვა სახეობები ძალიან პოპულარულია, ეს აიხსნება არა მარტო სერიოზული გარემოებებით,, რომლებიც შექმნილია დღესდღეობით, არამედ ახალი

სისტემების მაღალი ეფექტურობით ზომიერი დანახარჯების პირობების გათვალისწინებით. მსხვილი საოფისე და სავაჭრო ცენტრებში, დიდ ქალაქებში გაცილებით მცირე რაოდენობის დანაშაულები ხდება, თუ ისინი აღჭურვილია თანამედროვე კომპლექსური დაცვის სისტემებით.

3.15 ვიდეო დაკვირვების ციფრული კომპლექსები

ახალი დაცვის სისტემის აწყობა მოითხოვს დიდ შრომასა და გამოცდილებას, აგრეთვე წინასწარ რაღაც დონეზე გარკვეული მახასიათებლების ცოდნას, თუ როგორ უნდა იმუშაოს და რა მოთხოვნები წაეყენება ასეთ სისტემას, მაგრამ ხშირია შემთხვევები, როდესაც უკვე აწყობილი მოწყობილობა გამოუცდელობის ან რაიმე „ფორს-მაჟორული“ გარემოებების გამო გამოდის მწყობრიდან[5].

თანამედროვე უსაფრთხოებისა და ვიდეოდაკვირვების სისტემები უნიკალურ შესაძლებლობას იძლევიან მთლიანად გაკონტროლდეს სიტუაცია დასაცავ ობიექტზე, ეს ამცირებს ობიექტზე შეღწევის რისკს და გვაძლევს მაქსიმალურად ეფექტური რეაგირების საშუალებას, კომპლექსური უსაფრთხოების უზრუნველყოფის მიზნით შექმნილ სისტემემები აღჭურვილია ელექტრონული შეტყობინების მოდულებით, რომლებსაც დროულად შეუძლიათ მიაწოდონ ინფორმაცია ობიექტის შესახებ შესაბამის მორიგე სამსახურებს: დაცვას, პოლიციას ან სახანძროს [7,19,].

გარდა ამისა, უსაფრთხოებისა და ვიდეოდაკვირვების ბევრი სისტემა საშუალებას იძლევა დიდი მანძილიდან გააკონტროლოს მდგომარეობა ობიექტზე, პლანეტის ნებისმიერი წერტილიდან შესაძლებელია თვალყური ვადევნოთ და ვმართოთ უსაფრთხოების სისტემის მუშაობის რეჟიმები და ადვილად შევიტანოთ მასში ცვლილებები, რომლებიც ადეკვატური რეაგირების საშუალებას იძლევა.

ის საკითხი, თუ რომელი უსაფრთხოების სისტემა მიესადაგება კონკრეტულ ობიექტს, შეიძლება ცალსახად განისაზღვროს მხოლოდ იმ ამოცანებიდან გამომდინარე, რაც დგას ობიექტის დაცვის წინაშე.

დასაყენებელი მოწყობილობების ფუნქციონალური დატვირთვა უნდა განისაზღვროს წინასწარ, რათა საბოლოო მონტაჟამდე განისაზღვროს ის კომპლექტაცია და ადგილი, რომელიც საჭიროა სხვადასხვა სისტემების მოწყობილობებისათვის.

ვიდეოდაკვირვების ციფრული კომპლექსები -დაცვის ორგანიზების ერთ-ერთი ვარიანტია, მათი გამოყენების ძირითადი სფეროებია განსაკუთრებით მნიშვნელოვანი ობიექტები და დიდი ტერიტორიები, სადაც შენობები ერთმანეთისაგან შორს არიან განლაგებული, მათი განმასხვავებელი თავისებურებაა საშუალებაა ფართო სპექტრი, რადგანაც ინფორმაციის გადაცემა და ხარისხიანი გამოსახულების მიღება ნებისმიერ მანძილზე მოითხოვს სპეციალურ პროგრამულ უზრუნველყოფასა და დამატებით მოწყობილობებს.

თავი 4. ავტომატური პროექტირების სისტემები.

4.1. პროექტირების სისტემა Quartus II.

სპეციალიზებული ციფრული მოწყობილობების შესაქმნელად უკვე დიდი ხანია იყენებენ მაღალტექნოლოგიურ ბაზას-პროგრამირებად ლოგიკურ ინტეგრალურ სქემებს, სპეციალიზებული კონტროლერების, კომუნიკაციის სისტემების, სიგნალების ციფრული დამუშავების სფეროში და ა.შ. განსაკუთრებით მათი გამოყენება აქტუალურია მაღალი მწარმოებლურობის ისეთი სქემების რეალიზებისას, რომლებიც ორიენტირებულნი არიან აპარატურულ რეალიზაციაზე. სხვადასხვა სახის ამოცანების აპარატურული რეალიზაცია უზრუნველყოფს პროცესის განპარალელებას და და შესაბამისად ამაღლებს მწარმოებლურობას პროგრამულ გადაწყვეტასთან შედარებით.

სპეციალიზებული ციფრული მოწყობილობის შექმნისას QuartusII სისტემის გამოყენებისას სქემის შემქმნელი მიუთითებს საჭირო მოწყობილობას და ღებულობს პროგრამირებად ფაილს, რომელიც შემდგომში გამოიყენება პროგრამირებადი ლოგიკური სქემის კონფიგურაციისათვის, პროგრამირებაში იგულისხმება ფუნქციონალური გარდამქმნელებისათვის სპეციალური ფუნქციის მინიჭება და მათ შორის აუცილებელი კავშირის დამყარება. დიდი ინტეგრალური სქემის გამოყენება უზრუნველყოფს აგრეთვე მოდიფიკაციის ისეთ მოქნილობას, როგორიცაა პროგრამული გადაწყვეტილებების დროს.

ავტომატური პროექტირების სისტემა QuartusII-ი უზრუნველყოფს შემდეგ ძირითად ფუნქციებს:

— მოწყობილობათა ქცევისა და სტრუქტურის აღწერის სხვადასხვა მეთოდებს;

— რთული პროექტებისატვის დახმარების ინტეგრირებული საშუალებათა შექმნას;

— სინთეზის ქვესისტემებს;

— ინტეგრალური სქემების განლაგებისა და რესურსების ქვესისტემას;
— მოდელირების ქვესისტემის შექმნას;
— მოხმარებული ენერგიის ანალიზისა და დროითი ანალიზის შექმნას;
— დიდი ინტეგრალური სქემების პროგრამირების ქვესისტემის არსებობას;
— პროექტის სწრაფქმედებისა და ოპტიმიზაციის ქვესისტემის შექმნას;
— სიგნალების ციფრული დამუშავების ბლოკების შექმნას;
— IP-მოდულების მხარდაჭერის გამოყენებას;
— ოპერაციული სისტემების Windows, Solaris და Linux-ის მხარდაჭერას;
— ლიცენზირების სხვადსხვა სქემების მხარდაჭერას;

ელემენტების განლაგებისა და შეერთების ტრასირების ტექნოლოგია ამ სისტემაში იყენებს შემქმნელის მიერ მიწოდებულ დროით ინტერვალებს, სქემის ოპტიმალურად შედგენისა და ლოგიკური ელემენტების განლაგებისათვის, ამიტომ ყველაზე განსაკუთრებული ყურადღება უნდა დაეთმოს ისეთ შეერთებებს, რომლებიც კრიტიკულია დროითი პარამეტრების მიმართ, სწორედ მათი ოპტიმიზირება ხდება პირველ რიგში, დაყოვნების მაქსიმალური შემცირებისა და მაქსიმალური მწარმოებლურობის მისაღწევად (f_{max}), მისი შემდგომი გაუმჯობესება მიიღწევა უახლესი არქიტექტურის გამოყენებით, როგორიცაა Stratix, რის გამოც Quartus II აღწევს მაქსიმალურ მწარმოებლურობას და ყველაზე მცირე დროს საჭიროებს პროექტის კომპილაციისათვის სხვა მსგავს სისტემებთან შედარებით.

4.2 პროექტირების სისტემა LabVIEW

პროექტირების სისტემა LabVIEW- გრაფიკული პროგრამირების სივრცეა, რომელსაც იყენებენ გაზომვის, გამოცდის, სამეცნიერო და პრაქტიკული ექსპერიმენტების მართვის ამოცანების სწრაფი გადაწყვეტისათვის. ტრადიციული ტექსტური პროგრამირების ენებთან შედარებით გრაფიკული პროგრამირების ენა და მისი კონცეფცია საშუალებას იძლევა უფრო ეფექტურად გადაიჭრას ბევრი რთული ამოცანა. პროექტირების სისტემა LabVIEW-ს საფუძვლად უდევს გრაფიკული

პროგრამირების კონცეფცია: ბლოკ-დიაგრამაზე ფუნქციონალური ბლოკების მიმდევრობითი შეერთება. კონკრეტულად ინტუიტიურად გასაგები და თვალნათლივი გრაფიკული კოდი, ასევე პროგრამის შესრულებისას მონაცემთა ნაკადის მართვის ვიზუალური მონიტორინგის შესაძლებლობები ადამიანისათვის უფრო გასაგებს ხდის მთელ პროცესს.

პროექტირების სისტემა LabVIEW-ს აქვს მოწყობილობის უდიდესი სპექტრი სხვადასხვა მწარმოებლების მიერ შექმნილი მოწყობილობებისა და დამატებით კომპონენტების ძალიან დიდი ბიბლიოთეკა.

მძლავრი გრაფიკული პროგრამირების ენა საშუალებას იძლევა ასჯერ გაიზარდოს შრომის ნაყოფიერება. დასრულებული დანართის შექმნა ჩვეულებრივი პროგრამირების ენით ძალიან დიდ დროს მოითხოვს, მაშინ როცა პროექტირების სისტემა LabVIEW-ს სჭირდება სულ რამდენიმე საათი, რადგანაც პაკეტი შექმნილია სპეციალურად სხვადასხვა განზომილების დაპროგრამებისათვის, მას აქვს მოქნილი გრაფიკული ინტერფეისი და მარტივია პროგრამირებისათვის, იგი საუკეთესოა პროცესის მოდელირებისათვის, დანართების შექმნისათვის და უბრალოდ თანამედროვე პროგრამირების შესწავლისთვისაც.

აქ შექმნილი გამზომი სისტემა ბევრად უფრო მოქნილია ჩვეულებრივ ლაბორატორიულ ხელსაწყოებთან შედარებით, რადგანაც იგი წარმატებით იყენებს თანამედროვე პროგრამირების შესაძლებლობებს. პროექტირების სისტემა LabVIEW-ს საშუალებით მარტივად იქმნება ვირტუალური ხელსაწყოს საჭირო ტიპი საკმაოდ მცირე დანახარჯებით სხვებთან შედარებით. აუცილებლობის შემთხვევაში მასში ცვლილებების შეტანა წუთების საქმეა.

LabVIEW-ი შექმნილია ამოცანების დაპროგრამების გასაადვილებლად. ამისათვის მას აქვს ფუნქციათა გაფართოებული ბიბლიოთეკა და მზა ქვეპროგრამები, რომლითაც ხდება ტიპიური ამოცანების რეალიზაცია, რითაც გავთავისუფლდებით ძალიან ბევრი წვრილმანი მოქმედებებისაგან, თავისი გრაფიკული ბუნების წყალობით იგი

ეფექტურად ასახავს და წარმოადგენს მონეცემებს, გამომავალი მონაცემები შეიძლება მოცემული იყოს ნებისმიერი სასურველი ფორმით.

LabVIEW-ის პროგრამები ადვილად პორტირდება სხვა პლატფორმებზე, შესაძლებელია დანართები შეიქმას სხვა სისტემაქში და შემდეგგაუშვათ ისინი Windows-ზე, თანაც ისე, რომ მასში მნიშვნელოვნად არაფერი შეცვალოთ, ისინი ადამიანის მოღვაწეობის ბევრ სფეროში აუმჯობესებენ მუშაობას, მათ შორის ტექნოლოგიური პროცესების ავტომატიზაციაში, ქიმიაში, ფიზიკაში და ა.შ.

4.3 პროექტირების სისტემა Proteus-ი.

არსებობს ძალიან კარგი გამოსავალი ამ სიტუაციიდან პროგრამა-სიმულიატორების სახით, რომლებიც რეალურ დეტალებსა და ხელსაწყოებს ცვლიან ვირტუალური მოდელებით, ისინი საშუალებას იძლევიან რეალური მოწყობილობის აწყობის გარეშე დაალაგონ სქემის მუშაობა, მოძებნონ პროექტირების სტადიაზე დაშვებული შეცდომები, მოხსნან აუცილებელი მახასიათებლები და მრავალი სხვა. ერთ-ერთი ასეთი პროგრამაა PROTEUS-ი, რომლისთვისაც ელემენტების სიმულაცია არა ერთადერთი უნარია, იგი წარმოადგენს ე.წ. „გამჭოლი პროექტირების“ გარემოს, რაც ნიშნავს მოწყობილობის შექმნას მისი გრაფიკული გამოსახულებიდან მოწყობილობის დამზადებამდე წარმოების ყოველ ეტაპზე კონტროლის შესაძლებლობით. იგი თავის თავში აერთიანებს ორ ძირითად პროგრამას: ISIS-ელექტრონული სქემების რეალურ დროში დამუშავების და აწყობის საშუალებებს და ARES-ნაბეჭდი დაფების დამუშავების საშუალებებს. სხვა ანალოგური პროგრამული პაკეტებისაგან განსხვავებით, ისეთები როგორიცაა Multisim, Microcap და სხვა Proteus-ს აქვს კომპონენტების ძალიან ფართო ბიბლიოთეკა, მათ შორის პერიფერიული მოწყობილობებისთვისაც: შუქდიოდები და ინდიკატორები, ტემპერატურული გადამწოდები, რეალური დროის საათები, ასევე შეტანა-გამოტანის ინტერაქტიური ელემენტები: ღილაკები, გადამრთველები, ვირტუალური პორტები და გამზომი ხელსაწყოები, ხოლო მთელი რიგი

მიკროკონტროლერების, კომპონენტებისა და მიკროსქემების დამატებით იგი გახდა უფრო ძლიერი და საშუალებას იძლევა მთლიანად შემოწმდეს მიკროკონტროლერების ბაზაზე შექმნილი მოწყობილობები [1,3,4,8,].

სწორედ ისეთი სისტემების პროექტირებისა და კვლევისათვის, როგორიცაა დაცვის სისტემები ყველაზე ოპტიმალურ ვარიანტად განიხილება ეს პროგრამა, მართლაც ნებისმიერი პროცესის კვლევისათვის უკვე ნორმად იქცა სქემის შეყვანა და ეკრანული გრაფიკა, მაგრამ სიმულაციის პროცესი ამ დროს ინტერ აქტიურია, ჩვენ ვხაზავთ სქემას და გრაფიკის მიხედვით ვსწავლობთ, მაგრამ ეს კარგია, როცა სქემა სტატიკურია, მაგრამ სიგნალიზაციის სქემების აწყობისას, თუ ჩვენ გვაინტერესებს რა მოხდება, თუ კლავიატურიდან შეყვანილი იქნება არასწორი პაროლი, სწორედ ამ დროს ყველაზე ოპტიმალურია PROTEUS-ის გამოყენება, იგი წარმოადგენს არქიტექტურას, რომელშიც დამატებითი ანიმირებული მოდელები შეიძლება შეიქმნას ნებისმიერად, მათი ტიპების უმრავლესობა შეიძლება იყოს კოდირებისადმი მიმართვის გარეშე, შესაბამისად PROTEUS-ი საშუალებას აძლევს პროფესიონალ ინჟინრებს გაუშვან რეალური პროექტების ინტერაქტიური სიმულაცია, და ჯილდოდ მიიღონ შედეგი, რომელიც შეესაბამება სქემის სიმულაციას. თუ ესეც არ იქნება საკმარისი, შექმნილია მთელი რიგი პოპულარული მიკროკონტროლერების სიმულაციის მოდელები, რის შედეგადაც შესაძლებელია სრული მიკროკონტროლერების სისტემების სიმულირება და მათთვის პროგრამების შემუშავება მათი ფიზიკური პროტოტიპებისადმი მიმართვის გარეშე.

სქემის ასაწყობად პროგრამის გაშვებისა და ახალი პროექტისთვის სახელის მინიჭებისა და განლაგების ადგილის მითითების შემდეგ ეკრანზე ვღებულობთ ძირითად ფანჯარას, რომელშიც ყველაზე მეტი სივრცე ეთმობა რედაქტირების ფანჯარას Edit Window, სწორედ მასში მიმდინარეობს შექმნის ყველა ძირითადი ეტაპი, მათ შორის სქემის რედაქტირება და საბოლო აწყობა.

მარცხნივ ზემოთ გვაქვს წინასწარი დათვალიერების ფანჯარა Overview Window, მისი საშუალებით გადავაადგილდებით რედაქტირების ფანჯარაში (თაგვის მარცხენა ღილაკის დაწკაპუნებით წინასწარი დათვალიერების ფანჯარაზე, გადავაადგილებთ რედაქტირების ფანჯარას სქემაში, თუ რა თქმა უნდა სქემა არ დაეტევა ფანჯარაში)[2].

რედაქტირების ფანჯრის გადაადგილება სქემაში შეიძლება ასევე Shift ღილაკის დაჭერით თაგვის კურსორის გადაადგილებით სქემაში, სქემის მოახლოება ან დაშორება შეიძლება შესაბამისად F6 და F7 ღილაკებით, ან თაგვის ბორბლით, F5-ით ხდება სქემის ცენტრირება ფანჯარაში, ხოლო F8 ღილაკი სქემის ზომებს შეუსაბამებს ფანჯარას. წინასწარი დათვალიერების ფანჯარაში ინახება Object Selector, მოცემულ მომენტში არჩეულ კომპონენტთა, სიმბოლოთა და სხვა ელემენტების ჩამონათვალი.

პროგრამის ყველა შესაძლო ფუნქციები და ინსტრუმენტები შესაძლებელია მხოლოდ იმ მენიუს დახმარებით, რომელიც განლაგებულია პროგრამის ძირითადი ფანჯრის ზემოთ, პიქტოგრამების სახით ძირითადი ფანჯრის მარცხენა კუთხეში და ანთებული ღილაკებით, რომლებიც შეიძლება მომხმარებლის მიერ გამოყენებული იყოს სხვა დანიშნულებითაც[3].

ძირითადი ფანჯრის ყველაზე ქვემოთ განლაგებულია: მაცხნიდან მარჯვნივ ობიექტის საკუთარი ღერძის გარშემო შემობრუნების ღილაკები, შემდეგ სტატუსის სტრიქონი (მასში აისახება შეცდომები, კარნახი, სიმულაციის პროცესის მდგომარეობა და ა.შ.) და კურსორის კოორდინატები, გამოსახული დიუმებში.

ობიექტების მანიპულირებისათვის საჭიროა წინასწარ მათი გამოყოფა, ეს შეიძლება გაკეთდეს მხოლოდ შეჩერებულ პროექტზე, ერთი ობიექტის გამოყოფისათვის მასზე უნდა დავაწკაპუნოთ თაგვის მარჯვენა ღილაკი, ჯგუფის გამოყოფისათვის ან CTRL ღილაკით ან თაგვის მარჯვენა ღილაკით დაჭერილ მდგომარეობაში და შემდეგ საჭირო ობიექტებზე თანმიმდევრული დაწკაპუნებით., მარჯვენა ღილაკის განმეორებით

დაწკაპუნება წაშლის ობიექტს, თუმცა ბოლო და ბოლს წინა მოქმედებების აკრძალვა შეიძლება ღილაკებით Undo-Redo. გამოყოფილი ობიექტები შეიძლება გადავაადგილოთ სქემაში მაუსის მარცხენა ღილაკით, მარცხენა ღილაკითვე ხდება გამოყოფილ ობიექტებზე ჯგუფური ოპერაციები., როგორიცაა კოპირება, გადაადგილება, მობრუნება და წაშლა.

4.4 GSM-მოდულები.

თუ კომპლექსურად მივუდგებით უსაფრთხოების პრობლემას, შეიძლება ვილაპარაკოთ ამ სისტემის დაყენებისა და გამოყენების სიმარტივეზე, ხანგამძლეობაზე, საიმედობაზე, ფართო ფუნქციონალურობაზე, შეიძლება სრული დარწმუნებით ვთქვათ რომ დაცვის ინტელექტუალური სისტემები პასუხობს ყველა მოთხოვნას, რაც კი შეიძლება იდგეს დაცვის სისტემების წინაშე. იგი ოპტიმალური ვარიანტია სხვებთან შედარებით. მისი ერთ-ერთი ვარიანტია GSM-მოდულების გამოყენება.

თავისი მოქმედების პრინციპით GSM-მოდულები წარმოადგენენ გარკვეული სიხშირის რადიოტალღების მიმღებს, ინფორმაციის დამუშავებისათვის გამოიყენება კონტროლერი, კავშირის ოპერატორი შეიძლება იყოს არჩეული ნებისმიერად, მონაცემთა ბაზაში ინახება იმ მომხმარებლების ტელეფონის ნომრები, რომელთაც ნებადართული აქვთ მოცემულ ტერიტორიაზე შესვლა, ზოგადად მონაცემთა ბაზაში შეიძლება ინახებოდეს 2000 აბონენტის მონაცემები, თუმცა უფრო თანამედროვე და ძვირი მოდელები ინახავენ 10 000 და ბევრად მეტი აბონენტის შესახებ ინფორმაციას.

გამოძახების დროს მომხმარებლის სიგნალი მიეწოდება კონტროლერს, რომელიც ადარებს ამ ნომერს ბაზაში არსებულ ნომრებთან, თუ მოხდა დამთხვევა, მაშინ კონტროლერი გასცემს რაიმე მოქმედების შესახებ ბრძანებას რომელიმე მექანიზმზე, თუ ასეთი ნომერი არ არის ბაზაში, მაშინ კონტროლერი ახდენს გამოძახების განულებას და არ ხდება არანაირი ქმედება[9].

არავითარი დაკავშირება საუბრისათვის ან სხვა მიზნით არ ხდება, ან დაკავშირება მიმდინარეობს მხოლოდ რამდენიმე წამის განმავლობაში, ამიტომ კავშირის მომსახურებაზე არ არის არანაირი გადასახადი, შეიძლება ვისარგებლოთ უფასოდ. ზოგიერთი GSM-მოდულები დაპროგრამებულია იმგვარად, რომ ნებისმიერი ზარის შესვლისას არ ხდება ნომრის იდენტიფიკაცია და წვდომის უფლება ეძლევა ნებისმიერ ადამიანს, ვინც რეკავს [3,4].

GSM-მოდულების კონტროლერი განსხვავდება სხვა მოდელებისაგან იმით, რომ:

- ყველა აბონენტისათვის ცალ-ცალკე არ არის საჭირო მართვის სპეციალური პულტებისა და სხვა ბარათების შეძენა;
- ზოგიერთი GSM-მოდულებით აღჭურვილ სისტემებს აქვთ მომხმარებელთა რიცხვის შეზღუდვის პრობლემა;
- სისტემის ამა-თუ იმ ქმედებაზე ბრძანების გაცემა შეიძლება ნებისმიერი ადგილიდან, სადაც კი არის თქვენი მობილური ოპერატორის ქსელი;
- შესაძლებელია სისტემის დალაგება კომპიუტერის მეშვეობით, აბონენტთა ბაზაში დამატება ან ამოგდება, წვდომის შეცვლა და ა.შ.
- GSM-მოდულები შეიძლება გამოვიყენოთ ნებისმიერი მწარმოებლის;
- აპარატურის დაბალი ღირებულება, ისისნი ფასით უტოლდება მართვის სამი პულტის ღირებულებას, თუ აბონენტთა რიცხვი დიდია, მაშინ მაშინ უფრო მეტი ეკონომია გაიწევა;
- ადვილი და მარტივია სისტემის აწყობა, მისი დაყენება შეუძლია ნებისმიერ ადამიანს, რომელიც ფლობს ელექტროტექნიკის ელემენტალურ ცოდნას, ინსტრუქციის შესაბამისად;
- სხვა მოწყობილობებისაგან განსხვავებით, რომელთა მართვა ხორციელდება მავთულებით, აქ არის შესაძლებლობა უცვლელად დავტოვოთ შენობის ინტერიერი მონტაჟის დროს, არ დავაზიანოთ ის. არ არის მავთულების საჭიროება, რადგან სიგნალი გადაეცემა რადიოსიხშირით;

ასეთი სისტემის სერიოზულ ნაკლად ითვლება ის ფაქტი, რომ მიმყოლის მექანიზმი არ იმუშავებს, თუ სმარტფონის ბატარეები განმუხტულია, ან თუ ამ ნომერზე ანგარიშზე არ გაქვთ თანხა, ასევე ნაკლად შეიძლება ჩაითვალოს ის გარემოებაც, რომ შესაძლებელია სიგნალის ჩახშობა.

GSM-მოდულები გამოიყენებიან სხვადასხვა ტიპის მოწყობილობებში, როგორებიცაა:

- საავტომობილო სიგნალიზაციები;
- ოფისების კარები ელექტროსაკეტით;
- გათბობის ელექტროქვაბები;
- შლაგბაუმებისა და ჭიშკრების ავტომატიკა;
- სხვადასხვა სიგნალიზაციები და დაცვის სისტემები;

უსადენო სისტემები განიცდიან მუდმივად განახლების პროცესს, ხოლო ტექნოლოგიები უფრო სრულყოფილი ხდება, მათი აწყობისათვის არ არის საჭირო განსაკუთრებული კვალიფიკაცია, ყველაფერი კეთდება რამდენიმე წუთში, ისინი გამოიყენებიან იმ ადგილებშიც, სადაც არ არის ჩვეულებრივი სატელეფონო კავშირები, ამ უპირატესობების გამო GSM-მოდულები გახდნენ გაყიდვის ლიდერები[6].

მოდულის ნორმალური ფუნქციონირებისათვის წინასწარ უნდა შეირჩეს ადგილი წამოყენებული მოთხოვნების გათვალისწინებით, მხოლოდ მოწყობილობის მუშაობის რეჟიმებისა და პირობების გარკვევის შემდეგ შესაძლებელია სწორად იქნას შერჩეული ის მოდელი, რომელიც დიდხანს და გამართულად იმუშავებს.

ასევე მნიშვნელოვან მომენტს წარმოადგენს ობიექტის ტიპი, მასზეა დამოკიდებული კონკრეტული ტექნიკური მონაცემების მოდელის შერჩევა, ოფისებისა და სხვა სახელმწიფო ობიექტებისათვის უნდა შეირჩეს კომპლექტი კამერით, ის დაგვეხმარება შეღწევის მცდელობების და რაოდენობების კონტროლში, ასევე შევამოწმებთ თანამშრომლების მიერ სამუშაო რეჟიმის დაცვას[2].

4.5 სიგნალიზაციის სქემის განხილვა

Proteus-ის საშუალებით გადავწყვიტე სიგნალიზაციის სქემის აწყობა, ამ სქემის ერთ-ერთი მთავარი მოწყობილობაა მიკროკონტროლერი, სქემის საიმედობისათვის და ფუნქციონალურად სრულყოფისათვის გადავწყვიტე შემერჩია მიკროკონტროლერი Arduino Mega 2560, რომელზეც არჩევანი შევაჩერე რამდენიმე უპირატესობის გამო[29]:

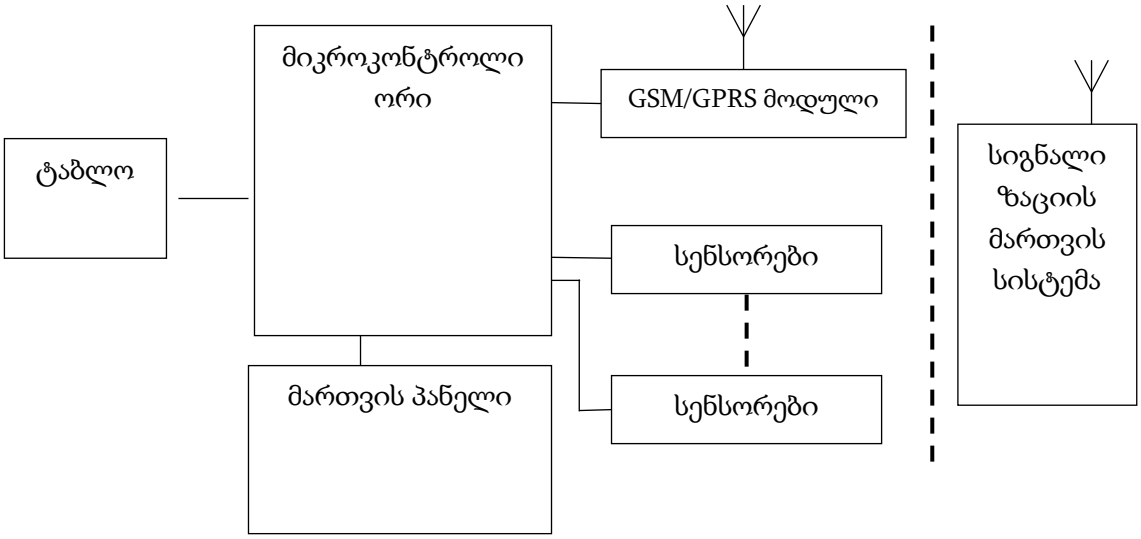
ა) **დაბალფასიანი** – სხვებთან შედარებით, არდუინო პლატფორმა საკმაოდ იაფია. ასევე, ღიად ხელმისაწვდომია დაფის ნახაზები და ყოველგვარი ინფორმაცია. ადამიანს შეუძლია თავისივე ხელით ააწყოს და აამუშაოს ეს დაფა.

ბ) **მარტივი და გასაგები შემუშავების გარემო** – შემუშავების გარემო IDE მეგობრულია ყველა დამწყებისთვის და ამავდროულად საკმარისად მძლავრია გაწაფული მომხმარებლებისთვის.

გ) **ღია-წყაროს-მქონე და ვრცელი მოწყობილობათა საფუძველი** – არდუინოს გული – მისი მიკროპროცესორი – არის Atmel ფირმის ATMEGA8 და ATMEGA168 მიკროკონტროლერი.

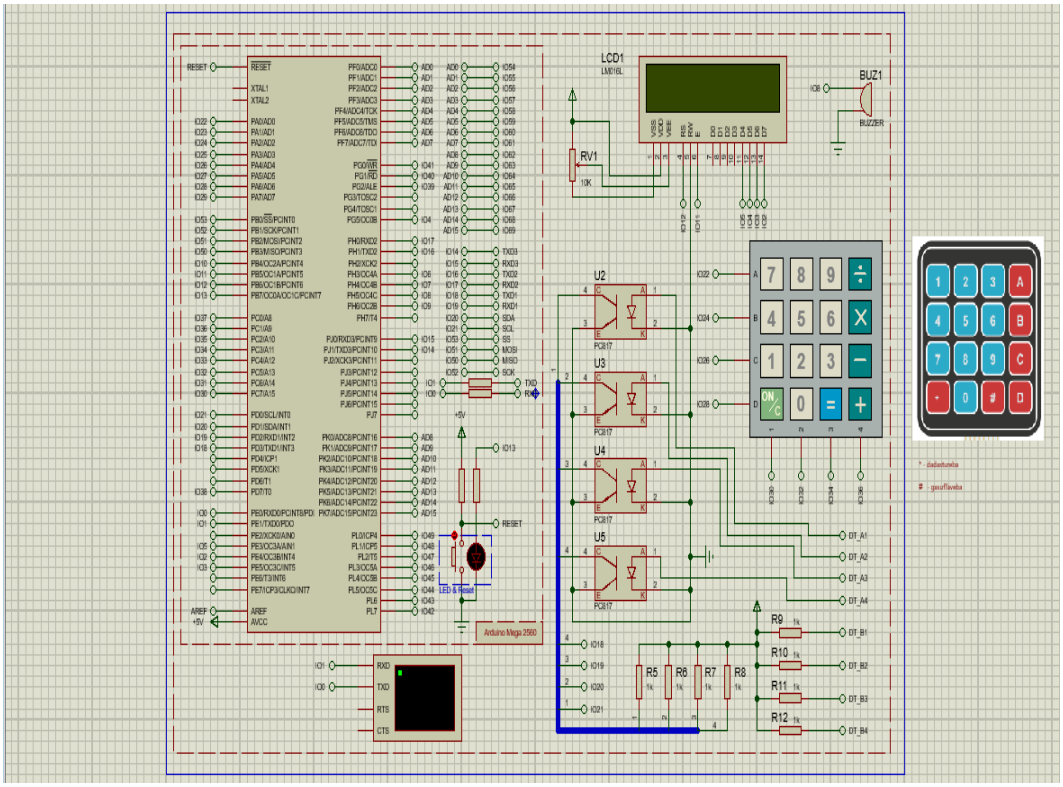
დ) **სქემაში ადგილების მინიმიზაციისა და შეტანა-გამოტანის პორტების სიმრავლის** გამო, მას გააჩნია 54 შეტანა-გამოტანის პორტი, რომელთაგან 15 მუშაობს სიმძლავრის, დენის, სიჩქარის, განათების რეგულირების სიგნალების წყაროდ, დამატებით 16 ანალოგური პორტით, რომლებიც ამუშავებენ გადამწოდებიდან მიღებულ სიგნალებს, ისინი გამოიყენებიან როგორც ციფრული გამოსასვლელები, მისი საშუალებით შესაძლებელია მძლავრი განშტოების ორგანიზება, აგრეთვე ავტომატური მართვის სისტემის მართვა დაცილებულად და ყველა პარამეტრების მონოტორინგი, ამიტომ ამ კონკრეტული მიკროკონტროლერის საშუალებით სრულდება არა მარტო სიგნალიზაციის სქემები, არამედ ბევრი სხვა პროექტები, როგორიცაა „ჭკვიანი“ სახლი, ავტომატიზებული საქვაბე, სასათბურე მეურნეობები ნიადაგის მარილების შემადგენლობისა და ტენიანობის ავტომატური კონტროლით, მეტეოსადგურები და მრავალი სხვა[28,29].

ჩემს მიერ აწყობილი სქემა შეიძლება გამოყენებული იქნას, როგორც სახელმწიფო ობიექტებზე, ასევე კერძო შენობებისა და ფართების დაცვისათვის. სქემაში გამოყენებულია შესასვლელი ერთჯერადი პაროლი, თუმცა შეიძლება მისი შეცვლაც, კარის გაღებისას სიგნალი აქტიურია 10 წამის განმავლობაში, შემსვლელი პირი სიგნალის განგაშის შესაჩერებლად კრებს 4 ციფრიან პაროლს (ჩვენს შემთხვევაში 1234). B ღილაკზე ხელის დაჭერისას ჩვენ შევდივართ პაროლის ცვლილების მენიუში, პაროლის შეცლის შემდეგ განგაშის შეჩერებას შევძლებთ მხოლოდ ახალი პაროლის აკრებით, თუ პაროლი შეყვანილია არასწორად, ეკრანზე მივიღებთ შეტყობინებას „კიდევ სცადეთ“. პროგრამის მუშაობის საწყის ეტაპზე ხდება ბიბლიოთეკის ინიციალიზაცია, მიკროკონტროლერის თითოეულ ფეხს ენიჭება გარკვეული ფუნქცია, ასევე მიმდინარეობს საწყისი პაროლის შეყვანა, კარის გაღებისას განგაშის სიგნალის გააქტიურება და ღილაკებისთვის ფუნქციონალური დატვირთვის მინიჭება. დაცვის ისიტემა ძალიან სწრაფად რეაგირებს კარის გაღებაზე, კვამლზე და მინის გატეხვაზე. შესაძლებელია აგრეთვე მისთვის ფუნქციების დამატება, ასევე მასთან დამატებითი მოდულების მიერთების შედეგად სრულყოფა. ახალი პაროლის დაყენების შემდეგ სიგნალიზაცია რეაგირებს მასზე, სპეციალურად სქემისათვის შეიქმნა ქართული უნიკოდი, ამისათვის გამოვიყენე 8X5-ზე სეგმენტიანი ქართული ანბანი და შემდეგ ის გადავიყვანეთ ციფრულ კოდში, ამისთვის სპეციალურად შევარჩიეთ ეკრანი შესაბამისი შესაძლებლობებით.



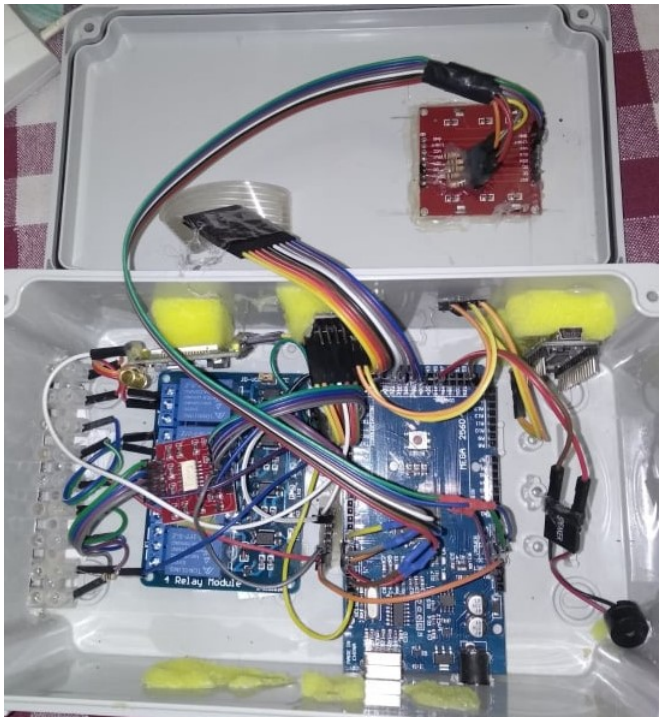
ნახ.1. დაცვის ციფრული სისტემის სქემა.

საბოლოოდ სქემას აქვს ნახ 2. და ნახ.3 -ის სახე, შესაძლებლია დიზაინის დახვეწა, რაც აუცილებლად განხორციელდება ფუნქციონალური სრულყოფის შემდეგ.



ნახ. 2 Proteus-ით აწყობილი სქემა

ნახ. 3 აწყობილი სქემის ხედი ზემოდან



ნახ.4. სქემის მთავარი პანელი

დასკვნა

1. შემუშავებული სქემა წარმოადგენს სახელმწიფო ობიექტის სიგნალიზაციის ერთ-ერთ შესაძლო ვარიანტს, რომელიც წარმატებით უზრუნველყოფს სხვადასხვა ტიპის ობიექტების დაცვას.
2. იგი აწყობილია მიკროპროცესორულ ბლოკზე და წარმოადგენს მოქნილ მოწყობილობას ფუნქციონალური ცვლილების თვალსაზრისით, მარტივია დასამზადებლად.
3. იაფია თვითღირებულებით, საიმედოა და აკმაყოფილებს თანამედროვე მოთხოვნებს, მისი მხოლოდ უმნიშვნელო ცვლილება უზრუნველყოფს აგრეთვე ერთდროულად რამდენიმე ობიექტის დაცვას, სისტემა საიმედოა შეუღწევლობის უზრუნველყოფით.
4. შესაძლებელია SMS შეტყობინებების გაგზავნა, მათი დამახსოვრება, ხასიათდება კვების მრავალსაათიანი ავტონომიურობით, მისი გამოყენება მცირე პროგრამული და აპარატურული ცვლილებებით შესაძლებელია საკმაოდ ფართო სპექტრის ობიექტებისათვის.

გამოყენებული ლიტერატურა:

1. С. Муратчаев, С. Скворцов, В. Смирнов PROTEUS по-русски, СПб 2013 г.-сс 204-212.

2. А.А. Алешин, В.В. Герасимов Аппаратные и програмные средства систем управления иниелектуальных мобильных роботов, Москва 2011 г.- сс 123-129.

3. Ю. Гришко руководство по проектированию печатных плат, СПб 2011 г.-сс 48-57ю

4. თ. გვალია. მიკროპროცესორული სისტემები და მათი დაპროგრამება C ენაზე. ქუთაისი 2013 წ. გვ 23-33.

5. Зеленский А.В. Расчет надежности электронных средств. Самара 2014.-сс 145-149.

6. Корольков В.И. Андреев В.В. Програмные и аппаратные средства современной схемотехники ипрограмирование микроконтроллеров. Москва 2008. –сс 234-245.

7. Мрыкин С.В. Метод структурных схеи и оценка безотказности системы. Москва 2011. –сс 35-47.

8. www. Michichip.ru

9. http://opsmontaj.ru/okhrana-perimetra

10.http://ohranivdome.net/ohrannaja-signalizacija/montazh-i-obsluzhivanie/obzor-sistem-okhrany-perimetra-i-ikh-kratkie-kharakteristiki.html

11. http://www.lntcenter.ru/tipy-ohrannoj-signalizacii.html

12.https://secandsafe.ru/stati/kompleksnye_sistemy_bezopasnosti/tiekhnichieskiie_sriedstva_okhrany_obiektov

13.http://studopedia.su/15_51891_programmnoe-obespechenie-vstroennih-sistem.html

14. http://smartstation.su/

15. http://www.bestreferat.ru/referat-325736.html

16. http://www.bezopasnost.ru/catalog/147/

17. http://controleng.ru/programmnye-sredstva/vstraivaemy-e-sistemy-upravleniya/

18. Волковицкий В. Д. Цшфровые системы ТВ-наблюдения. Санкт-Петербург 2012 г.-сс 85-92.

19. Гедзберг Ю.М. Охранное телевидение. Москва 2002 г.-сс 34-39.

20. Загретдинов Р.В. Спутниковые системы позисионирования. Казань 2014 г.-сс 104-109.

21.Барабанова М.И., Кияев В.И. Информационные технологии: открытые системы, сети, безопасность в системах и сетях: Учебное пособие.- СПб.: Изд-во СПбГУЭФ, 2013.- 267 с.

22.Тихонов И.А. Информативные параметры биометрической аутентификации пользователей информационных систем по инфракрасному изображению сосудистого русла Биомедицинская техника и радиоэлектроника. 2012. № 9. С. 26-32.

23. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. - Феникс, 2012 г.-сс 121-128.

24. Галатенко В.А. Идентификация и аутентификация, управление доступом лекция из курса «Основы информационной безопасности». - Интернет Университет Информационных Технологий, 2011г.-сс 125-132.

25. Рыжова В.А Проектирование и исследование комплексных систем охраны и безопасности. СПб -2012 г.-с128.

26. Волхонский В.В. Системы охранной сигнализации, 2-ое изд. СПб -2009 г.-сс23-34.

27. Идентификация обьектов управления. Самарскии государственный технический университет 2009. С56.

28. Sook-Ling Chua and Stephen Marsland and HansW. Guesgen" Beha viour Recognition in Smart Homes Sook" Proceedings of the Twenty-Second International Joint Conference on Artificial Intelligence 2015. pp34-45.

29.ია მოსაშვილი, სალომე ონიანი. Arduino პროგრამირების საფუძვლები.

საქართველოს ტექნიკური უნივერსიტეტი. 2016წ. ISBN 978-9941-20-711-2.

30. *Волхонский В. В.* Устройства охранной сигнализации. Ч. 1. Извещатели / В. В. Волхонский. — СПб. : Экополис и культура, 2001.-с 122.

31. *Волхонский В В.* Устройства охранной сигнализации. Ч. 2. Контрольные панели / В. В. Волхонский. — СПб. : Экополис и культура, 2002. –сс38-47.

32. *Волхонский В. В.* Системы охранной сигнализации / В. В. Волхонский. — СПб. : Экополис и культура, 2005.-с127.

33.*Волхонский В. В.* Телевизионные системы наблюдения / В. В. Вол хонский. — СПб. : Экополис и культура, 2005.-сс-67-79.

34. *Коротких В. Е.* Современные средства технической безопасности /В.Е.Коротких, О.С.Киселев. — Казань : Новое знание, 2003.-сс79-87.

35. Алексеев, А. А. Идентификация и диагностика систем / А.А. Алексеев, Ю.А. Кораблев, М.Ю. Шестопалов. - М.: Academia, 2016. - 352 с.

36. Дьяконов, Владимир Matlab. Анализ, идентификация и моделирование систем. Специальный справочник / Владимир Дьяконов , Владимир Круглов. - М.: СПб: Питер, 2013. - 448 с.

37. Задорожный В.В. Идентификация по отпечаткам пальцев. PC Magazine/Russian Edition №1, 2004, - С. 25 -35.

38. Комплексные системы безопасности. М. Научно-производственный центр “Нелк”, 2001.-сс 134-139.