SAVONIA

Access Control System

ACS

Abuov Timur

Bachelor's

___. ___. _____ _____

Bachelor's degree (UAS)

SAVONIA UNIVERSITY OF APPLIED SCIENCES **THESIS**
Abstract

Field of Study Technology, Communication and Transport			
Degree Programme Degree Programme in Information Technology			
Author(s) Abuov Timur			
Title of Thesis Access Control System			
Date	11.06.2017	Pages/Appendices	33
Supervisor(s) Pekka Granroth			
Client Organization/Partners Technical Competence Centre DEMEU Ltd.			

Abstract

The purpose of this work was to review an access control system as a whole, to consider its advantages and to determine the reasons why it is relevant; to consider installation from the company IDmatik and find out which services they provide today and determine their superiority over other companies; to describe in details the installation process of this system.

Access control system (ACS) is a modern, convenient and effective security tool in buildings and industrial complexes. The access control system is designed to record working hours, prevent unauthorized access to facilities, to organize a pass system for employees and guests, to control the actions of operators and security guards. The system also solves the problems of delineation of access and control of the situation on the site, helps to ensure order and discipline. The installation of the access control system allows restricting the passage of strangers to certain premises.

The result of this work was the possibility of understanding the access control system, understanding the need of this system, considering advantages and benefits of the system from the company IDmatic and considering the process of installing an access control system.

Keywords
ACS, IDmatic, Access Control System, Networking Systems, Autonomous systems

SAVONIA-AMMATTIKORKEAKOULU

OPINNÄYTETYÖ
Tiivistelmä

Koulutusala Tekniikan ja liikenteen ala	
Koulutusohjelma/Tutkinto-ohjelma Tietotekniikan tutkinto-ohjelma	
Työn tekijä(t) Abuov Timur	
Työn nimi Pääsyvalvontajärjestelmä	
Päiväys 11.06.2017	Sivumäärä/Liitteet 33
Ohjaaja(t) Pekka Granroth	
Toimeksiantaja/Yhteistyökumppani(t) Technical Competence Centre DEMEU Ltd.	

Tiivistelmä

Tämän työn tarkoitus on katsoa pääsynvalvontajärjestelmää kokonaisuutena,
tutkia sen etuja ja selvittää syyt, miksi se on aiheellista. Myös pitää mielessä palvelun asentamisen IDmatik yrityksestä, selvittää, mitä palveluja he tarvoavat tänään ja selvittää mikä tekee tästä yrityksestä parhaan muiden yrityksen nähden. Ja myös kertoa yksityiskohtaisempi järjestelmän asentamisesta.

Pääsyvalvontajärjestelmä (ACS) on moderni, kätevä ja tehokas työkalu rakennuksissa ja teollisuuskomplekseissa.
Pääsyvalvontajärjestelmä on suunniteltu tallentamaan työntekijoiden työaikaa, estämään luvattoman pääsyn laitokseen, järjestämään sisäänpääsyjärjestelmän työntekijöille ja vieraille sekä hallitsemaan operaattoreiden sekä vartioiden toimintaa. Järjestelmä ratkaisee myös ongelmat, jotka liittyvät alueen pääsyn ja valvonnan määrittelyyn, varmistaa järjestyksen ja kurinmukaisuuden. Volvontajärjestelmän asennus mahdollistaa vieraiden rajoittamisen tiettyihin tiloihin.

Tämän työn tuloksena oli mahdollisuus ymmärtää pääsyvalvontajärjestelmä, ymmärtää sen tarve ottaen huomioon järjestälmän edut ja hyödyt IDmatik yrityksestä sekä pohtia järjestelmän asentamista.

Avainsanat
ACS, IDmatic, Access Control System, Networking Systems, Autonomous systems

CONTENTS

LIST OF ABBREVIATIONS

ACS - Access Control System

SAS - Security Alarm System.

FAS - Fire Alarm System

RFID - Radio Frequency Identification

RS - Recommended Standard

PC - Personal computer

Wi-Fi - Wireless Fidelity

GSM- Global System for Mobile Communications

GPRS - General Packet Radio Service

SMS - Short Message Service

RF - Radio Frequency

VPN - Virtual Private Network

IP – Internet Protocol

EDS – Encrypted Data Store

QR - Quick Response

GPS - Global Positioning System

DC - Direct Current

LAN - Local Area Network

GUID - Globally Unique Identifier

AMS – Advanced Multithreaded Server

1 INTRODUCTION

Last year I had an internship in Kazakhstan. I was practicing in Demeu, Technical Competence Centre DEMEU Ltd., which is one of the largest companies in Kazakhstan market providing services in outsourcing and integrated services of technical infrastructure of large organizations.

The purpose of my practice was to familiarize with the functions and features of different Telecommunicational equipment and to get practical experience in searching and troubleshooting problems which appear in Network infrastructure of companies with more than 2000 active users.

During my practice I did various tasks. One of them was an installation of access control system. Is required quite a big competence so I've been doing this for about a week with other professional workers.

Due to the fact I was studying in sphere of computer networks and because the installation of this system includes installation and configuration of servers and routers, cabling, software installation, I became very interested in this topic and wanted to know more about it.

So I decided to write a thesis about this system.

Today access control system is widely used all over the world and is used by various customers. By customers I mean any enterprise or organization that must be equipped with systems that reduce the risk of unauthorized entry into enclosed spaces. In order to increase security, access control system is installed. The installation of the access control system allows to restrict the passage of strangers to certain premises.

Installation of the system is handled by different firms. Nevertheless, the system implementation process as a whole is the same across all the firms. The main difference is in the software. In my work I will consider the access control system from the company IDmatic, because when I was in practice in Demeu, we made installation of this system together with IDmatic and today it is one of the leading firms in this field.

2 ACS, WHAT IS IT

Access control system (ACS) is a modern, convenient and effective security tool in buildings and industrial complexes. The access control system is designed to record working hours, prevent unauthorized access to the facility, organize a pass system for employees and guests, and control the actions of operators and security guards. The system also solves the problems of delineation of access and control of the situation on the site, helps to ensure order and discipline.

The main tasks are:

- Restricting an access to a given territory
- Identification of a person who has access to a given territory

Additional tasks:

- Accounting of working hours;
- Maintaining a staff / visitor base;
- Integration with the security system, for example:
  With a video surveillance system for combining the archives of system events, transfer to the video surveillance system notifications about the need to start recording, turn the camera to record the consequences of a fixed suspicious event;
  With a security alarm system (SAS), for example, to restrict access to premises that are guarded, or for automatic removal and arming of premises.
  With a fire alarm system (FAS) to obtain information on the status of fire detectors, automatic release of evacuation exits and the closing of fire doors in case of fire alarm.

2.1 Components of ACS

Let us consider the devices of which the ACS consists.

2.1.1 Blocking devices

Installed on the door:

- Electric locks are the least protected from hacking, so they are usually installed on internal doors (intra-office, etc.). Electric locks, like other types of locks, can be opened by voltage (that is, the door opens when the supply voltage is applied to the lock) and closed by voltage. Open, as

soon as they are removed from the supply voltage, therefore recommended for use by fire inspection.

- Electromagnetic locks - almost all are locked by voltage, so they are suitable for installation on evacuation routes during a fire.
- Electromechanical locks are sufficiently resistant to burglary (if the lock is strong mechanically), many have a mechanical re-set (this means that if an opening pulse was applied to the lock, it will be unlocked until the door is opened).

Are installed on the aisles / passageways:

- Turnstiles (Figure 1) - used at checkpoints, publicly significant facilities (stadiums, train stations, subway, some state institutions) - wherever a controlled passage of a large number of people is required. Turnstiles are divided into two main types: belt and full-height.

FIGURE 1. Turnstile with access control system reader. (Oleg Chirkov, 2008)

- Gates and barriers (Figure 2) are mainly installed at entrances to the territory of the enterprise, car parks, at entrances to the adjacent territory. The main requirement is resistance to climatic conditions and the possibility of automated control (with the help of an access control

system). When it comes to the organization of access control, additional requirements are imposed on the system - range of reading tags and recognition of car numbers are increased (in case of integration with a video surveillance system).

FIGURE 2. Automatic gates. (Oleg Chirkov, 2008)

- Automatic road barriers (Figure 3) - used to ensure the prevention of unauthorized passage of vehicles to the protected area. These are the measures of antiterrorism protection, because the passage through the raised barrier leads to the destruction of the suspension of the car.

FIGURE 3. Automatic road barriers. (Oleg Chirkov, 2008)

2.1.2 Identifier

The main types of performance are card, key chain, and tag. These are the basic element of the access control system, since they store the code that serves to determine the owner's rights ("identification"). This can be Touch memory, a contactless card (for example, an RFID tag), or an aging type of cards with a

magnetic stripe. The identifier can also be the code entered on the keyboard, as well as individual biometric signs of a person - a fingerprint, a drawing of the retina or iris, a three-dimensional image of the face. The reliability (resistance to burglary) of the access control system is largely determined by the type of identifier used. A higher level of security is provided by RFID tags in which the card code is stored in a protected area and encrypted.

2.1.3 Controller

The stand-alone controller is the "brain" of the system: it is the controller that determines whether or not the owner of the identifier is to be passed through the door, since it stores identifier codes with a list of access rights of each of them in its own nonvolatile memory. When a person presents (presents to the reader) an identifier, the code read from it is compared with the code stored in the database, on the basis of which a decision is made to open the door. The network controller is integrated into a single system with other controllers and a computer for the possibility of centralized control and management. In this case, the decision to grant access can be made both by the controller and by the software of the host computer. Most often, the controllers are connected to the network by means of an industrial RS-485 interface or an Ethernet local network. In cases where it is necessary to ensure the operation of the controller during power outages, the controller unit is provided with its own battery or an external backup unit. The battery life can range from several hours to several days.

2.1.4 Reader

This device, which receives ("reads") the identification code and passes it to the controller. The reader's (Figure 4) options depend on the type of identifier: for a "tablet" there are two electrical contacts (in the form of a "pocket"), for a proximity card is an electronic board with an antenna in the housing, and for reading, for example, the figure of the iris the reader should include a camera. If the reader is installed outdoors (gates, external door of the building, passage to the parking lot), then it must withstand climatic loads - temperature changes, precipitation - especially if it is a matter of objects in areas with harsh climatic conditions. And if there is a threat of vandalism, you also need mechanical strength (steel case). Separately, you can select readers for the long-term identification of objects (with an identification distance of up to 50 m.). Such systems are convenient on road passes, parking lots, at entrances to toll roads, etc. Identifiers (tags) for such readers are usually active (contain a built-in battery).

FIGURE 4. Various types of readers. (Yesenia Rosas, 2012)

2.1.5 Converters environment

They are used to connect the hardware modules of the ACS to each other and to the PC. For example, converters RS-485 ↔ RS-232 and RS-485 ↔ Ethernet are popular. Some ACS controllers already have a built-in Ethernet interface, which allows you to connect to a PC and communicate with each other without using any additional devices.

2.1.6 Auxiliary equipment

Uninterruptible power supplies, door closers, door openers, buttons, wires, video surveillance, etc.

2.1.7 Software

It is not an obligatory element of the access control system, it is used in cases when it is required to process information about passes, build reports. It is also used for initial programming, management and collection of information during the operation of the system, network software installed on one or several PCs connected in net.

2.2 ACS classification

All ACS can be classified as two large classes or categories: network systems and stand-alone systems. In my work, the biggest part will be devoted to network systems.

2.2.1 Networking Systems

In a networked system, all controllers are connected to a computer, which gives many advantages for large enterprises, but is not required for a "one-door" access control

system. Network systems are convenient for large objects (offices, manufacturing enterprises), since it is extremely difficult to manage even a dozen doors with autonomous systems installed. Indispensable network systems are used in following cases:

- If it is necessary to implement complex algorithms for allowing groups of employees with different privileges to enter different zones of the enterprise and be able to change them quickly;
- If it is necessary to selectively remove or create passes (tags) for a large number of access points or for a large number of employees (large turnover and loss of permits);
- If you need information about past events (archive of events) or require additional monitoring in real time. For example, in the network system, there is a function of photo-verification: on the gateway when an incoming person submits an identifier to the reader, the employee (guard) can see on the monitor's screen a photograph of the person to whom the given identifier is assigned in the database and compare it with the appearance of the passing one, which insures against transfer of cards to other people;
- If it is necessary to organize the recording of working hours and control of labor discipline;
- If it is necessary to provide interaction (integration) with other security subsystems, for example, video surveillance or fire alarms).

In a networked system from one place, you can not only monitor events throughout the protected area, but also centrally manage the rights of users, maintain a database. Network systems allow you to organize several workplaces, dividing the management functions between different employees and services of the enterprise.

In network access control systems, wireless technologies, so-called radio channels, can be used. The use of wireless networks is often determined by specific situations: it is difficult or impossible to lay wire communications between objects, reducing the financial costs of installing a point of passage, etc. There is a big amount of radio channel options, but only some of them are used in the ACS.

- Bluetooth. This type of wireless data transmission device is an analog Ethernet. Its feature is that there is no need to build parallel communications for combining components when using the RS-485 interface.

- Wi-Fi. The main advantage of this radio channel is the long range of communication, capable of reaching several hundred meters. This is especially necessary for

connecting objects at large distances. At the same time, both temporary and financial costs for laying street communications are reduced.

- ZigBee. Initially, the scope of this radio channel was a security and fire alarm system. Technologies do not stand still and are actively developing, so ZigBee can be used in access control systems. This wireless technology operates in an unlicensed band of 2.45 GHz.
- GSM. The advantage of using this wireless communication channel is almost a continuous coverage. The main methods of information transmission in this network are GPRS, SMS and voice channel.

It is not uncommon for a situation when the installation of a full-fledged security system can be unjustifiably expensive for the solution of the task. In such situations, the optimal solution would be to install an autonomous controller on each of the access points that need to be equipped with access.

2.2.2 Autonomous systems

Autonomous systems are cheaper and easier to operate. They do not require the installation of hundreds of meters of cable or the usage of interface devices with a computer, the computer itself. At the same time, the disadvantages of such systems include the inability to create reports, keep records of working hours, transfer and generalize information about events, and to be managed remotely. When choosing an autonomous system with high security requirements, it is recommended that you pay attention to the following points:

- The reader must be separated from the controller so that the wires through which the lock can be opened are not accessible from the outside.
- The controller must have a backup power supply in the event of a power failure.
- It is preferable to use the reader in a vandal-proof housing.

As part of the autonomous access control system, electronic locks that transmit information via wireless communication channels are also used: a mechanical lock with electronic control and an integrated reader is installed in the door. The lock on the radio channel is connected to the hub, which already by the wires exchanges information with the workstation on which the software is installed.

Additional features of access control system

- GSM module, which allows you to send SMS with information about the passage (used, for example, in schools)
- For network ACS (also some autonomous systems) - the ability to remotely control over the Internet (for example, to manage the access control system from the central office, if the enterprise has many branches).
- Complex for the personalization of plastic cards (a printer for printing data on the owner's plastic card, including photographs).
- "Antipassback" mode - if a person has already passed to the protected territory, the repeated presentation of his identity to the entrance will be prohibited (until the card is presented on the way out), which will prevent the possibility of two or more people crossing one card. At the same time, the network access control system allows to organize such a mode at all points of the passage united in the network, which provides full-function protection along the entire perimeter of the monitored territory.

3 Use of ACS

The areas of use of ACS are different:

- Offices of companies, business centers;
- Banks;
- Educational institutions (schools, technical schools, universities);
- Industrial enterprises;
- Protected areas;
- Parking;
- Private houses, residential complexes, cottages;
- Hotels;
- Public institutions (sports complexes, museums, underground, etc.)

The main types of companies on the market are:

- Manufacturers
- Distributors
- Designers
- Integrators
- Trading houses
- Mounting organizations
- End customers
- Large end customers (have their own security service)

4 IDmatic

4.1 About company

The group of companies "Control" has been working on the security systems market since 1992 and performs a full range of works: research of objects, design, production and delivery of equipment, software development, installation and commissioning, warranty and service. The company was one of the first that switched to digital technology in security systems.

The main products of the company are: integrated security systems, automated training systems, accounting and production of passes, digital television security surveillance systems, access control systems, life support systems and magnetic resonance imaging.

4.2 Advantages of IDMatic ACS

The access control system IDmatic has, perhaps, the widest set of functions and capabilities in the world.

Four-level architecture of IDmatic

The architecture of solutions and methods of hierarchical construction of a geographically distributed system IDmatic can be represented in the form of four levels or categories of objects depending on their functionality and connections.

1) Single, detached objects. For example, doors in freestanding buildings (Figure 5), turnstiles, barriers.

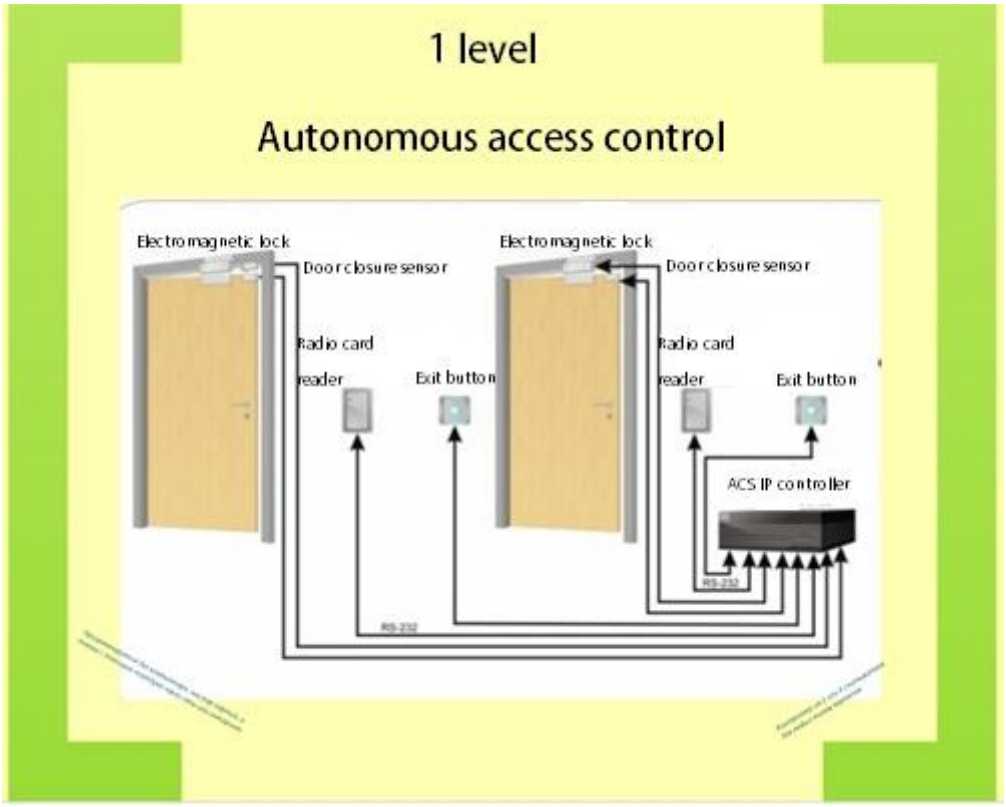


FIGURE 5. Logical plan for autonomous access control. (IDmatic, 2017)

The basis for building these solutions is the IDmatic RF controller for two or four readers with controlled relays and dry contacts for connecting sensors. The controller supports working with cards of almost all types. The controller can work autonomously. In the simplest case, for the registration of users' cards only a special administrator card is needed. For the convenience of the controller via the Ethernet network, you can connect a laptop with a special program for controlling the parameters and reading the archive of events.

Integration of a separate controller with a geographically distributed access control network is possible via an additional communication module via Ethernet, WiFi, Intranet, Internet, 3G with VPN support.

2) Small objects with a group of access points for the entrance group and doors (Figure 6).

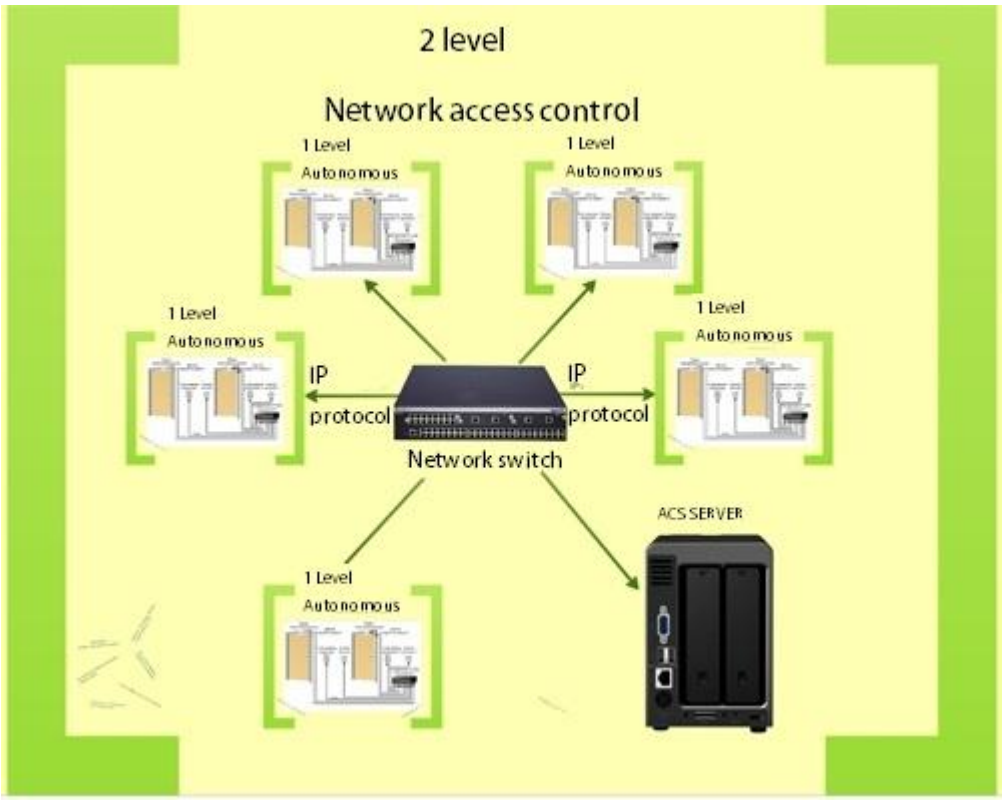


FIGURE 6. Logical plan for network access control. (IDmatic, 2017)

It takes only 3 elements to build an IDmatic ACS of any size, up to tens of thousands of doors. At the same time, its operation does not require large server capabilities, since it is created on the basis of the distributed computing environment principle. The operating system uses the Linux platform. On each of the objects there are several components installed:

1. IDMatic RF controller, to which doors, gateways, turnstiles, barriers and the like are connected;
2. An IDmatic ACS server that combines a group of controllers on the site;
3. IDmatic ST workstations for setting system parameters and monitoring events.

At this level, the number of access points usually does not exceed 32. Such objects, as usual, do not have a special security service and security administrators. Maintenance should be kept to a minimum. The main tasks are: to control an access of employees to separate premises and to control working hours.

The construction of solutions of this category of objects is based on the use of several IDmatic RF controllers, united by a computer network based on the IP protocol with the management server.

This server has a processor class Intel Atom with the operating system Linux Red Hat. To increase the reliability of work in the event of a failure of the network or the management server, the controllers go into stand-alone operation mode, and the personnel will not even notice the problem. After the network and server are restored, the archive of events from each controller is transferred to the server's shared archive. The management the server can be done either from a workstation on a shared network, or through Intranet, Internet with VPN.

Integration of the control server of a group of controllers with a geographically distributed access control network is possible via Ethernet, WiFi, Intranet, Internet, 3G with VPN support. Remote control is carried out via the WEB interface.

Each object can work autonomously or as part of a geographically distributed network of objects (Figure 7).

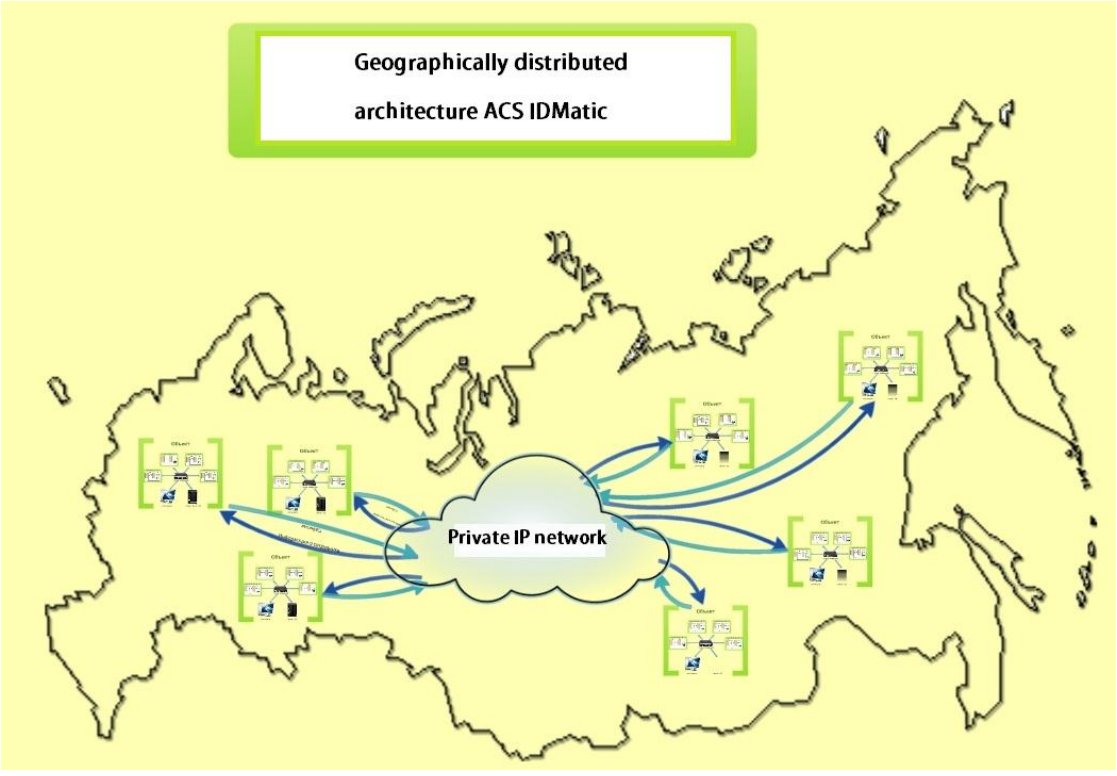


Figure 7. Logical plan of geographically distributed architecture. (IDmatic, 2017)

3) Objects of large sizes, requiring the widest functional filling and integration with various systems, including IT (Figure 8).

Figure 8. Logical plan of integrated system. (IDmatic, 2017)

The whole system in this case has certain working algorithms and has on-duty services and personnel for administration and technical support.

The IDmatic solution architecture for this category of objects is also constructed according to the principles of the computer network topology based on the IDmatic RF controllers and the management server. The hardware platform of the server in this case is much more powerful – it is based on Intel Xeon. Operating system is the same Red Hat. The number of controllers is almost unlimited. An object can contain, for example, 2,000 readers. Additional services are provided by new application servers. These servers are also based on server platforms with Intel Xeon class processors, but they have a Windows server 2008 operating system. To reduce the number of hardware servers and increase reliability, a new system has been developed on the VMware virtual platform. Workstations have processors not lower than Intel I3 class. Operating system is Windows 7. All applications are developed by IDmatic.

The following features are available in this level system:

- a system of electronic applications with the ability to encrypt EDS;
- the most economical types of paper passes with a bar code and QR code;
- gateway systems with control of passage one at a time and a group pass;
- system for entering, registering and storing the profile of passes and personal data, including passport recognition;

- Automated input of passport data and issuance of passes with the help of the terminal Fractal T;
- electronic checkpoint with photo identification program;
- a system of biometric control by fingerprint and face;
- car number recognition system;
- a single client with maps and tables to display data from all systems;
- server integration with logical scenarios to manage the algorithm of the object;
- a single meta data server with archives;
- Diagnostic system;
- GPS time synchronization system;
- a system of communication, including videoconferencing;
- a system for controlling access to computer hardware - server racks and workstations;
- a system for controlling climatic parameters and controlling air conditioners in server rooms;
- loud notification system for announcements, as well as during evacuation and fire;
- integration with video surveillance systems, fire alarm and fire extinguishing systems;
- integration with information security systems;
- integration with systems of counteraction to insiders;

The integration of any service in this category of objects with a geographically distributed access control network is possible via Ethernet, WiFi, Intranet, Internet, 3G with VPN.

4) Central management, collection, processing of information and monitoring (Figure 9).

   One of the network objects can be converted to the Control Center. This is done to solve the problem of centralized collection and information processing about the operation of the entire network of facilities and to store common databases of employees, premises and access profiles.

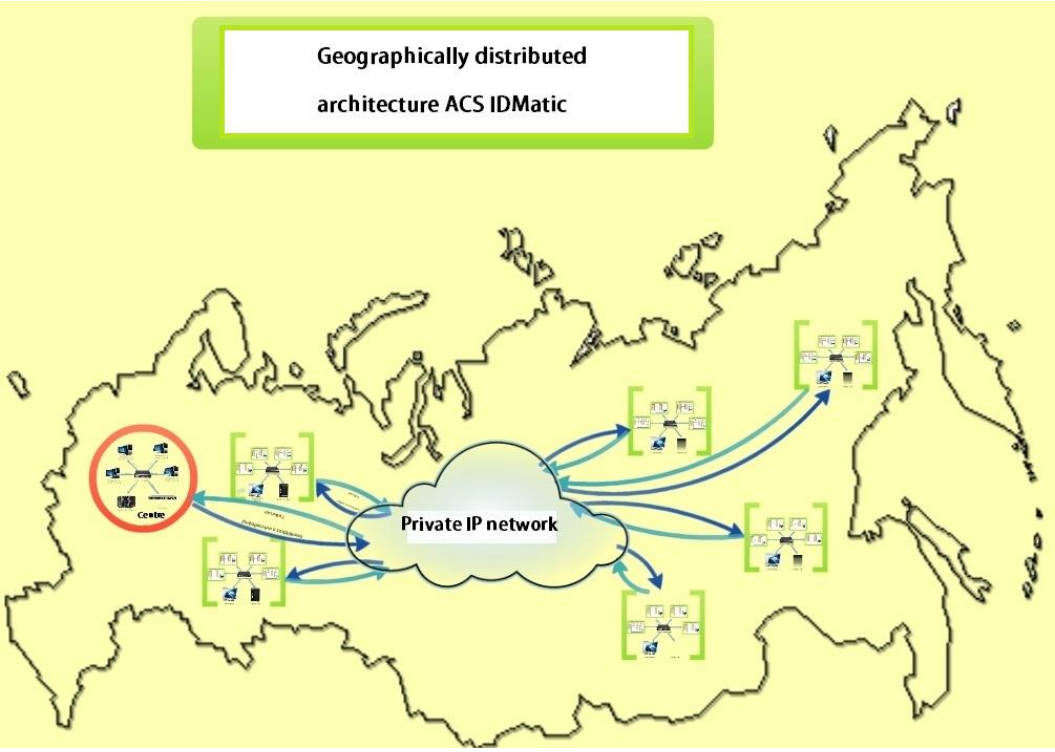


Figure 9. Logical plan of geographically distributed architecture. (IDmatic, 2017)

The control center (Figure 10) includes:

1. The server of ACS IDmatic-Center;
2. The server of the centralized Database of employees (provided by the Customer)
3. Multiple IDmatic ST workstations for management and monitoring of the whole system.

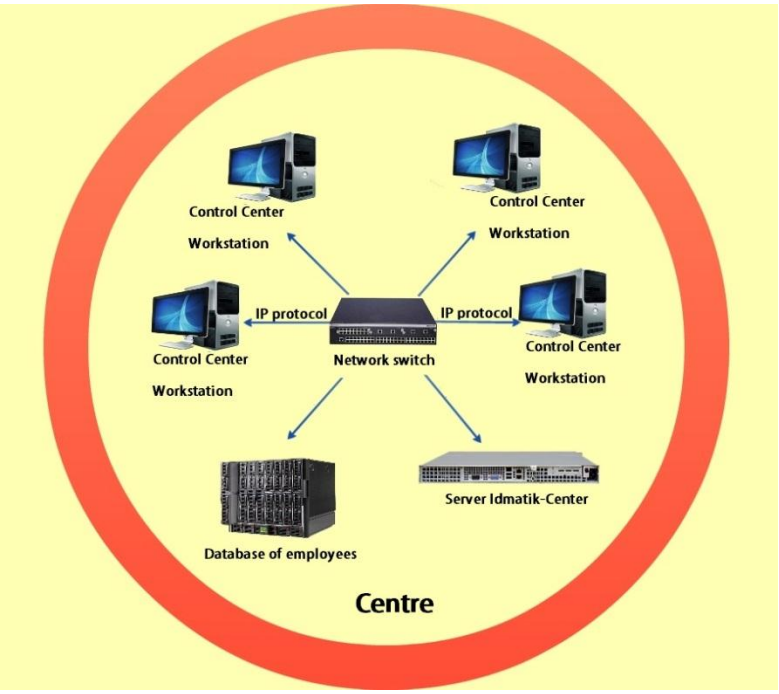


Figure 10. Logical plan of the control center. (IDmatic, 2017)

At this level, the following systems are developed

- IDmatic-center for data collection and processing by persons, passes;
- Generators of samples are used for data analysis;
- The archive system XArchive is divided into operational and long-term archives, and the capacity of the latter can reach 5 Petabytes;
- The XVmatic center system with logical scenarios can control the operation logic and the connections of all objects of the first three levels;
- In order to increase reliability and catastrophic stability, the control center can be separated into two remote territories with the possibility of both cold and hot backups.
- Internet services based on cloud technologies is developed as a promising direction for solving centralized top-level tasks.

How this system works.

On any of the objects using the workstation, you can specify the source data for the object ACS. When issuing a pass, a request is made to the server of the Employee Database. From there, information about the employee and the premises to which he can access is loaded. Information is supplemented on site by the time allowed for visiting each room.

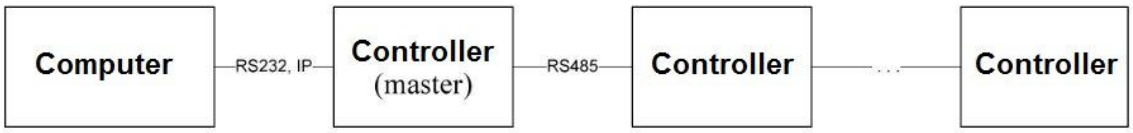
After that, all necessary data is downloaded from the IDmatic server to the object controllers. If necessary, these parameters can be managed by the workstations of the Control Center. Then the system works in the established mode.

5 Comparative characteristics of IDmatic access control system.

Access control systems are diverse. The simplest ACS can be considered an ordinary door with a latch. To automate this process, controllers with plug-in readers are used.

There are three ways to implement the ACS:

1)



Advantages:

- a hierarchical branched system

Disadvantages:

- limitations on RS232 / 485
- Increases equipment costs
- Laying additional communication lines.

To this architecture can be attributed products of KABA, Northern, Bolid, Apollo.

2)

Advantages:

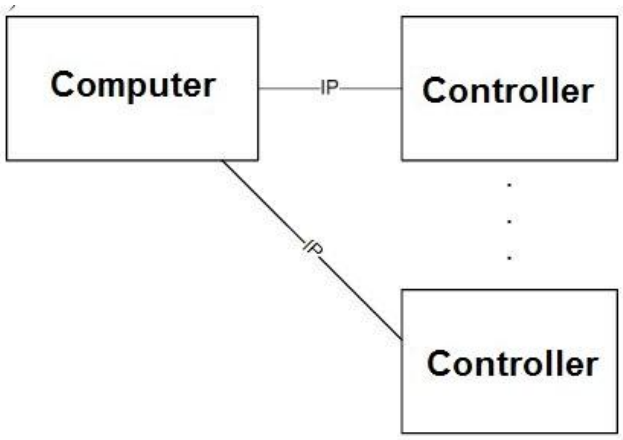
- No need in additional equipment

Disadvantages:

- limitations on RS232
- Laying additional communication lines

Implementation of the architecture – Gate

3)



Advantages:

- An autonomy
- The company's existing network capabilities are used
- Ease of implementation

To this architecture can be attributed products of IDmatic, Alfa

On the basis of the presented schemes it is evident that the basic element in all cases is the controller.

The most relevant for the controller are the following characteristics:

- Reliability
- Functionality
- Cost of equipment
- Cost of ownership
- Scalability

Based on these criteria, we will analyze controllers from different manufacturers (Figure 11). (KABA, Apollo, Northern, Perco, Bolid, Gate, IDmatic)

Parameter name	Method of evaluation	ID-matic	APOLLO	KABA	N-1000	Bolid C-200	Perco S-20	Geta
Number of stored card IDs	number	65535	16000	2000	25000	4096	10000	4072
Number of stored events	number	14560	8000	8000	6600	2047	10000	4095
Calendar with holidays and weekends	availability	yes	yes	yes	yes	yes	yes	yes
Working offline (lock management)	availability	yes	yes	yes	yes	yes	yes	yes
Working offline (recording events)	availability	yes	yes	yes	yes	yes	yes	yes
Number of types of identifiers (card, tablet, ...)	Enumeration	barcode, proxy card, magnetic card, biometric reading	plastic card, proximity, magnetic card, barcode, biometric reading	plastic card, proximity, magnetic card, barcode	proximity, barcode, code set	tablet, proximity, code, biometrics, infrared reading	proximity card, Keychain with standard EM-Marin	proximity card, code set
Mode of updating data with the server after restoring communication	availability	yes	yes	yes	yes	yes	yes	yes
Configuration mode without a server	availability	yes	no	unknown	yes	no	yes	no
Interface for connecting to the system	type	Ethernet	RS-485	Ethernet	RS-485	RS-485	Ethernet	RS-485
Number of connected readers	number	2	4	4	4	2	2	2
Fault tolerance	number (h)	120000	unknown	unknown	90000	20000	70000	unknown

Figure 11. Table with comparative characteristics. (IDmatic, 2017)

One of the main criteria is reliability. The access control system, built on the basis of IDmatic IP, has about twice the fault tolerance (120,000 hours) in comparison with other manufacturers (70,000 hours).
This is achieved through the use in the element base of components of world manufacturers, which have proven effective.

"IDmatic IP controller" provides storage of up to 65 thousand identifiers and 14 thousand events, which exceeds existing analogues. The development took into account the possibility of developing and enlarging the customer company, increasing the number of employees, the flow of visitors. In this situation the usage of controllers made by other manufacturers will require equipment upgrading and, therefore, will lead to additional costs. The controller "IDmatic IP" also supports a large number of different types of identifiers.

The IDmatic ACS is based on the use of existing Ethernet communication links. Therefore, no additional cabling costs are required. It also simplifies communication with other objects, located in other buildings, cities, countries.

The maintenance of an ACS, based on the controllers KABA, Apollo, Bolid, requires a certified specialist. To work with the ACS based on IDmatic IP, it is enough to have an idea about the structure of networks and how to transfer information. The required person can be an IT specialist, a system administrator, who can be found in any company. Consequently, there is no need for expensive training of employees. Setting up and managing "IDmatic IP" is simple and intuitive and all information is publicly available.

6 Designing of access control system

Designing is an indispensable part of creating an object's security systems. Due to the optimal design of the project, the cost of consumables, equipment and work is minimized. If the project documentation is compiled correctly, the installation and commissioning are performed quickly and efficiently.

The design includes the following steps:

- Inspection of the Object,
- Formulation of the Technical Assignment,
- Draft and Technical Design,
- Production and operational documentation.
- Technological project

Object inspection involves studying on site the exact parameters of the object, the purpose of which is to determine the set of measures and develop technical proposals taking into account the generated standard solutions.

The basis of the technical assignment is the technical requirements of the customer. These are the document from which work begins on the creation of an object security system. In addition to technical requirements, at the first stages of the design work, the information obtained during the survey of the object is used as the initial information. On the basis of the technical assignment, a Draft Design is created.

Stage "Draft Design" - the development of preliminary design solutions. In other words, the Technical Proposal is being prepared at this stage. The documentation at this stage has a general character and a small amount. As a rule, as a result of the Draft Design, the Customer receives a set of documents consisting of preliminary estimates for equipment, materials and work.

Stage "Technical Design" - as a result of deep development and justification of design solutions for the system as a whole and on its separate parts, a Technical Design is being created. At this stage of the design, the basic principles of the system operation are worked out, as well as the solution of specific tasks and wishes by the customer for each of the systems for each particular facility.

Stage "Working Documentation" - at this stage, accurate drawings, diagrams and tables are prepared, which will guide installers in the work to create the system. The working documentation provides a detailed binding of system components to the object, contains drawings, connection tables, layout plans for equipment and postings, and other documents.

"Technological project". The main difference is that at this stage both the "Technical Design" and the "Working Documentation" are prepared, that is, you receive all necessary materials for installation of the system at once.

One example of the composition of a working project (Figure 12):

- Contents of the working draft;
- An explanatory note containing the characteristics of the ACS;
- Electrical structural scheme;
- Schema of electrical connections with reference to the object;
- Drawings of placement and installation of the equipment of system;
- Floor plans of the placement of equipment and postings (including communication lines and embedded pipelines);
- Cable magazine;
- Floor schemas of cable communications of ACS;
- Specification of access control equipment;
- Drawings of installation of controllers, actuators, access identification devices;
- Drawings of equipment installation in racks, switching cabinets;
- Calculation of DC current consumption of ACS equipment in nominal mode.
- Calculation of the choice of backup uninterruptible power supplies, calculation of the total cross-section of wires and cables laid in pipes and ducts;
- Design documentation for non-standard products;
- Estimated documentation;
- Program and test procedure;
- The maintenance regulations of the ACS.

The timing of the order depends on the features of the object:

- the number of points of passage;
- complexity of the object;
- engineering communications;
- individual order.

Figure 12. Image of the amount of documentation created by IDmatic personnel for one of the projects. (IDmatic, 2017)

7 ACS installation

Last year I had internship in Kazakhstan. I was practicing in Demeu, Technical Competence Centre DEMEU Ltd. It is one of the largest companies in Kazakhstan market, which provides services in outsourcing and integrated services of technical infrastructure of large organizations.

During my internship I had many different tasks, one of which was the installation of an access control system to the business center for one large organization (the name of the organization is not disclosed).

The installation of this system was started after long negotiations with the customer. The main point was the coordination of all the details, as well as the timing of the installation works. There were also some difficulties due to the fact that the customer already purchased some equipment for installing an access control system from another supplier. And it was necessary to connect different equipment from two different integrator companies. And there was also a need to connect video surveillance to the IDmatic system.

The object for installation was a multi-storey business center. Namely, on one of the floors (#5) it was necessary to make an installation of the ACS, because there was a fairly important IT department.

There was a need for centralized management of the system and for the operational monitoring of current events. And network systems allow creating a single security information space, which increases the level of security of the object and allows for centralized management of the elements of the access control system. So the choice fell on the network system.

The integration of the elements of the access control system into a single network also provides the opportunity to organize the interaction of the ACS with other systems, such as a badge office, a video surveillance system, etc., and the creation of a single integrated security complex at the site.

Preserving all the advantages of autonomous systems, network ACS provide users a number of additional services. Network ACS allows to easily organize services such as time management, multi-level access of employees and visitors to the premises, etc.

The effectiveness cost of network ACS increases with the increase in the number of access points, but in small companies the use of network access control systems is economically justified.

The access control system of buildings is designed to distinguish between access zones in residential, public and industrial buildings and structures. The system allows to limit an access to individual rooms or groups of rooms for different categories of persons.

7.1 Information about the installed system

Access of employees to the premises is carried out by personal identifiers, such as personal magnetic passes.

When employee enters the room, the identification code is read by a special reader. The type of reader corresponds to the type of identifier used. The exit of the employee from the room, depending on the current access mode, can be carried out either with the help of an output reader (with identification) or with the help of the exit button (without identification).

In the system being installed, the input and output readers operate under the control of the IDmatic RF controller. Each controller provides control of two independent readers. This allows to use one controller to install the elements of the access control system on two doors (input - reader, exit - exit button) or to one door with two readers (input and output), including a set of door control devices (Lock opening buttons, door open sensors, electromechanical or electromagnetic locks). All controllers (ACS) are integrated into the network and operate under the control of the ACS server.

In the absence of communication with the ACS server, the controllers can operate in an autonomous mode, using information on radio cards and time zones, previously stored in the controller memory. When communication with the ACS server (ACS) is restored, the admission is carried out according to the regulations in its database. Events that occurred in the offline mode are transferred from the controllers to the server.

IDmatic AMS and IDmatic RF controllers are implemented on the basis of highly reliable computers that do not require daily maintenance.

The ACS server receives messages from the IDmatic RF controller, provides identification of users and sends back to the controller a message about the permission or prohibition of access of a person to the premises. In the case of allowing a person to enter the room, the controller sends a signal to open the access restriction device. In

addition, based on the ACS server, the functionality of the time management system and a number of other service functions are implemented. Data about the identifiers of persons are registered directly in the IDmatic AMS Server.

IDmatic AMS server provides management of all system components (Figure 13). The server provides implementation of various access control algorithms, supports the time management system, and controls the ACS peripherals (controllers).

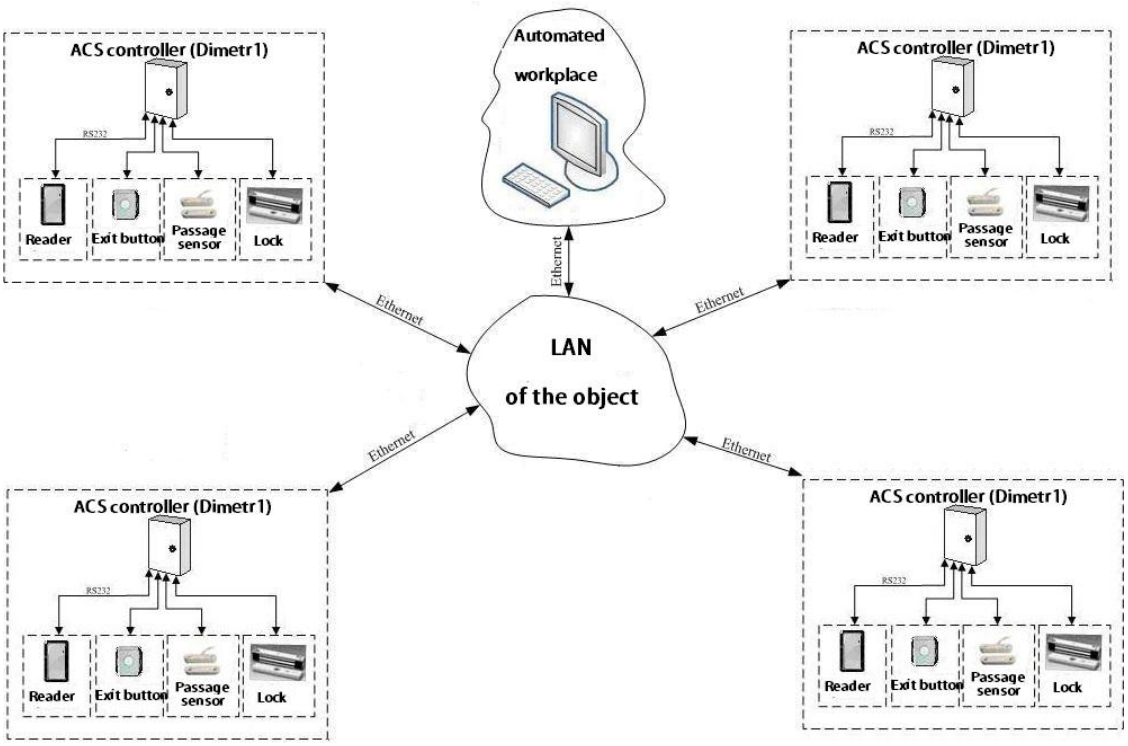


Figure 13. Logical implementation plan. (IDmatic, 2017)

IDmatic AMS:

1. Supports an unlimited number of cards with the following parameters:

- Site-code and Card number
- Cardowner
- Access level
- Card expiry date
- A sign of the validity of the card

2. Supports the list of holders of ACS cards with the following parameters:

- Personal Identifier (GUID)
- Surname, First name
- The photo
- Unlimited list of additional parameters
- Schedule

3. Supports a list of readers with the following parameters:
    - Unique name (or ID)
    - The IP address of the controller to which it is connected
    - Internal number on the controller
    - Operating mode (reading the card, barcode, card and pin code, photo identification, etc.)
    - Status (working or not)
    - The time to deny re-entry for this reader

4. Provides implementation of the anti-pass-back algorithm
5. Supports a list of access routes that are tied to time zones

The built-in security subsystem of the server IDmatic AMS allows working in the system only for authorized users.

The client program IDmatic AMS Client implements a Web-interface to work with the system, which allows you to use any Internet browser to view information and configure the system. At the same time, users have the opportunity to work in the system from any workstation connected to the network.

The client module provides the following functions:

- viewing the archive of events with filtering by calendar (year, month and day)
- adding personal personnel cards (including photos)
- the insertion of the ACS cards with the assignment of the access level, the owner, the validity period, and the sign of the valid card
- creation of access levels
- creation of access routes
- creation of checkout zones
- creation and setting of time zones (including holiday calendars and working days)
- configuration of equipment - readers and controllers
- creation, viewing and printing of reports on accounting of working hours (including viewing the list of passes per day, setting up work schedules and calendar of holidays, etc.)

7.2 Designing of ACS

When all the installation issues were agreed and the choice of equipment was made by the customer, we started the design of the ACS. For this purpose there were special people who were engaged completely in preparation of the documentation.

My task, with the help of two more experts was:

- Exploring the object
- Selection of places for installation of controllers, identifiers
- Selection of the server and its location
- The choice of places for cabling, as well as the type of cables.

In this case the design of installation of an access control system was a bit easier, because telecommunication room was on the same floor. And almost every office had a computer, so there had already been a local network. Therefore Ethernet sockets were in each of the room. We did not need to lay network cables from the controller to the server. We needed to lay the cables from the doors (readers) to the controllers and connect the cables from the controllers to the network.

7.3 Installation of ACS

Adjustment of the access control system is taking into account wishes of the customer on the basis of the agreed technical task.

Installation of ACS includes the following stages:

- laying cable routes connecting peripheral equipment with a control panel;
- installation of access control devices;
- installation and adjustment of the ACS control panel;
- installation of additional ACS elements;
- installation and configuration of specialized equipment and software;
- preparation of identification keys (magnetic card);
- creation of employee databases, assignment of individual identification keys to employees, differentiation of access rights;

The set of equipment for constructing a building access control system (excluding network and switching equipment and the administrator's workstation):

- IDmatic AMS server

- IDmatic RF controller per one (2 door readers) or two (1 door reader) of the controlled door.
- A set of door control devices (lock opening button, door opening sensor, electromechanical or electromagnetic lock, door closer) for each door. In the case of using two readers for one door, the door opening button is not used.

When all the documentation of the design of the ACS was ready it was possible to proceed with the installation. All works were carried out on the basis of the contract.

Installation of ACS was implemented on the 5th floor of the building (Figure 14).

In the telecommunications room the fiber optic cable comes, which is connected to the router. The router is connected to the switch via the internet. Next step is the routing of cables from the switch to the offices.

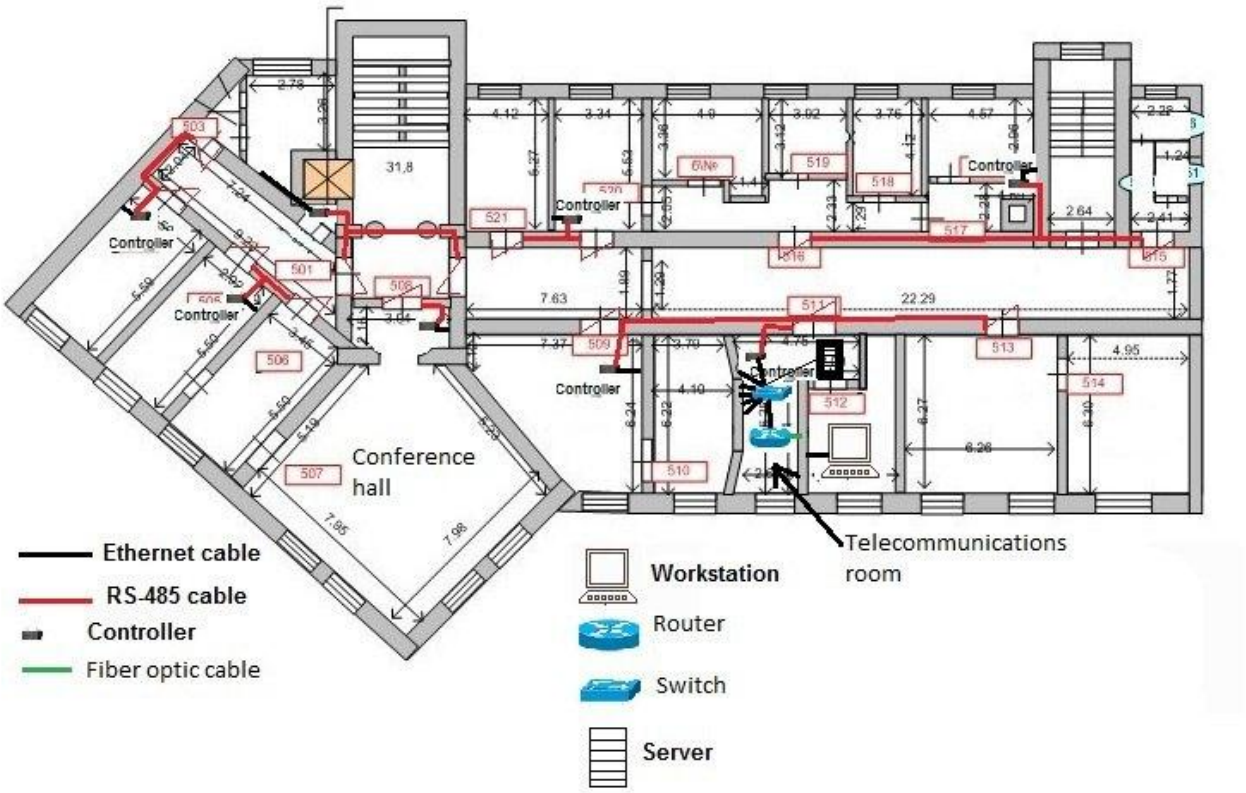


Figure 14. Floor plan of the building. (own picture, 2017)

Firstly, an installation of access control devices was made. Electromagnetic locks on the door, exit button and readers were installed. Two rooms were equipped with the help of an output reader (with identification), namely the conference hall and telecommunications room. Also in there was installed a fingerprint reader.

After that controllers were installed in their places (mostly they were fixed on the wall) to offices.

The next stage consisted in laying cables from doors to controllers and connecting cables from controllers to the network. All controllers are in the same network and each of them has its own IP address.

Then we proceeded to installation and configuration of the IDmatic AMS server. The Linux operating system and IDmatic software have been installed. A database of employees was created. The rights of employees were defined and personal cards for each employee were registered.

The main task was the configuration of the system of control and accounting of working hours, allowing groups of employees with different privileges to enter different zones on this floor of the building. And also use of an already installed video surveillance system on the IDmatic AMS server.

7.4 Benefits of system we have installed.

- the possibility of independent connection of up to two doors to one controller reduces the cost of the system per one point of passage;
- the ability to connect various types of readers;
- the possibility of expanding the system;
- Built-in software protection from external connections;
- Web-based management allows to manage the system from any computer;
- Common control center;
- Reliability (autonomous work) ;
- Ability to program without a PC any controller, regardless of whether it is connected to the information network or not;
- General Information Space;
- Convenience of programming;
- Protection against malicious software and programs.

8 Conclusion

Summing up, it can be said that an access control systems are very much in demand, since such systems can provide the required level of security at the facility.

The access control system can be installed in the enterprise, in the office, in the educational institution and so on. It allows you to control the passage, manage the rights remotely or locally, generate various reports about the events in the system. The ACS detects user IDs, transmits data to the controller and / or software, and then a decision is made as to the possibility of passage.

On the basis of this work it will be possible to learn about the access control system as whole, understand the need of this system and consider advantages; to learn the benefits of the system from the company IDmatic; consider comparative characteristics from different manufacturers and familiarize with installation process of access control system.

Besides, nowadays an access control system is widely used all over the world by various customers. There are many companies-integrators on the market that are engaged in the installation of these systems. So they need specialized employees and there is an opportunity to get a job in this field if you have sufficient theoretical and practical knowledge.

REFERENCES

Access control [web page]. [accessed 13 April 2017]. Available from: https://en.wikipedia.org/wiki/Access_control

Demeu, Services [web page]. [accessed 15 April 2017]. Available from: www.demeu.com

IDmatic, Access Control System [web page]. [accessed 24 April 2017]. Available from: http://idmatic.ru

Bolid, Access Control System [web page]. [accessed 6 May 2017]. Available from: https://bolid.ru

Introduction to Access Control Systems [web page]. [accessed 15 May 2017]. Available from: http://silvaconsultants.com/introduction-to-access-control-systems.html

William Deutsch, 2016, Introduction to Electronic Access Control [web page]. [accessed 28 May 2017]. Available from: https://www.thebalance.com/introduction-to-electronic-access-control-394578