THE MINISTRY OF DEVELOPMENT OF INFORMATION TECHNOLOGIES AND COMMUNICATIONS OF THE REPUBLIC OF UZBEKISTAN

TASHKENT UNIVERSITY OF INFORMATION TECHNOLOGIES

Allowed to defense
Head of «IS» Department
Irgasheva D.Y.______
«___» __________ 2015

Final work of the bachelor

Theme: "Development of hardware part of access management control system for enterprise"

Graduate	_______	*Alyabev I.V.*
Supervisor	_______	*Ganiev S.K.*
Life safety consultant	_______	*Borisova E.A.*
Reviewer	_______	*Zaripov O.O.*

Tashkent - 2015

Table of contents

Introduction

In conformity with the Resolution "On measures for further implementation and development of modern information and communication technologies» № PP-1730, which was adopted by the President of the Republic of Uzbekistan on March 21, 2012, current work was designed and implemented.

Protection of an object consists of several lines, the number of which depends on the level of regime object. In all cases, an important milestone will be the access control systems (ACS).

Well organized ACS will allow to solve a number of problems. The most important include the following:

- countering industrial espionage;
- opposition to theft;
- countering sabotage;
- counter intentional damage of property;
- time tracking;
- monitoring the timeliness of arrival and departure of staff;
- protection of confidential information;
- regulating the flow of visitors;
- control of entry and exit of vehicles.

In addition, ACS is a barrier for the "curious."

The purpose of current final qualification work is to make hardware part of an access control system and implement base functionality in a ‘low’ software level.

This work is devote to study basic principles of making an access control system and of solve problems during its implementation.

1. Theoretical part. Introduction to ACS

1.1. Introduction to ACS

Access control system (ACS) - is combined into complexes electronic, mechanical, electrical, hardware and software and other tools that provide the ability to access certain individuals in certain areas (land, building, room) or to a specific hardware, facilities and objects (personal computer (PC) car, safe and so on. d.) and limiting access to persons who do not have such a right. Such systems can monitor the movement of people and transport through the territory of the protected object, to ensure the safety of staff and visitors, as well as the preservation of material and information resources of the enterprise. Access control used in industrial plants, offices, stores, parking lots and car-care centers, in a residential area.

Interest in access control is increasing also because the presence of such a system is important for the efficient operation of the enterprise. Control not only significantly increases the level of security, but also allows you to respond quickly to the behavior of staff and visitors. It is also an important task for many companies is the need to monitor the schedule and keep a record of working time. Particular attention is paid to systems that allows you to build the necessary configuration of the building blocks, considering all the features of the enterprise.

Below is one of the classifications of ACS:

- control method;
- the number of controlled access points;
- functional characteristics;
- control objects type;
- the level of protection against unauthorized access.

It is possible to divide all ACS into four classes:

- ACS Class 1 - low capacity of little functional working offline and exercising tolerance of all individuals with the appropriate identifier. In such a system, use manual or automatic actuators, as well as the light and / or audible alarm;
- ACS Class 2 - mono-functional system. They can be single-level and multi-level job and provide both off and on-line. The admission of persons (group of persons) may be performed on the date, time intervals. The system is capable of automatically logging and automatic control actuators;
- ACS Class 3 and 4, as a rule, are networked. In them, the identifiers are more sophisticated and different levels of networking (client-server interfaces Wiegand card readers or magnetic cards, and other custom interfaces.).

Today, there are so many varieties of different manufacturers ACS and its components. Despite the uniqueness of each individual access control system, it contains four main elements: the user ID (card, badge, key), device identification, management controller and actuators. The general scheme of the ACS is shown in Fig. 1.1.

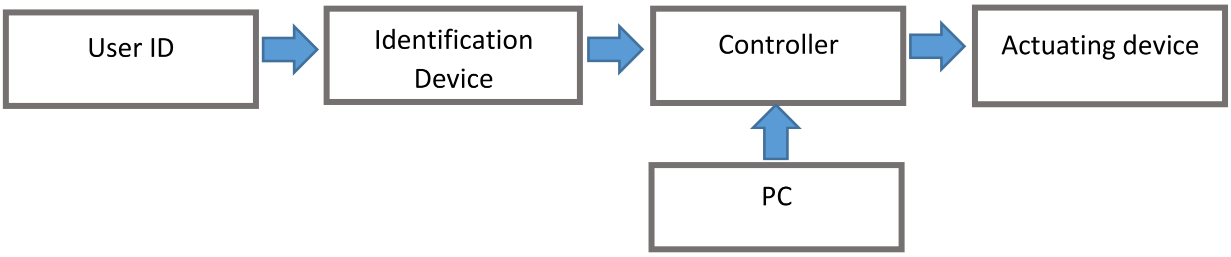


Fig.1.1. The general scheme of ACS

The work of access control can be simplified as described as follows. Each employee or a regular visitor organization receives an identifier (electronic key) - a plastic card or key ring with contained therein individual code.

Electronic keys are issued as a result of registration of these persons by means of the system. Passport details, photo (video), and other details about the owner of the electronic key entered into personalized e-card. Personal e-card owner and his electronic key code associated with each other and recorded in specially organized computer databases.

At the entrance to the building or premises to be monitored are established readers that read the cards with their code and information about the access rights of the card holder, and transmit this information to the system controller.

Depending on the method verification there are several types of ACS:

- manual (defining the identity of the controller is carried out based on the charge against skipping a photograph of the holder);
- mechanical (in fact, the same manual check with elements of automation of storage and presentation of passes);
- automated (user identification and verification of personal attributes made electronic machine and the operator checkpoint performs authentication and decision to grant access)
- Automatic (the whole test procedure and the decision by the computer).

A set of functions performed by complex systems, enables the use of the control system to perform various control tasks on site. Depending on the task at hand, you can choose an appropriate system of access control. Partly ACS will prevent access to undesirable persons, and employees to pinpoint those areas in which they have access. A more complex system will allow, in addition to restricting access, assign each employee an individual time schedule, save and then view the information about the events of the day. Integrated security systems allow solving the issues of security and discipline, to automate HR and Accounting, create a workstation guard.

When choosing a system structure and its equipment it is necessary to pay special attention to thorough analysis of its characteristics.

The main characteristics of the ACS are:

- cost;
- reliable operation;
- speed;
- time of registration of the user;
- storage capacity;

- resistant to malicious acts;
- the likelihood of false rejection legitimate user;
- the likelihood of false illegal user access.

1.2. User identifier

User identifier - a device or an indication which identifies a user. For identification attribute and biometric identifiers are used. As a stand-alone media attribute identifiers signs tolerance used: magnetic cards, contactless proximity card, key "touch-Memory", different key fobs, the image of the iris, fingerprint, handprint, facial features, and many other physical signs. Each identifier is characterized by certain unique binary code. The ACS each code is associated with information on the rights and privileges of the owner of the ID. Currently used:

- contactless RFID proximity card - the most promising at the moment type of card. Contactless cards are activated at a distance and do not require a clear positionning, which ensures stable operation and ease of use, high capacity;
- magnetic cards - the most widespread option. There are cards with low coercitive both highly magnetic stripe and recording on different tracks;
- Wiegand Cards - named after the scientist who discovered the magnetic alloy with a rectangular hysteresis loop;
- bar code card - the card is applied to a bar code. There is a more complicated version: bar code is closed by material, which is transparent only to infrared light, reading occurs in the IR region;
- key-fob touch-memory - a metal tablet in which the chip is the ROM.

ACS permits of users (identifiers) may have a different status. To ensure the most essential requirements in real life, at least, it is necessary that the controller supports the following types of cards:

- constant: to the company's employees;
- time: the limited period of validity;
- X-time: automatically annihilated after the exhaustion of the number of passes;

- disposable - a special case, and single-card.

1.3. Controllers

Controllers - devices for processing information from the reader IDs, decision-making and control actuators. This controller allows passage through checkpoints. Controllers differ database capacity and event buffers, serviced identification devices.

Any ACS controller consists of four main parts (Fig. 1.2): reader, signal processing circuits, the decision and the buffer circuit events.

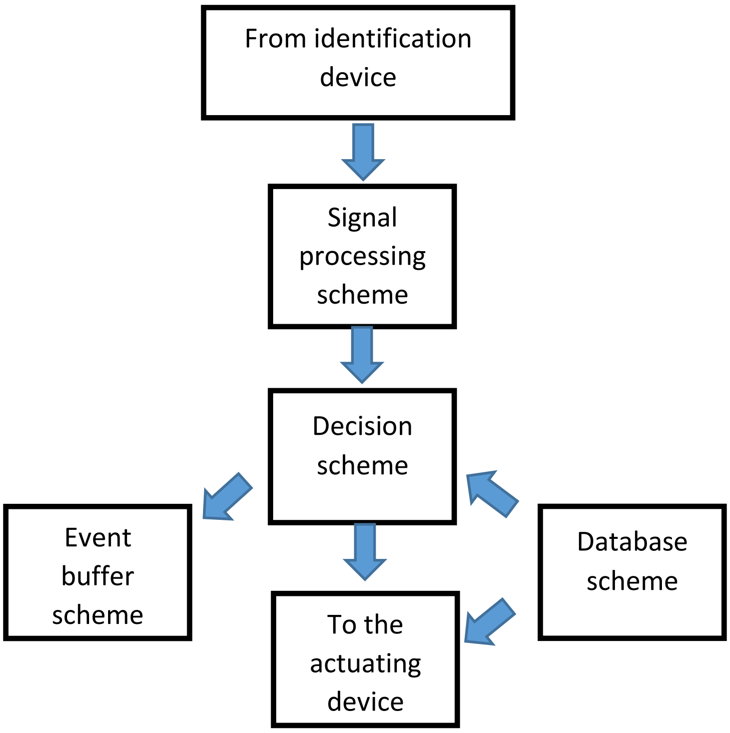


Fig.1.2. ACS controller scheme

Card reader device transmits information to a signal processing controller. Further information in digital form is issued for the decision logic that puts the fact of attempted pass into the scheme of the event buffer, it asks the database schema for the eligibility of passage and, if so, drives the actuator. Limitation already removed, but access control system has not yet completed the processing of information: the mere fact of passage of this particular person is entered in the event buffer circuit.

According to the method of management (the possibility of unification) ACS controller is divided into three classes: autonomous, network (centralized) and combined.

Regardless of the type of reader controllers must support the following access modes:

- one card and / or PIN code;
- Access with the confirmation by the operator;
- Control the number of people in the room (minimum and maximum).

The last is important in situations where, for example, under a given service in the environment must not be less than one (two or three). The basis of modern security systems make automatic and automated access control. They verification procedure may also include a comparison of the audited entity with the filmed on the monitor controller. Modern automatic and computerized security systems, depending on the method of management are divided into autonomous, network (centralized) and distributed (combined).

Autonomous controllers - completely finished devices intended to serve, as a rule, a single point of passage. The possibility of combining with other similar controllers are not available. There are many types of such devices: controllers combined with a reader, controllers, embedded in the electromagnetic lock and so on. In stand-alone controllers, various types of readers are used.

Typically, the autonomous controllers designed to serve a small number of users, usually not more than 500. They work with a single actuator without transmitting information to a central point guard and without the control of the operator. An example of such an access control system can serve as a fairly simple combination of "electromagnetic lock + card reader identification". If you want to control only one door in the future expansion of the system of access control is not planned, it is the best and only affordable solution.

Network controllers can be controlled by a computer over network. In this case the decision is made by a personal computer with specialized software. Network controllers are used to create access control systems of any complexity. The number of network controllers in the system can be from two to several hundred with an exchange of information with the central point of the protection and control, management system by the attendant. In this case, the dimensions of the system are determined by the access control device identification number, and not controlled by the number of doors, since each door can be equipped with one or two identification device depending on the technology used passageway.

Using network controllers, the administration receives a number of additional features:

- Receive a report on the presence or absence of employees at work;
- Clarification of the concrete location of the employee;
- keeping timesheets;
- drafting of the report on the movement of employees virtually any period of time;
- formation of the passage of time schedules of employees;
- maintaining a database of employees (e-filing).

Network access control systems are used in large enterprises and in those cases, if you need its specific features, such as keeping employee time. Network controllers are networked. By the basic characteristics of network controllers include the following quantitative characteristics:

- the number of supported passage points;
- The amount of database users;
- The amount of buffer events.

The number of supported passage points. The optimal solution in this case is the following: a network controller for two access points, as shared resources (housing, power supply with battery) are required in smaller quantities. Controllers with a large number of service doors there, but many of them for the following reasons:

- the high cost of power for 4-5 A redundant;
- increasing the cost of communications between the controller and doors.

Moreover, if the doors are located far from each other, it becomes a problem and wire lock power supply, since the consumption currents of about 1 A large losses occur.

The amount of the user database is defined exclusively of people who will walk you through the most intense point of passage (checkpoint).

Volume of the event buffer of determines how long a network system can work when power off (hovering, burnt) computer, without losing information about the events. For example, the number of office staff of about 20 people the buffer size of events of 1000, may be enough for a week. And for the factory entrance, through which three thousand. People and buffer 10,000 of events hardly enough for a day.

Almost all controllers support Wiegand interface, and virtually all types of readers, including biometric support this format.

Modern access controller must support flexible time schedules on which the decision on access of a person. This standard weekly cycles with days off - this is the most simple solution. Really want to ask more holidays, weekdays during the holidays, and most importantly different "floating" graphs in an "after three days" and so on. N In the professional controller time schedules can manage not only the user access, but also automatically open and close the doors to given time to arm and take a room with a guard (with security functions) to switch auxiliary relay.

The combined controllers combine the functions of the network and stand-alone controllers. If you have a connection with the host computer (online) controllers operate as a network device in the absence of communication-as autonomous.

1.4. Identification devices (readers)

For personal identification, modern electronic access control system is used in several types of devices Depending on the type of user ID.

Identification devices (readers) decode information recorded on cards or other types of keys and transmits it to the controller often in the form of digital sequences. Readers access cards can be contact and contactless. The following ways to enter characters:

- manually, by pressing buttons, turning switches and so on;
- pin - as a result of direct contact between the reader and the identifier;
- remote (non-contact) for presentation ID to the reader a certain distance.

To remove the information about the biological signs of human use special biometric readers (terminals), and enter the PIN using the keypad types.

That readers determine the appearance and the basic performance of the entire system. Consider how they work. Button keypad. The principle of operation is quite clear: if the keypad access code is correct, the passage of the protected area is allowed. Code-dial devices are sometimes combined with a card reader, in this case, the code is to confirm the authorized use of the card.

Barcode readers at the moment virtually installed in the access control system as extremely easy to fake a pass to a printer or copier.

Magnetic-card reader. The main element of the magnetic card reader is a magnetic head, similar to a tape recorder. Identification code is read while moving magnetic stripe cards.

The main advantages of these identifiers:

- the cost of readers and magnetic cards is quite low;
- you can change the code by using a magnetic card encoder.

The main disadvantages:

- protection against unauthorized access is low because the offender, having captured a very limited time a foreign card, it can forge many duplicates as it needs;
- magnetic-card reader rather unreliable in operation: magnetic heads become clogged over time and shifted;
- low capacity of such a system of access control, as is often necessary to identify the magnetic card several times;
- magnetic stripe cards require very careful storage, it is necessary to avoid exposure to electromagnetic fields.

For these reasons, complex access control system are rarely equipped with devices such personal identification. Magnetic subway maps - an exception to the rule, because of the cheapness of technology.

Readers of contactless cards (Wiegand). The reader is an induction coil with two magnets, which is in a plastic or metal body and a complete seal is filled with a special insulating material. When carrying out a plastic card through the reader access control system receives the binary code of the card. Reading is carried out non-contact induction method.

The main advantages:

- High reliability due to the simplicity of the device;
- impossibility of a fake credit card, as there is no information on the structure;
- high resistance plastic card to external shocks: to spoil the card, it must be broken.

"Touch Memory” readers. "Touch Memory" Reader is very simple and consists of a pad is actually intended for the special touch of the keys. The key "touch Memory" is a chip placed in a cylindrical stainless steel housing.

1.5. Actuating devices

Among access control actuators, the most common are: locking or managed blocking devices: locks, latches, turnstiles and sluice cabin, automatic gates, elevators. In modern security systems, electromagnetic and electromechanical locks are mainly used.

Door locks and latches. Principle of operation, which is used in electromechanical locks and latches is very simple: when feeding on their special contact terminal voltage (typically in the range 9-16 V) the solenoid pulls the stopper mechanical device allowing to open the door. Powerful pluggable electromechanical locks safe type when voltage is applied to a special electric motor is carried out in the movement of locking pins in on construction sites it is advisable to use electro-mechanical locks, and if necessary to quickly install an access control system on the existing site is better to use electromechanical latches that allow the use of existing mechanical locks . Electromagnetic locks consist of an electromagnet is attached to the door frame, and the response of the metal plate mounted on the door. In standby mode, the coil of the electromagnet is energized with DC holding current, which causes a strong magnetic field, which attracts a metal plate door, holding it closed. When a signal is applied to the special input of the magnetic field disappears and the door can be opened.

All electromagnetic locks are characterized by maximum mechanical load retention, which is measured in kilograms and can reach up to 1,000 kg.

Door closers, which returns the door to its initial position, always should be used with door locks.

The advantage of the electromagnetic locks - a small, compared to electromechanical locks, current consumption and a lack of impulse surge when opened. The negative side - large, dull industrial design and the complete dependence on the availability of power.

Turnstiles. Turnstiles and access control systems can be divided into two types: Full height and waist. The principle of operation of the turnstile is well known that if the access request is legitimate, the mechanical system, turning, opens the passage to the protected area.

Belt turnstiles belt leaves allow the jumping over, because, like their name suggests, protecting barrier comes only from the waist up man, so they should be considered only next to the guard post.

Full height turnstiles can be installed in remote locations and guard post used in a fully automatic mode.

Automatic barriers and automation for gates. Gates can be hinged (ram their resistance is not very high and they require cleaning the roadway in front of the gates of snow and ice), sliding, lifting and rolling. As attribute identifiers on the vehicle used waybill, stating the registration number of the car, the driver and the name of the person responsible for shipping (often these functions are performed by the driver), type and amount of cargo. Identity of the driver and passengers are their badge.

Modern security systems and remote vehicle equipped attribute identifiers (such as proximity) inspection of transport means (special mirrors and Industrial Group), as well as on the most important objects - anti-terrorist tool for extra-term stop cars trying to ram the gate. The latter means is a metal column (blocker) to50 cm in diameter, which is installed in front of the gate from the outside in concrete or metal well. At the bottom of the well placed can of compressed air and squibs, which explodes on the electrical signal from the gearbox, and the compressed air rises column for a split second in front of a moving car. This lock can stop the 20-ton vehicle moving at a speed of 60 km / h.

Elevator controllers. The principle of operation is as follows. Access control system for personal code determines the available floor and trying to get on any floor, coming out of this range, blocks the movement of the elevator into the forbidden sector. In addition to access control based on reader access cards, access control systems are used on the basis of video intercom and access control based on the turnstile, the reader access cards and video intercom.

ACS based on the principle of operation of a video intercom system is based on transmission of video from a camera mounted on the front door or in its area, to monitor security post. The system also includes remote door opening system based on the electromechanical lock and intercom. The system can be complemented with a video recorder, a leading continuous recording camera signal. Installation of additional cameras for security systems integration and video surveillance systems require installation "multiplexer" - a device that outputs a signal to the monitor at the same time from multiple cameras.

ACS through the turnstile, the reader access cards and video intercom. This ACS is a model project for a business center or any other complex premises. Employees are in a complex of rooms for individual access card reader which controls the turnstile located at the guard post. After hours (weekends, holidays, night) pass through the main door is locked electromechanical lock. Intercom and outdoor video surveillance systems enable protection of the front door to remotely control the front door after hours, when the door is in "always closed" in contrast to the working time "is always open." In after hours, such a system can reduce the number of security guards without compromising security. In the framework of the turnstile metal detector can be located.

1.6. Requirements for Access Control System

As mentioned above, access control systems (ACS) designed to provide authorized entry to the building and access to restricted areas and leaving through the identification of combinations of different signs, as well as to prevent unauthorized passage of the premises and the restricted area of the object.

ACS should consist of barrier-controlled devices (BCD) in the composition of the barrier structures and actuators; Input Devices indicia composed of readers and identifiers; control unit (CU) n composed of hardware and software.

Readers and BCD are equipped with main and service entrance, check point, areas that directly focused wealth, facilities management, other premises by a decision of the company's management. Skip employees and visitors to the object of the enterprise through access control points should be made to the building and offices - one basis; entrances to restricted areas (storage box, safe rooms, storage rooms of weapons) - for at least two characteristics identification.

ACS should provide the following main functions:

- BCD opening when reading an identification tag, access to which is permitted access to the zone (room) in a given time interval, or by the access control operator;
- prohibition of opening the TOS when reading an identification tag, access to which is not allowed access to the zone (room) at a predetermined time interval;
- protection against unauthorized access to the software to change the CU (add, delete) identification signs;
- protection of hardware and software from unauthorized access to the controls, the mode setting, and to information;
- save settings and database indicia during a power failure; manual, semi-automatic or automatic opening for the passage of BCD at emergencies, fire, technical faults in accordance with the rules and regulations established by the regime of fire safety;
- automatic closing of BCD in the absence of the fact of passage through certain time after reading the authorized identification tag;
- alarm signal (BCD or blocking a certain time) when trying selecting indicia (code);
- the registration and recording of current and alarms;
- autonomous operation of the reader with BCD at each access point in case of failure due to the CU.

At the sites of the enterprise, which is necessary to monitor the safety of subjects, should be installed ACS controlling unauthorized removal of these items from the rooms or buildings protected by a special identification mark.

BCD with actuators must provide:

- partial or complete overlap of the passageway;
- automatic and manual (emergency) opening;
- Blocking insider BCD (for gateways, walk-through cab);
- amount of bandwith required.

Readers of Identification attributes input devices (IAID) should provide:

- Reading identification tag with IDs;
- comparison with the introduction of the ID tag is stored
- The memory or database CU;
- Signal to open BCD in the identification of the user;
- Exchange information with the CU.

IAID must be protected against manipulation by searching or selecting identification attributes.

IAID identifiers must arrange to keep the ID tag for the entire life of the identifiers without built-in elements of the power supply and at least 3 years - for identifiers with built-in power supply components.

The design, look and feel of the inscription on the identifier and the reader should not lead to the disclosure of the code.

CU must provide:

- receiving information from IAID, processing, display in a predetermined manner and the production of control signals BCD;
- database maintenance staff and visitors with the ability to specify object characteristics of access (code access slot, the level of access, etc.);
- maintenance of an electronic log of employees and visitors passes through the AP;

- Priority display information about the alarming situation in the access points; monitoring health and status BCD, IAID and communication lines with them.

Structurally, the ACS should be built in a modular fashion and provide:

- interchangeability of replacement the same type of technical equipment;
- Ease of maintenance and operation, and maintainability;
- removing the possibility of unauthorized access to controls;
- authorized access to all elements, nodes and blocks, requiring adjustment, maintenance or replacement during operation.

1.7. Identification and authentication tools

Identification cards with a magnetic track. This type of car-points was developed in the 60s. XX century, but it has since been significantly improved: increased data capacity, durability, increased protection from abuse. Early samples of the recording of information was carried out by a magnetic field strength of 300 Oe. It does not provide reliable protection against accidental or deliberate erasure. In addition, the recording magnetic field intensity so allows an attacker to simply forge such cards, without the help of sophisticated equipment. It managed to overcome these disadvantages by the use of special magnetic materials requiring a recording magnetic field of 4000 Oe. Such magnetic materials in the late 1970s. It became the first company to apply the ZM. Currently achieved recording density of 75 bits / cm. High density recording enables the card to store a sufficiently large amount of information.

To enhance the security of cards, along with the usual information about the owner, can be applied, for example, a special security code that describes the structure of the material from which they are made. This method was used by Copytex GmbH (Germany), where we used the fact that each card has a unique structure of the material, which can be fixed by means of appropriate technical means. When issuing cards in circulation structural features of its foundation in the digital code is recorded on the magnetic track. When testing special optoelectronic device scans the card reader terminal, shining through its surface, after which the system automatically determines the compliance of the data recorded is loosed code.

Identification cards with magnetic barium-ferrite interlayer Coy. In such cards is a middle magnetic layer "sandwich" of the base substrate (with a photo and personal data of the owner) and the plastic cover. Disposed therein and polarity charges barium-ferrite particles form code. The advantage of such cards is a very low cost in comparison with all the other species, and increased protection against copying. However, they do not provide reliable protection against accidental or intentional deletion or change the embedded code.

Additionally, they are insufficiently durable. Their field of application is limited to those areas that do not require any high level of security in controlling access.

Identification cards encoded on the basis of Wiegand. The basis of such cards are embedded tiny pieces of thin ferromagnetic wire of a special form (located in a strictly defined sequence different for different cards), which contain information about its owner's personal code (Fig. 1.3). When you attach a card to the reader, these so-called "Wiegand wire" cause a change in magnetic flux that fixes the corresponding sensor that converts the pulses into a binary code. Wiegand coding technology provides a very high degree of protection of identity cards against accidental and deliberate erasure rigging fixed code and duplication.

Fig. 1.3. Contactless card (Wiegand interface)

Contactless RFID proximity card. Reader generates electromagnetic radiation of a particular frequency and in making the card reader within range of this radiation through a built-in antenna in the card powers the chip card. After receiving the necessary energy to work on the card reader sends a unique identification number by means of an electromagnetic pulse shape and a certain frequency.

The very proximity card consists of a transceiver antenna and an electronic chip (Fig. 1.4).

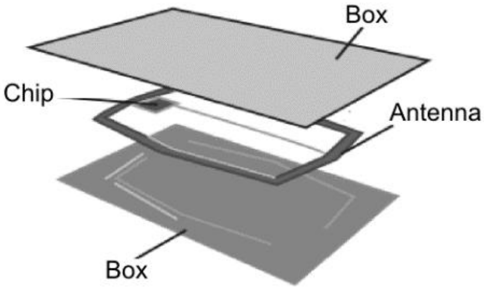


Fig. 1.4. Proximity card

Identification cards with hidden bar code (bar code). The invisible bar code imprinted on the base card and read by radiation in the infrared spectrum. The code generated by the configuration of the shadows during the passage of infrared radiation through the card and has a high degree of protection against forgery. However, this technology freely expensive, although the cost of these cards and lower than the cost of cards Wiegand.

Identification cards with optical memory. Encoding information on such cards made approximately the same as when recording data on optical discs - computer storage media. Reading is done by laser. Modern technology provides a very high recording density, so the storage capacity of such cards is calculated in megabytes. This makes it possible to store not only alphanumeric data and images and audio information. Cards of this type have a low cost and a high degree of security against unauthorized copying. However, the high density data storage requires rather careful attitude and complex reading terminals.

Identification cards with artificial intelligence (smart card). These documents provide the foundation built in miniature integrated circuits - memory and a microprocessor. One advantage of this type of cards - the possibility of registering the identity of a significant volume. They have quite a high degree of protection of the information stored in them from the rigging and all kinds of abuse. In the literature, there are other names for these cards - "smart" or "intelligent." Computing microblocks this card contains three types of memory. For storage software designed type ROM memory in which information is entered by the manufacturer at the stage of manufacture cards in circulation and does not allow making any changes to the stored instructions.

To store the intermediate results of calculations and other data of a temporary nature used memory type RAM (random access memory). It is managed by an integrated microprocessor which monitors the process of interaction with the reader. After disconnecting electrical power information is not saved.

Memory of the third type - programmable read only memory (PROM) - provided to the user to record personal information. She is also under the control of the built-in microprocessor, t. E. Only for his team in this memory can be made any changes. The recorded data is not erased and disconnected power supply. In this type of memory is usually divided into three zones: an open access, and secret working. The open area may be stored, for example, your user information (name, address, and so on. F.), Which allowed unauthorized reading terminal of the appropriate type. However, any changes in the records may be made only with your permission and with the help of special equipment.

The working area is used for entering specific information, and reading the change which is allowed only at the user and with the appropriate technical means.

In a secret area recorded identifying information such as serial number or passcode. In addition, there is usually stored and territorial temporary user credentials for access to protected sites and premises. Information classified areas can be read only by the terminal access control system, which is designed for this card. Changes are also being made only by command of the system.

Stored data is not disclosed to any outside reading equipment, including the manufacturer. Sensitive information recorded in this zone when the user logs checkpoint system. Until recently used as such a memory storage device EPROM (erasable programmable ROM). Information entry can be erased only by UV radiation and special equipment. A more advanced type of memory is an EEPROM - electrically erasable programmable read only memory, which unlike the previous more durability (service life - up to several years) and is more flexible.

Some smart cards allow you to store digital images of the biometric characteristics of the user (dynamic painting, fingerprint, palm, geometric parameters of the brush pattern of the fundus, the portrait image). In order to protect against unauthorized use of identification cards used by users of such systems, electronic "portrait" is stored in memory in digital encrypted, which greatly complicates the recovery of the recorded information and its fake hackers.

Contactless ID cards. These cards do not differ in appearance from the others, but along with the usual trappings with a built-in miniature-held transceiver that provides remote interaction with the reader access control system. As a means of communication in remote reading can serve as directional electromagnetic field (microwave radio signals), the optical beam (infrared light) or acoustic waves (ultrasound).

Feature contactless reader compared with other types of devices is that the outer part of their structure (an antenna) can be mounted, eg in the wall next to the door secured. This ensures secrecy and thus protection from attempts of physical destruction. The distance at which communicates with a contactless ID card antenna of the reader, modern contactless checkpoints machines may vary depending on the particular model from a few centimeters to 10 meters and more. The most widespread now have microwaves readers and ID cards with built-in electronic circuitry or "electronic tokens" (which the user can wear in the inner pocket, briefcase or attached to a keychain). These identifiers are also called "electronic labels".

There are two types of electronic tags: passive and active.

Passive electronic tags. They work is based on re-emission electron energy from the microwave transmitter terminal. Re-emitted signal is detected by the radio terminal, and then fed the appropriate commands to unlock the door mechanism. Semi-active electronic tags. It contains miniature battery, which is a source of power for the transceiver. Himself transceiver is usually in standby mode, and if it enters the zone of the microwave transmitter sends a signal post of a certain frequency, the receiving terminal of the system.

Active electronic tag. It is a microwave transmitter-beacon transmitting a signal of a certain frequency (for some models coded) continuously.

The simplest model of contactless terminals checkpoints, the development of which began in the early 1970s. in the USA, can only transmit baseband signal without dividing members individually. In the future, with the development of electronic technology appeared identification cards, which in addition to the transceiver chip includes in its membership the memory. This memory stores multi-valued code that the exchange of signals is transferred to the control terminal and is identified in accordance with the authority of a particular user.

Special electronic readers’ proximity identifiers recognize the identity of the owner of the ID recorded on the personal code. The mechanism of recognition (reading) based on remote radio frequency technology. Proximity reader constantly sends a radio signal. When injected into the zone of the proximity reader identifier is activated and sends a response signal comprising a unique access code recorded in the memory of its electronic circuit. Reading code proximity identifier occurs at a certain distance from the reader, without direct contact. This relative positioning identifier reader does not matter.

All proximity identifiers are divided into two groups - active and passive.

Currently there are both active and passive proximity identifiers. Passive proximity ID does not contain built-in energy source, it is completely sealed and has a virtually unlimited service life. The distance at which it is stable, is 10 to 50 cm away from the reader. Typically, these identifiers are used for fast and reliable service a large flow of people, such as the admission of the company through the checkpoint. Active proximity ID can operate at a distance of one to three meters, but it requires constant monitoring of the degree of built-in battery and its timely replacement (usually not more than 5 years).

All HID proximity identifiers have a high degree of protection against forgery. Due to the lack of mechanical contact between the proximity reader and the ID, the ID does not wear out, and its service life is practically unlimited. Proximity IDs have sufficient mechanical strength, resistant to bending, impact, are not afraid of moisture and dirt.

In proximity identifiers can be applied labels, photos, logos. For this purpose, special PVC labels, and images and graphics on the surface of thin proximity identifiers are printed on special printers.

Plastic keys. Plastic keys are used in all the above encoding methods. Their difference lies in the constructive way of unlocking that looks like a way to unlock the conventional mechanical lock - insertion of the key into the lock, access control and an indication of the key owner permission to open the lock (turn key).

This identifier has a higher degree of wear resistance as compared with the identification card. The memory of such key stored personal number of the owner verification principle is based on comparing user input numbers with the number stored in the memory key that is read by the terminal when it is inserted into the slot.

Memory of the key usually contains the following information:

- system identification number (unique to each installation, and available by the manufacturer when ordering the system and the maximum number of different system numbers more than 65 thousand.);

- user identification number (determined by the buyer when issuing and programming key, you can order up to 9999 different numbers);
- access levels (for offline reader for up to 256 levels of the system provides access from this level or higher);
- days of the week (7 days a week correlated with time zones, a combination of day and time zone defines the right of access through any reader at any given time);
- time Zones (each system has up to 16 separate zones that can be assigned to the user);
- code dial pad (for important objects in the key memory can store up to 10 different numbers).

Terminals based on a combination of reader and code dial device. Combining identity authentication methods can improve the protection against unauthorized access. However, this increases the runtime checking procedure.

Currently, various foreign firms mastered production a number of models. Of greatest interest is the combined terminal of Security Dynamics company. Used identity card (similar in size to a standard credit, but twice as thick as it) contains a built-in microprocessor, a miniature power supply, liquid crystal display, digital clock, as well as two storage units in a type - random access memory (RAM) and permanent (ROM) . Every minute is displayed on the display the number of pseudo-random sequence generation algorithm which is known for microcomputer systems. So that the terminal "knows" a particular number on which identification cards, in which particular time period will be recorded. Essentially, this is a pseudo-random number in the password within 60 seconds. The verification procedure is as follows. The user enters via the keyboard your personal identification number, then the number that is currently displayed on the display of his identity card. The system determines the correct number of cards for this length of time.

To counter threats to intercept legitimate user personal identification code can be programmed such an opportunity when, instead of separate data entry owner identification card typed on the keyboard identification number and the amount of numbers read on the display.

1.8. ACS features for large distributed objects

The ACS for large distributed object with different architectures swarm uses powerful central controller performing the control process using specialized remote interface modules. Features of the application determine the requirements for the software for such systems most commonly used access control system with a centralized or distributed architecture, but sometimes used and the architecture of the mixed type.

1.9. The centralized architecture of ACS

In large, distributed access control, especially at large distances between the individual buildings protected object, every building must have its central controller. This provides stand-alone operation of the security system of each building in the event of breakdown in communication between the individual objects. The number of connected readers per controller, usually ranges from 16 to 96, so it is usually a power controller is enough to create a single object ACS in a large distributed system. Centralized access control system controllers are purely logical devices not controlled doors, t. E do not have a lock control relay outputs, inputs for connecting readers ACS management functions doors and other external devices perform external interface modules and relay units. They are usually installed near the control objects (doors, security cables, etc.). For the exchange of information between the controller and interface modules most commonly used

RS-485 interface, but there is already a system in which it is possible to connect interface modules for LAN standard.

It should also be noted that the most powerful central controllers have several communication interfaces RS-485, which provides a broad coverage of large buildings without the use of amplifiers, interface. In fact, you can pave your RS-485 interface in several ways from the central controller. As for the network interface, the large object interface modules can be connected to a central controller ACS standard LAN is very relevant, because in this case there is the prospect of using the existing on-site network infrastructure and significantly reduce the cost of laying communications. The controller in systems with centralized architecture keeps all database identifiers and events in the system. It is usually located near the control computers (servers) in places the highest security (guard room, server, and so forth.). Separating the functions of decision-making and management directly increases the security of access control as the controller itself is well protected and set at a distance from them managed TOS In addition, this approach helps reduce the cost of larger systems as the price of the controller "dissolve" in the overall system cost. It should be noted that the controllers themselves may be combined in a network, thereby allowing the creation of significant size ACS (fig. 1.5). If you violate controller communication with the computer system is operating in stand-alone mode. In other words, centralized system - a rigid vertical of power or pyramid where the top of a steering controller ("Head"), and below - the usual interface modules ("Contractor"), which actually implement the control commands.

1.10. The distributed architecture of ACS

A distinctive feature of ACS with a distributed architecture is that the database identifiers (and events in the system) contains not one, but several controllers. They usually serve as the control of external devices and security loop through inputs and relay alarm located directly on the board of the controller.

These controllers are usually installed directly inside their protected areas. It is not likely to reduce whith unauthorized manipulation of the controller, but it has its advantages - such an approach is less critical communication failure between the controller and the interface module (as in a conventional centralized system). In case of breaking the link between the controllers and the computer system continues to perform basic process control functions offline access. Disabling one controller will not affect the work of others. Most often in systems with distributed architecture controller controls the passage of the door 2-4. Using these access control in large distributed sites must be remembered that each individual building, most likely, will be equipped with its subsystem, consisting of a group controller with its own control computer. This feature is associated with the restriction of the length of the most commonly used in such systems interfaces - RS-485 and 20-mA current loop. Laying of communication between remote buildings will require the use of amplifiers interface, which is not always convenient and somewhat reduces the reliability, so we can consider the system as a whole as a collection of sub-systems of several buildings. If you go to the construction terminology, the distribution of ACS - a certain number of controllers - "foremen" who are only responsible for your part of the work by themselves and perform them. They independently analyze and store the information on the operation of their small part of the system.

1.11. The mixed architecture of ACS

Typically, such systems are obtained from the ACS with a centralized architecture by adding specialized readers or interface modules with their own memory buffer identifiers and events - "intelligent interface modules." We can say that each such unit is a small controller ACS comparable with the controller in a distributed system. Through the use of this technical solution is achieved excessive redundancy features, dramatically increases the security of the system. Because the ACS controller with a centralized architecture manages a large number of doors, damaged communication line between the interface modules and the control terminals can block significant portion or even the entire system. Local reader or intermediate interface unit with a built-in buffer memory, in this case goes offline access control list (on the site). Systems built using data modules have the highest degree of safety and extremely reliable operation. For large distributed security systems with mixed hardware architecture, it is important that some manufacturers have in the nomenclature of the interface modules can be connected to a central controller for LAN-interface. In the presence of advanced network communications Onsite these modules are installed in remote buildings, which makes the system more flexible and allows significant savings.

Thus, the mixed system - a pyramid with the possibility of transferring part of the management functions to a lower level in the event of an emergency.

2. Main part. Design and development of ASC hardware

2.1. Raspberry Pi

The **Raspberry Pi** is a series of credit card-sized single-board computers developed in the UK by the Raspberry Pi Foundation with the intention of promoting the teaching of basic computer science in schools.

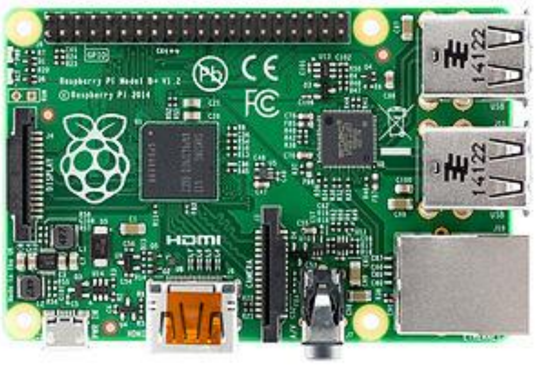
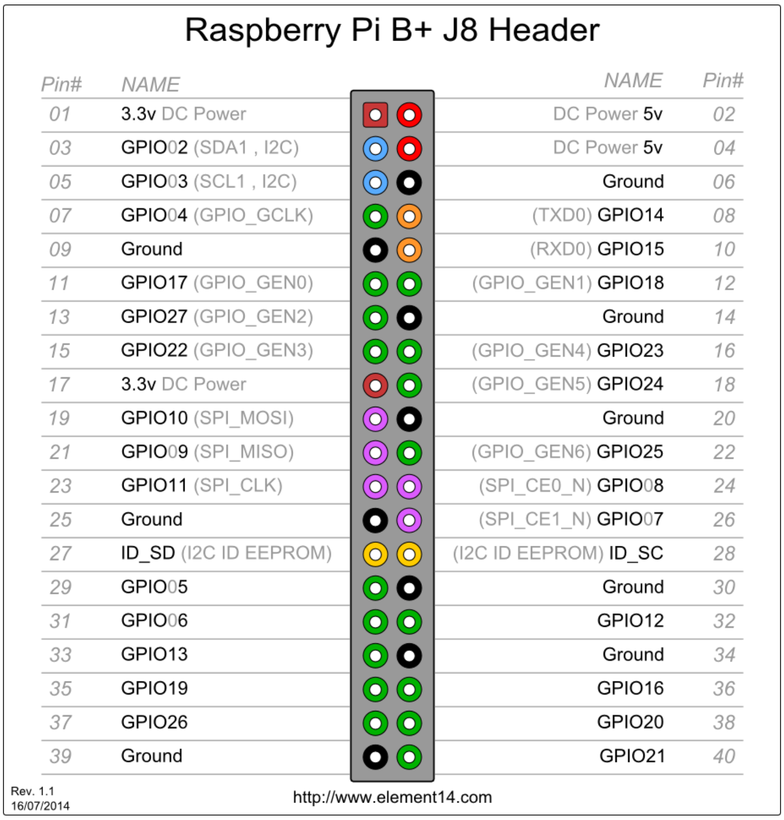


Fig.2.1. Raspberry Pi b+

It is pretty easy to use Raspberry Pi GPIO to connect some peripheral LEDs, buttons, etc.



Raspberry Pi B+ J8 Header

Pin#	NAME	NAME	Pin#
01	3.3v DC Power	DC Power 5v	02
03	GPIO02 (SDA1 , I2C)	DC Power 5v	04
05	GPIO03 (SCL1 , I2C)	Ground	06
07	GPIO04 (GPIO_GCLK)	(TXD0) GPIO14	08
09	Ground	(RXD0) GPIO15	10
11	GPIO17 (GPIO_GEN0)	(GPIO_GEN1) GPIO18	12
13	GPIO27 (GPIO_GEN2)	Ground	14
15	GPIO22 (GPIO_GEN3)	(GPIO_GEN4) GPIO23	16
17	3.3v DC Power	(GPIO_GEN5) GPIO24	18
19	GPIO10 (SPI_MOSI)	Ground	20
21	GPIO09 (SPI_MISO)	(GPIO_GEN6) GPIO25	22
23	GPIO11 (SPI_CLK)	(SPI_CE0_N) GPIO08	24
25	Ground	(SPI_CE1_N) GPIO07	26
27	ID_SD (I2C ID EEPROM)	(I2C ID EEPROM) ID_SC	28
29	GPIO05	Ground	30
31	GPIO06	GPIO12	32
33	GPIO13	Ground	34
35	GPIO19	GPIO16	36
37	GPIO26	GPIO20	38
39	Ground	GPIO21	40

Rev. 1.1
16/07/2014

http://www.element14.com

Fig.2.2. Raspberry Pi B+ GPIO

2.2. Input: RFID reader

Radio-frequency identification (**RFID**) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. The tags contain electronically stored information. Some tags are powered by electromagnetic induction from magnetic fields produced near the reader. Some types collect energy from the interrogating radio waves and act as a passive transponder. Other types have a local power source such as a battery and may operate at hundreds of meters from the reader. Unlike a barcode, the tag does not necessarily need to be within line of sight of the reader and may be embedded in the tracked object. RFID is one method for Automatic Identification and Data Capture (AIDC).

In this work I used RC522 RFID reader.

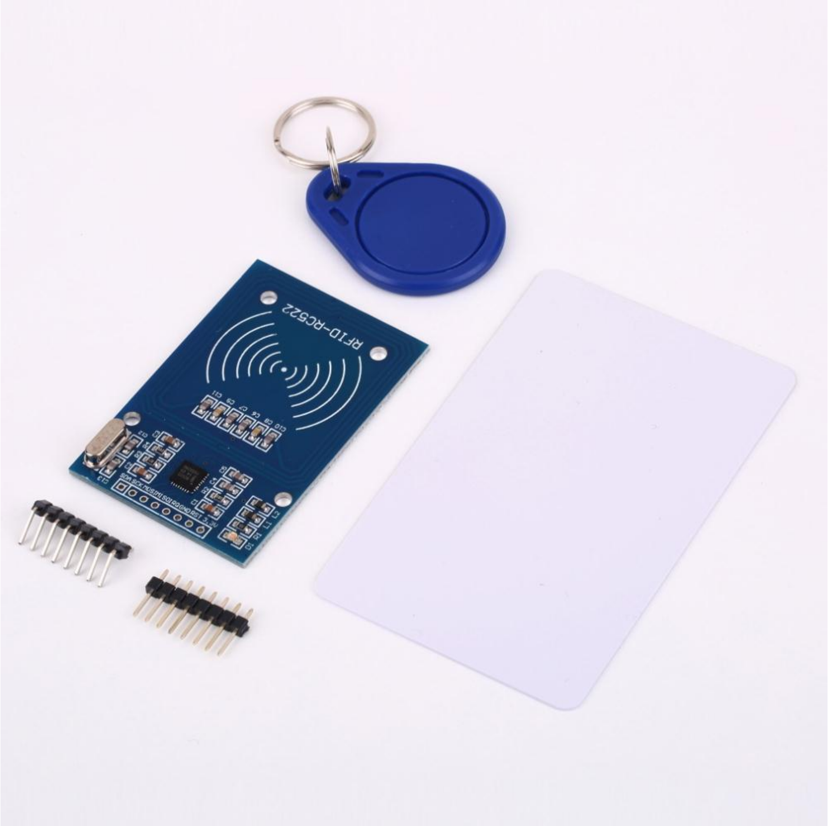


Fig.2.3. RFID reader RC522 and tags

This reader uses SPI. The **Serial Peripheral Interface** (**SPI**) bus is a synchronous serial communication interface specification used for short distance communication, primarily in embedded systems. The interface was developed by Motorola and has become a *de facto* standard. Typical applications include sensors, Secure Digital cards, and liquid crystal displays.

SPI devices communicate in full duplex mode using a master-slave architecture with a single master. The master device originates the frame for reading and writing. Multiple slave devices are supported through selection with individual slave select (SS) lines.

Sometimes SPI is called a *four-wire* serial bus, contrasting with three-, two-, and one-wire serial buses. The SPI may be accurately described as a synchronous serial interface,[1] but it is different from the Synchronous Serial Interface (SSI) protocol, which is also a four-wire synchronous serial communication protocol, but employs differential signaling and provides only a single simplex communication channel.

The SPI bus specifies four logic signals:

- SCLK : Serial Clock (output from master);
- MOSI : Master Output, Slave Input (output from master);
- MISO : Master Input, Slave Output (output from slave);
- SS : Slave Select (active low, output from master).

Alternative naming conventions are also widely used, and SPI port pin names for particular IC products may differ from those depicted in these illustrations:

Serial Clock:

- SCLK : SCK, CLK.
- Master Output --> Slave Input:
- MOSI : SIMO, SDO (for master devices), SDI(for slave devices), DI, DIN, SI, MTST.
- Master Input <-- Slave Output:

- MISO : SOMI, SDO (for slave devices), SDI(for master devices), DO, DOUT, SO, MRSR.
- Slave Select:
- SS : nCS, CS, CSB, CSN, EN, nSS, STE, SYNC.

The MOSI/MISO convention requires that, on devices using the alternate names, SDI on the master be connected to SDO on the slave, and vice versa. Chip select polarity is rarely active high, although some notations (such as SS or CS instead of nSS or nCS) suggest otherwise. Slave select is used instead of an addressing concept.

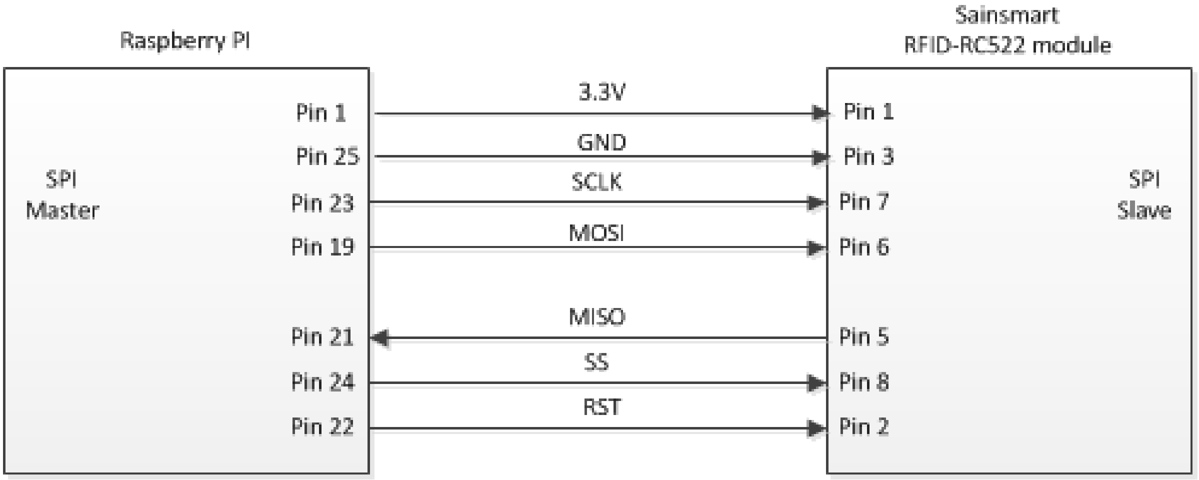


Fig.2.4. The RC522 to Raspberry Pi connection

2.3. Input: buttons and sensor

Access control system should know the door is closed or not. So, it is necessary to use sensor, which will report every time when the door was opened/closed, and after that ACS will be able to lock the door. I used wired magnetic contact MC-38 as sensor.

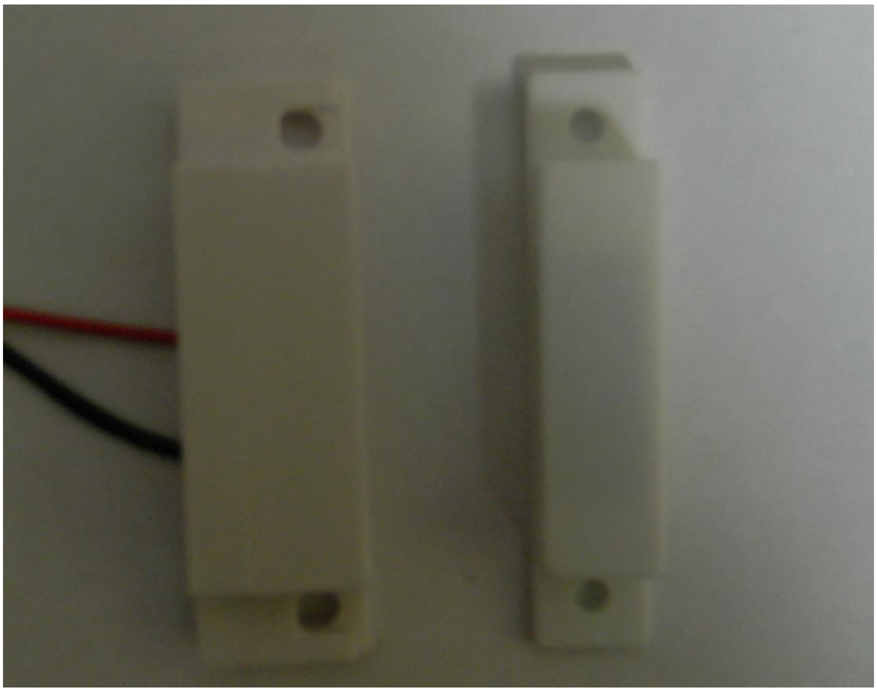


Fig.2.5. I used wired magnetic contact MC-38

In fact, it works as a button. Moreover, I included the ‘open from the inside’ button and the ‘reset’ button.

Fig.2.6. ‘Open from the inside’ and ‘reset’ buttons

It is necessary to choose safe way of connecting these buttons.

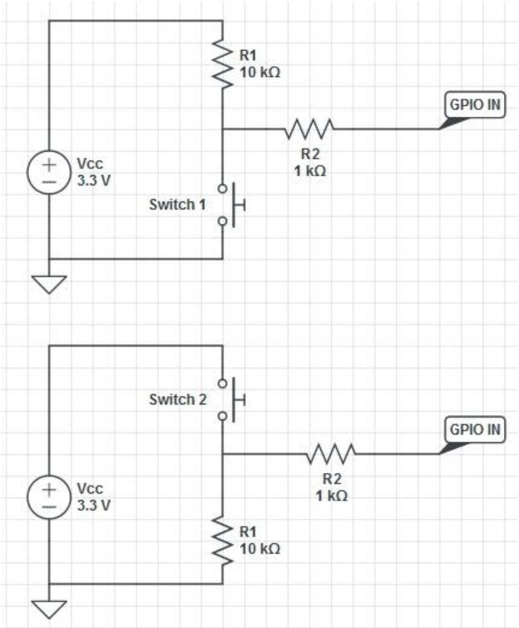
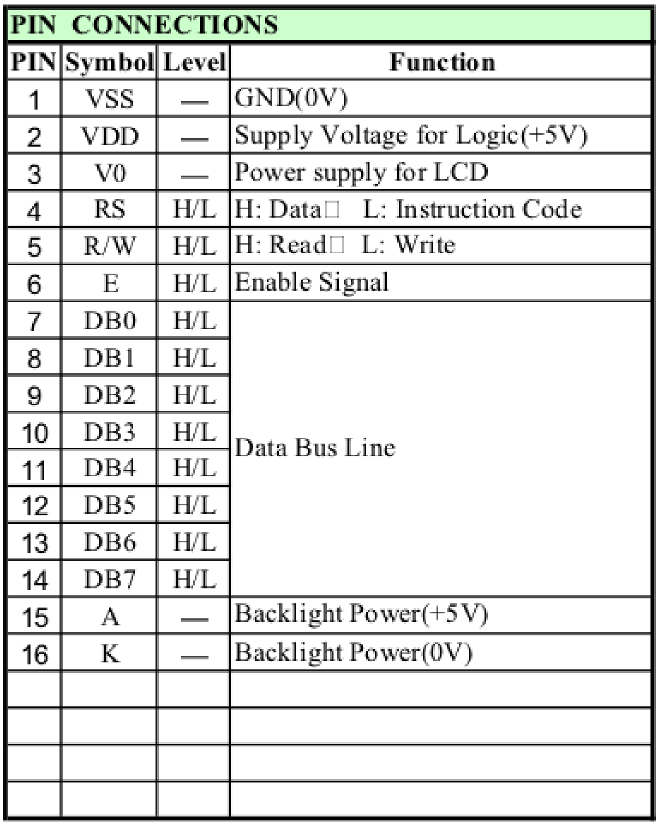


Fig.2.7. Safe button to GPIO connection scheme

2.4. Output: display

In this project I used 16x2 LCD.



PIN CONNECTIONS			
PIN	Symbol	Level	Function
1	VSS	—	GND(0V)
2	VDD	—	Supply Voltage for Logic(+5V)
3	V0	—	Power supply for LCD
4	RS	H/L	H: Data□ L: Instruction Code
5	R/W	H/L	H: Read□ L: Write
6	E	H/L	Enable Signal
7	DB0	H/L	Data Bus Line
8	DB1	H/L	
9	DB2	H/L	
10	DB3	H/L	
11	DB4	H/L	
12	DB5	H/L	
13	DB6	H/L	
14	DB7	H/L	
15	A	—	Backlight Power(+5V)
16	K	—	Backlight Power(0V)

Fig.2.8. 16x2 LDC pins description

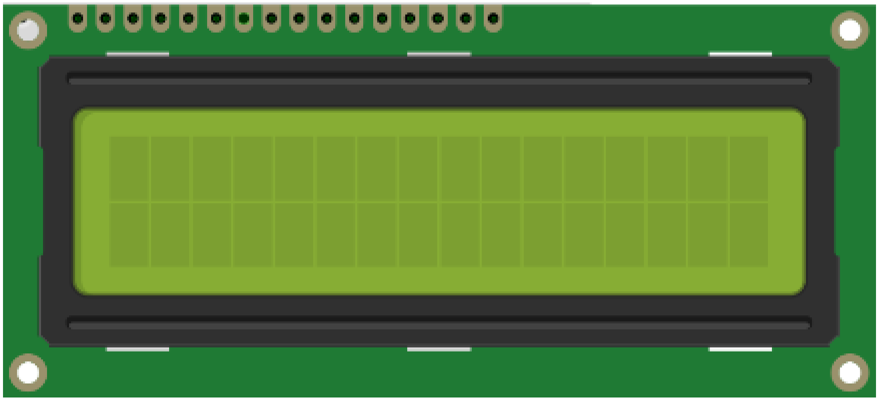


Fig.2.8 16x2 LCD

The problem is about incompatible voltage level - 3.3V is required for Raspberry PI GPIO input, but this display uses 5V. So, direct display to Raspberry Pi connection will burn out GPIO. That’s why it is neccesary to use some microcontroller for safe usage of our display. I used Arduino Uno board as controller for display, and connected it to Raspberry Pi over USB port. Connecting diagram is shown o

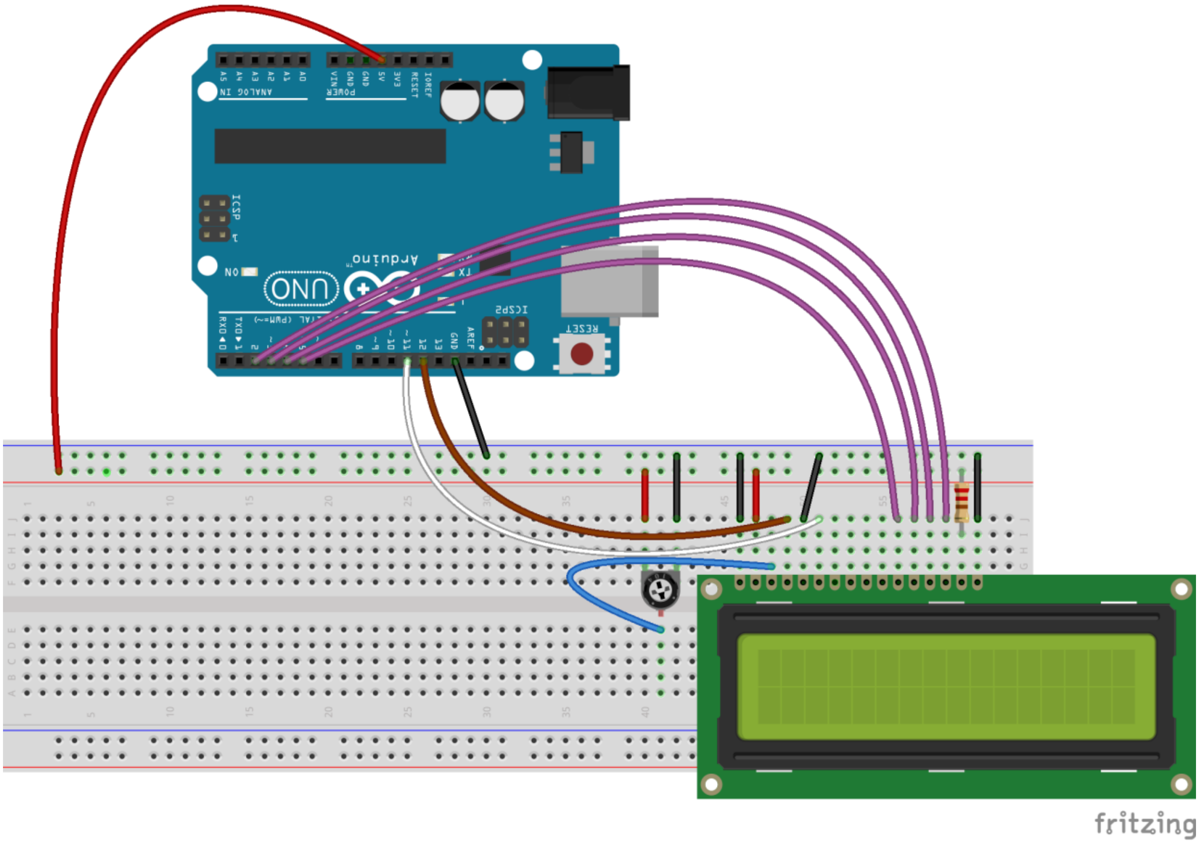


Fig.2.10. LCD to Arduino board connection scheme

After connecting LCD to Arduino board I wrote simple program to output information about state.

The output method is shown below:

```
void printFromValue(char a) {
  if(a == '0'){
    lcd.setCursor(0, 0);
    lcd.print("Access granted!");
  }
  if(a == '1'){
    lcd.setCursor(0, 0);
    lcd.print("Access denied!");
  }
//etc
}
```

To output some string, I just send 1 byte from raspberry PI to Arduino board, and depending on value of that byte some string will be displayed on the LCD.

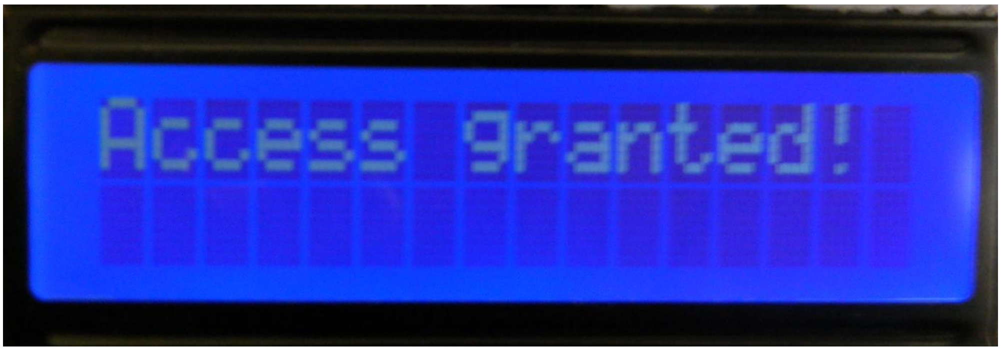


Fig.2.11. LCD output example ‘Access granted!’

2.5. Output: LEDs and the door lock.

In my demonstration stand, there are two LEDs for indication: red and green. And there is door lock which is required 12V for supply.

Fig.2.12. Indication LEDs

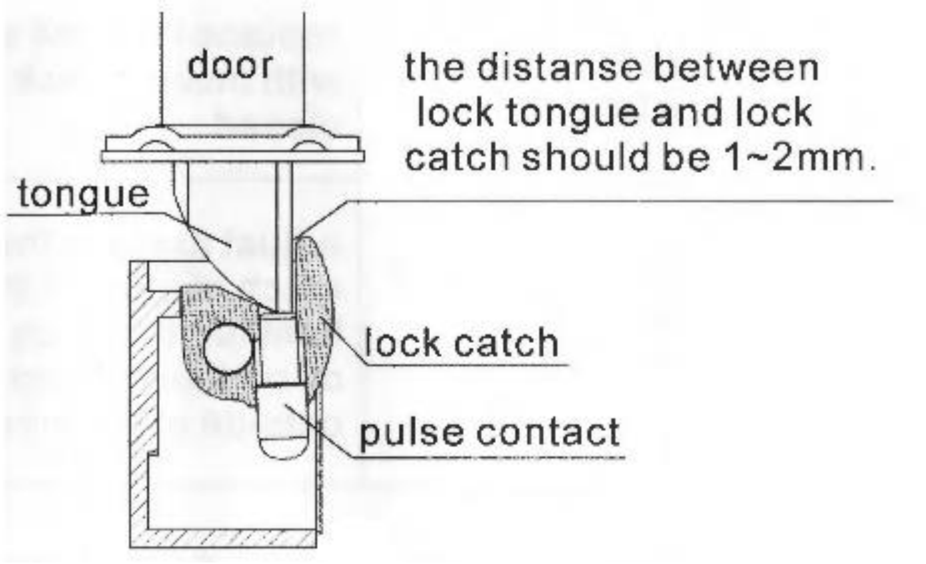


Fig.2.13. The diagram of door lock installation

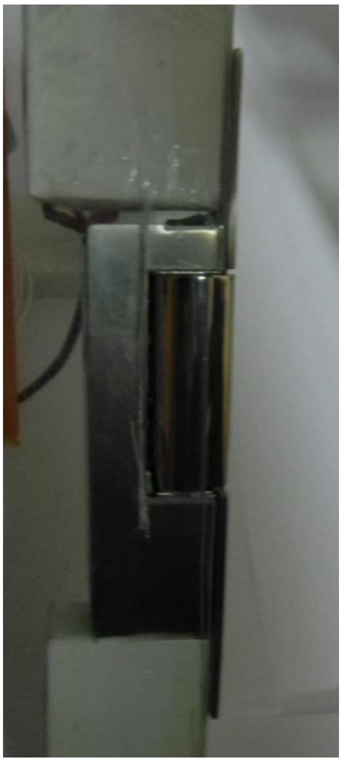


Fig.2.14. Door lock at the demonstration stand

Usually, door locks in ACS are highly reliable and may use separated power supply. In this case I did the same. I just made the scheme with optical pair which allows to use the door lock as LEDs are used, and is just connected 2 LEDs and optical pair using 550 Ohms resistors and with common ground.

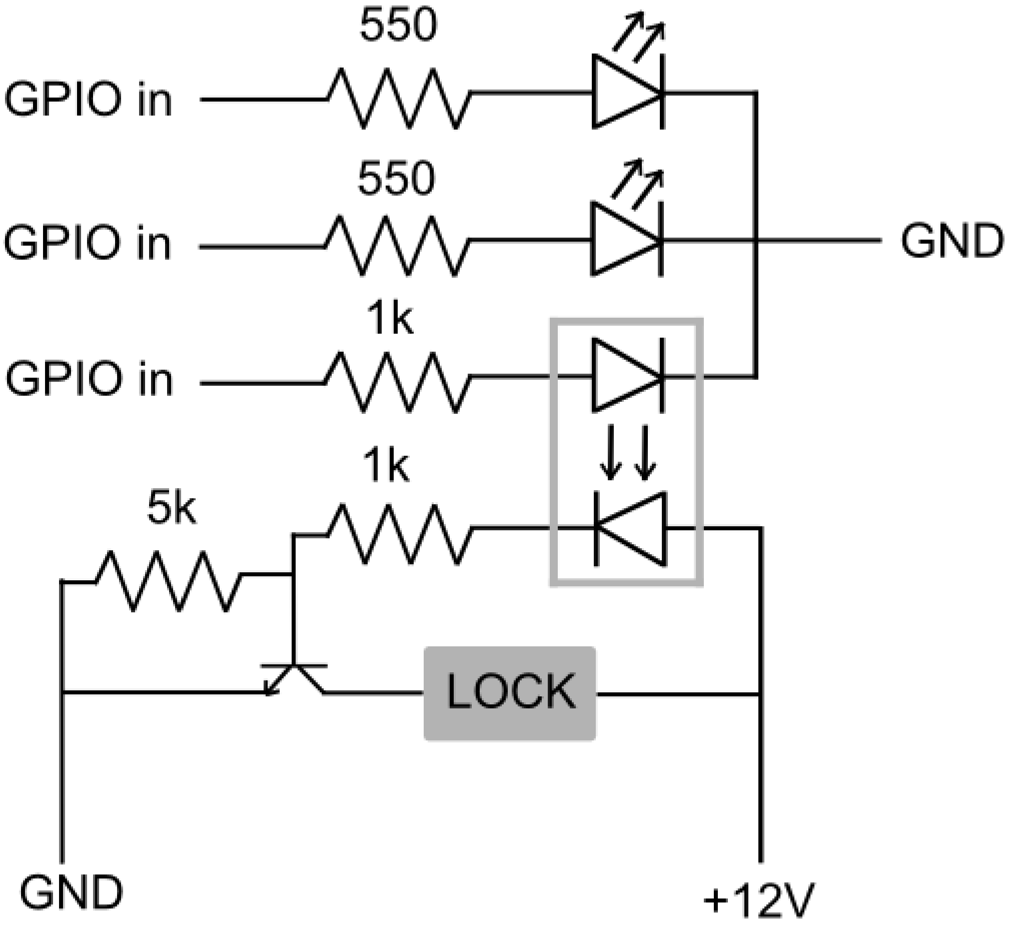


Fig.2.15. LEDs and door lock connection scheme

As we can see, the door lock has separate 12V power supply unit.

2.6. Result

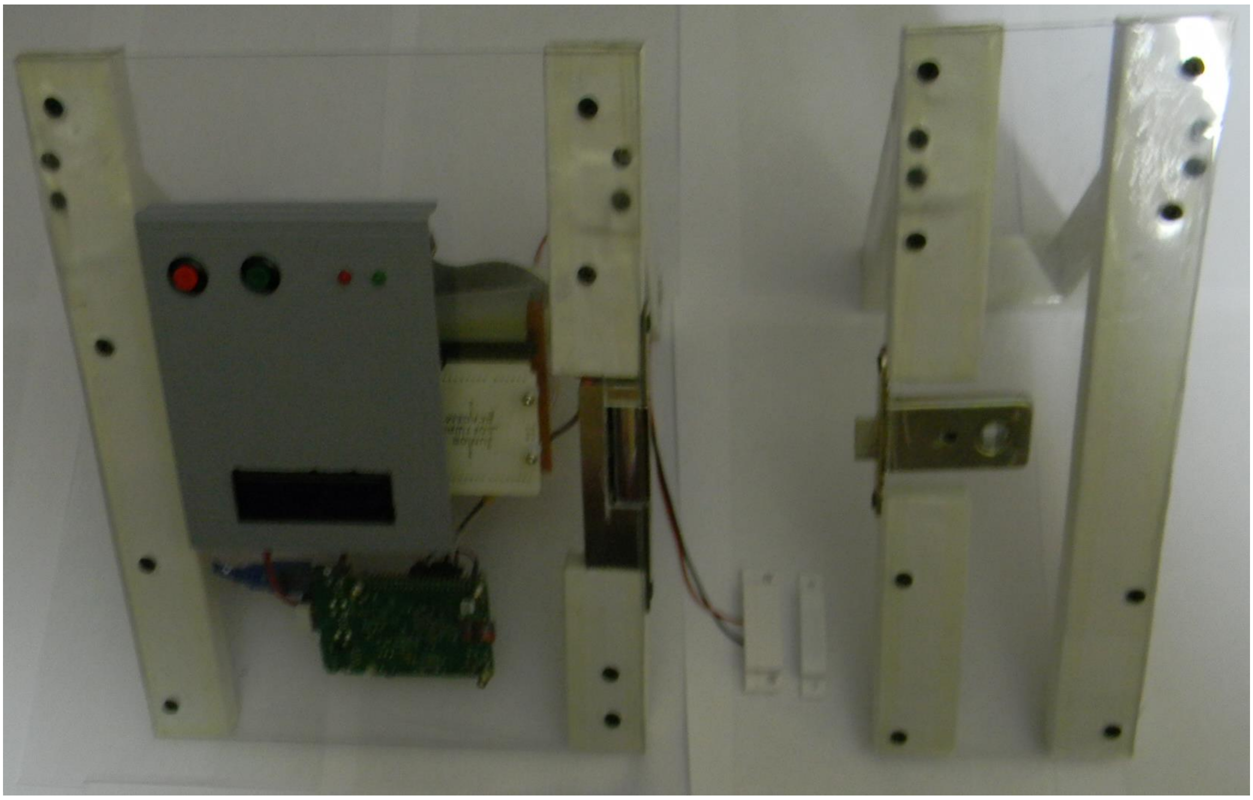


Fig.2.16 Front view of the demonstration stand

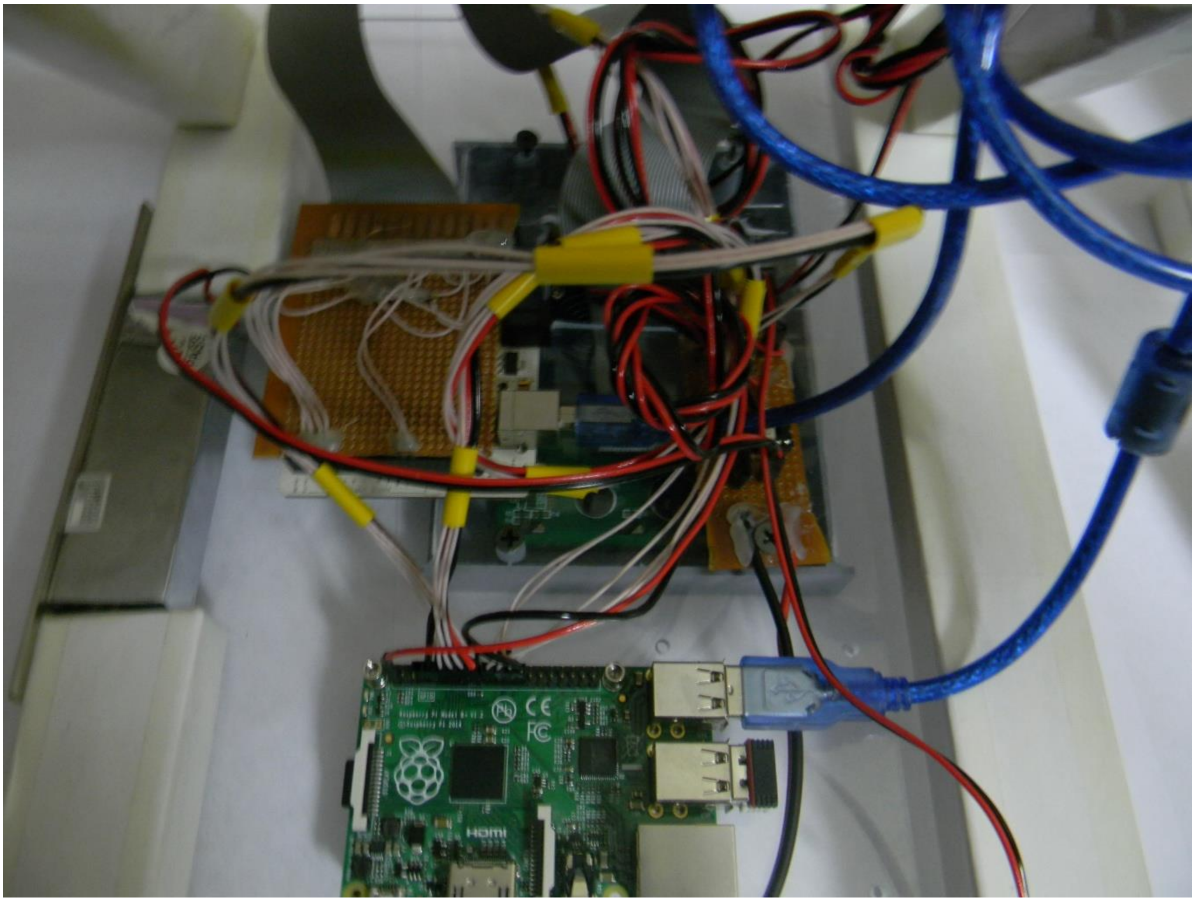


Fig.2.17. Back view of the demonstration stand

3. Safety of vital activity

3.1. Development of a plan placement of equipment in with the sanitary requirements of fire prevention.

Creating a rational sanitary conditions in enterprises - is important problem, the solution of which depends on the health of the labor collectives, safe environment; productivity and crop production in general.

Common sanitary requirements for production facilities, workplaces and work areas, as well as the microclimate set out in building regulations and sanitary design standards of the enterprise.

The area for enterprise is selected on the basis of the general planning of human settlements. Dimensions area determined in accordance with the construction and sanitary norms in view of the possible expansion of the company in the future. The site should be dry, non-callow place with direct sunlight, natural ventilation, have a relatively flat surface, located near a water source with sewage. Comfortable approach and entrance of vehicles must be provided. Conditions labor protection and safety as well as fire protection must be complied. The location of enterprises should prevent adverse effects of one company to another.

Companies with technological processes, which are sources of release hazardous substances into the environment, as well as a source of increased levels of noise, vibration, ultrasound, electromagnetic waves, radio frequency, static electricity and ionizing radiation, must be separated from the settlement areas of sanitary protection zones.

Sanitary classification of industrial enterprises provides the size of the sanitary protection zone, which must be landscaped. Sanitary gaps between buildings are important. If the buildings are illuminated by window apertures, the health gaps must be not less than the greatest height from ground level to the eaves of the opposite building.

Space planning and design solutions of industrial buildings must comply with common sanitary requirements (technological and sanitary engineering section).

The volume of industrial premises per employee must be at least 15 m^3, the area - not less than 4.5 m^2, height - not less than 3.2 m .

The formation of condensation on the inner surface of the outer fences in heated production and auxiliary premises is not permitted, except wet rooms. Therefore, the walls in these areas are covered with steam protective insulating layer.

The walls decoration should be strong, hygienic and economical in operation and correspond to the aesthetic requirements.

Floors in production areas should be made from materials which provide a comfortable and clean them to appropriate performance standards for this production.

Floors and topcoats design is selected in accordance with the process performed in certain types of rooms. The most common are cement concrete, asphalt concrete, asphalt, tile and wood floors. Operational and sanitary requirements for the storage facilities comply floor asphalt coverings. During operation, cement floors emit large amounts of dust, harmful effect on the human body and equipment.

Usually, enterprises must have auxiliary sanitary facilities (dressing rooms, washrooms, toilets, showers, rest rooms, a health center, personal hygiene rooms, etc.). The composition of these rooms, sizes and equipment depend on the sanitary characteristics, production processes, the number of employees and other factors identified in the common sanitary requirements.

Proper planning exits, passages, stairs and platforms is essential to the protection of employees of enterprises. They must comply with building, operating, sanitary and fire protection requirements.

Efficient process equipment indoors affects the organization of technological processes, increase productivity and protect it. Placement of the equipment should be comfortable and safe in operation.

The water supply of enterprises is very important for the protection of labor. It must satisfy the needs of businesses in the drinking water for household hygiene, industrial and fire-fighting purposes. There are two types of water supply: centralized and decentralized.

Selecting sources of drinking water supply should be coordinated with local authorities and local Sanitary Epidemiological Service. The water quality must comply with requirements for drinking water.

The production and auxiliary premises lighting, heating, ventilation and air conditioning provide optimal parameters of the air environment that contribute to the preservation of human health and increase his capacity for work.

The air temperature in production premises, depending on the severity of the works in the cold and transitional periods of the year should be between 14 and 21 ° C during the warm period - from 17 to 25 ° C.

Physiology of labor that studies the physiological processes in the body related to his employment is an integral part of health. Physiology of labor aims to find rational (from a physiological point of view) the organization of labor in which the person reduces fatigue, increases efficiency and productivity.

Ventilation and air conditioning enterprises creates air environment, which complies with occupational hygiene. Temperature, humidity and air quality in the rooms can be controlled using ventilation. Air conditioning creates an optimal artificial climate.

Inadequate ventilation in the premises of undertakings decrease workers' sight and ability to work, it causes nervous irritability, and as a result - reduce the productivity and labor quality.

There are natural and artificial ventilation. As a result of wind and thermal heads (obtained from the different density of the air indoors and outdoors), natural ventilation provides ventilation in the rooms. Natural ventilation is divided into organized and unorganized. Organized natural ventilation is performed by aeration or deflectors. When natural ventilation air circulation occurs through ventilation ducts (which are located in the walls), lights and special air ducts.

Aeration provides Channel Free exchange of air through windows, vents, skylights, folding glass surfaces, and so on. The deflector ventilation - through the channels and air ducts with special nozzles.

Unorganized ventilation is carried out through leaks designs (windows, doors, pore walls).

Artificial ventilation (mechanical) is achieved by the fans or ejectors. It can be inflow (injection), exhaust (suction) and the inflow and exhaust.

Effectiveness of ventilation is the value that indicates how quickly the polluted air is removed from the premises. Effective ventilation is often used for the qualitative assessment of the system to provide a comfortable environment of clean air. It must be borne in mind that the high mobility through the air causes hindering the work and causing colds.

Air conditioning is to create and maintain indoors certain parameters of ambient air temperature, humidity, composition, speed and air pressure. The parameters of the air environment should be favorable for human and sustainable.

Modern automatic air conditioning systems clean, heat or cool, moisten or dry the air, depending on the time of year and other conditions, subjected to ionization or ozonation, and serves its premises at a certain speed.

Proper placement of the equipment is the main element in the organization of the safe operation of the production area. When placing the equipment necessary to comply with the established minimum gaps between machines, between machines and the individual elements of the building, to correctly determine the width of walkways and driveways. Failure to comply with rules and regulations placing equipment leads to clutter premises and injuries.

Location of equipment on an area of land or plant is mainly determined by the process and the local conditions.

With automated production (integrated circuit plants or plant, automated production lines, mass production) equipment is placed on the downstream side in a single chain with compliance with the distances between the equipment and structural elements of the building. In the automatic production lines and long distance to go from one side to the other line satisfied catwalks.

When multi-machine-tool maintenance equipment have given the maximum possible reduction of the distances between workplaces. If the conditions of the process is necessary to provide racks or tables for blanks and finished products, then this is given more space in accordance with the peculiarities of production.

Placement of machine tools, tool benches and other equipment in the shops of cold treatment is adopted so that the distance between the individual machines or groups of machines was sufficient to enable free passage of workers engaged in their maintenance and repair. In all cases, placement of equipment should provide a sufficient number of passes to people and driveways for vehicles to ensure the safety message. The width of the walkways and driveways assigned depending on the location of the equipment, the nature of motion, method of transportation, and the size of the details, but in all conditions received at least 1 m. For the transportation of goods by motor vehicles arranged passages 3.5 m wide. Overload aisles and driveways, as well as workers' places various objects is not allowed.

Walkways and driveways need to keep clean and tidy, their boundaries are usually marked with white paint or metallic bright buttons. The width of the working area is taken not less than 0.8 m. The distance between the equipment and elements of the building, as well as the size of the passages and passages defined by the norms of technological design of mechanical and engineering works assembly plants.

In single and small-scale production equipment is often placed in groups of machine tools (lathes, milling, boring, grinding and so on. N. Machines); However, it should seek to ensure that the location of the equipment eliminates the possibility of a collision in the process of material flow, semi-finished and people. It is advisable to arrange in the spans between the equipment one-way traffic. When transporting a variety of workpieces in the aisles (especially blanks great length) should not be allowed to vehicles and hampered harvesting work area or out of travel abroad, pass.

The workplace is a primary element of production, it represents a certain part of the production area of the shop is designed to perform one worker (or a team) assigned work, specially adapted and technically equipped in accordance with the nature of the work. On how correctly and rationally will be organized workplace safety depends and productivity. As a rule, every workplace is equipped with main and auxiliary equipment and tools. The lack of convenient workplace accessories or irrational its location, clutter creates conditions for the occurrence of injuries.

3.2. Types and forms of human activity.

Labor - a form of purposeful human activity aimed at creating customer value. Existing forms of labor are different relative to each other corresponding muscle energy costs, the degree of exploitation of the brain, central nervous system and sense organs.

It has long been accepted to divide labor on the mental and physical, although there is no clear border. Physical labor is considered the prevailing load on the system, providing the muscle activity (breathing, circulation). Mental labor load to a greater extent the central nervous system with a relatively small enhancing metabolism.

From the point of view of physiology should distinguish between the concept of "labor" and "work". By working to understand all the activities related to energy consumption and the output from the rest of the body. If any form of labor carried out work that can not always be attributed to the work.

Physical work can be static and dynamic. Dynamic work consists in moving cargoes up, down and across. Static work - is the maintenance of human effort without moving the body and limbs in space. This work is characterized by the product of the mass of the load on the length of his confinement and is considered a tedious compared with the dynamic work.

Depending on the basic characteristics and requirements to the physiological requirements of the organism there are the following forms of labor:

- physical - differs large muscle activity and high cost of energy (porters, etc..);
- mechanized - linked to service cars (car drivers, and so on.);
- automated and semi-automated (weavers, stampers and so.), Sometimes it requires great energy;
- conveyor (group) - is associated with the movement of products in the processing of one job to another, it may be easy (for radio factory assemblers) and heavy (collectors in the tractor factory);
- intellectual - is divided to labor in material production (engineers, accountants, machine operators with a remote control, and so on.), And outside the sphere of material production (writers, teachers, and so on.).

All the works, depending on the intensity of the overall energy of the body are divided into the following categories:

- Ia - operation with the intensity of energy consumption to 120kkal / h (up to 139 W) produced by sitting and accompanied by a slight physical stress (enterprises precision instrument and engineering industry, in the watch, garment production, in management, and so on.);
- Ib -Work with energy intensity 121 ... 150kkal / h (140 ... 174 W) produced by sitting, standing or associated with walking and accompanied by some physical stress (in the printing industry, Telecommunications, inspectors, masters in the factories etc);

- IIa -Work with energy intensity 151 ... 200kkal / h (175 ... 232 W), associated with the constant walking, moving small (up to 1 kg) products or objects standing or sitting, and requires a certain physical strain (in Smith departments of engineering enterprises, spinning and weaving, and so on);
- IIb -Work with energy intensity 201 ... 250 kcal / h (233 ... 290 W) associated with walking, movement and transport of loads up to 10 kg and are accompanied by moderate physical stress (in the mechanized casting, rolling, forging, thermal, welding departments of engineering and metallurgical plants, etc.);
- III - operation with the intensity of energy consumption of more than 250 kcal / h (over 290 W), associated with the constant movement, the movement and carrying significant (over 10 kg) heavy and require more physical effort (in forging shops with hand-forging, casting shops with hand-packing and filling the flask engineering and metallurgical enterprises, and so on.).

Fatigue is a decrease in performance that occurs as a result of a great of labor of high intensity or duration, and expressed in a quantitative and qualitative deterioration of the results.

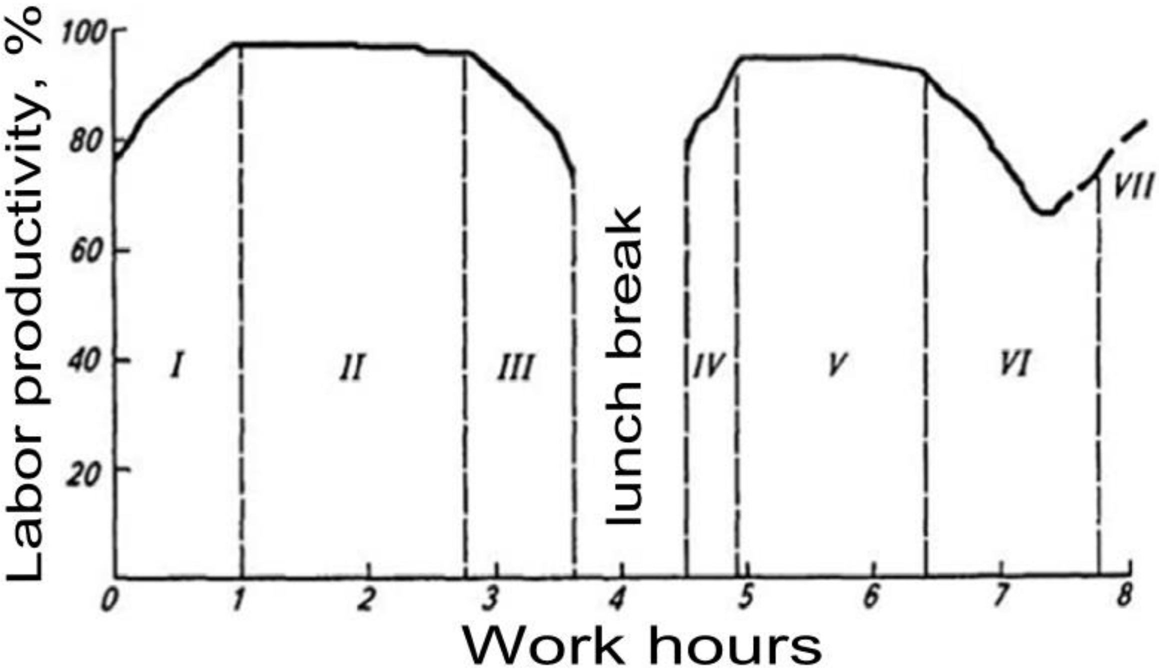


Fig. 3.1. The periods of change performance during the work shift:

I and IV - the beginning of the work; II and V - stable performance; III and VI - decreased performance; VII - "the ultimate rush"

Fatigue is a physiological state of the reversible. However, the accumulated, it can move into a qualitatively different state - fatigue, characterized by a persistent decline in performance. In both states, it increases the level of injury, and in some cases, fatigue may have the disease, and drop resistance to various infections.

Each operation corresponds to a certain individual character changes curve performance. Figure 3.1 shows the curve of the normal type, the corresponding light work. Medium-heavy and tension is characterized by early onset of fatigue, loss of productivity and loss of smooth generating.

In severe the coordination function of the central nervous system is broken due to fatigue. This condition takes stagnant and goes into exhaustion. The period of performance is not sustainable. Productivity declines, the number of defective products.

The biological criteria for severity and intensity of labor in addition to fatigue include the incidence of working.

There is a hygienic classification of labor, which is based on the factors of production environment and labor process and their impact on people's health and performance. It includes four classes.

Class 1 - the optimal working conditions, characterized by the preservation of the health of workers and the creation of preconditions for maintaining a high level of efficiency. The parameters of the microclimate and the factors of the labor process are in optimal ranges, unfavorable factors are absent or do not exceed the levels accepted as safe for the population.

Class 2 - acceptable conditions of work, in which the set hygienic standards for workplaces are respected, and possible changes in the functional state of the body are restored during the rest of the regulated or the beginning of the next shift. Acceptable working conditions are conventionally considered to be safe.

Class 3 - harmful working conditions in which the factors of production exceed the hygienic standards and adversely affect the body working.

Class 4 - dangerous (extreme) conditions of work, characterized by such terms of production factors, the effects of which during the work shift or part of a threat to life, a high risk of acute occupational injuries, including severe.

The working conditions of the third class, depending on the level exceeding hygienic standards and severity of changes in the body work is divided into four levels of hazard:

Level 1 - deviation levels of harmful factors on hygiene standards cause functional changes in the body, restore, usually for longer than the beginning of the next shift, interrupt contact with harmful factors, and increase the risk of injury to health;

Level 2 - the levels of harmful factors cause persistent functional changes leading in most cases to an increase in production due to morbidity. This is evident in the increase in the incidence of workers, the initial appearance of symptoms or mild forms of occupational disease occurring after prolonged exposure (15 years or more);

Level 3 - working conditions, which are characterized by such levels of harmful factors, the effects of which often leads to the development of occupational diseases of mild to moderate gravity, associated with the loss of occupational disability, chronic growth (due to production) pathology, including an increased incidence of employees;

Level 4 - the working conditions in which there may be severe occupational diseases with loss of total disability, there is a significant increase in the number of chronic diseases, there is a high incidence of workers.

Intellectual work can be divided into a monotonous associated with the monotony of the functions, and creativity - with the adoption of various decisions and the elaboration of the new information.

Mental labor is characterized by its intensity. Muscle activity is reduced. The intensity of mental labor depends primarily on what is required of the functions of attention, and it determines the number of production-critical facilities, for which it is necessary to observe at the same time, the duration of the concentrated observation, the number of incoming signals at a time. Important criteria include emotional stress intensity, the amount of load on the organs of hearing and vision, the degree of flatness of labor.

The most intense work of the operators consider associated with the solution of complex problems under time and information, improve operational responsibility, personal risk, responsibility for the safety of others.

Physiological parameters estimating the labor intensity are divided into:

- heart rate (exceeding the allowable value is unacceptable by more than 28 beats per 1 minute);
- rhythm of heartbeats;
- blood pressure (the upper limit must not be exceeded more than 30 mm Hg. Art., Bottom - 15 mm Hg. V.); respiration rate, which should not be higher than the frequency of respiration at rest (7 to 22) more than 30 cycles per minute.

The energy required for the life of man, distinguished in his body in the process of redox collapse of carbohydrates, proteins, fats and other organic compounds contained in food. Redox reactions in living organisms can occur both with oxygen (aerobic oxidation) and the absence of oxygen (anaerobic oxidation). Anaerobic oxidation is characterized by a smaller number of the released energy is of limited value in higher organisms.

Aerobic oxidation of 1 g of fat in the body is released 38.94 kJ, and the oxidation of 1 g or 1 g of protein carbohydrate -17.6 kJ. This energy is partly used to perform useful work, and partly dissipated as heat, warming the human body and the environment (the efficiency of muscle tissues -40 ... 60%).

The set of chemical reactions in the human body called metabolism. To characterize the total energy metabolism using the basic concepts of sharing and exchange in various activities.

Basal metabolism characterized by the energy expenditure in a state of dormancy muscle under standard conditions (at a comfortable ambient temperature, after 12- 16 h postprandial supine). Energy consumption in the processes of life in these conditions for a person weighing 75 kg is 87.5 watts.

Changing posture, the intensity of muscle activity, information saturation of labor, the degree of emotional stress and other factors result in additional costs of energy. So, in a sitting position by the operation of trunk muscles energy costs exceed 5-10% of the total exchange rate, standing - 10 ... 15%, with a forced an uncomfortable position - 40 ... 50%.

When the need for intensive intellectual brain power of 15-20% of the basal metabolic rate (the mass of the brain is 2% of body weight). Increase of total energy consumption in the mental work is determined by the degree of neuro-emotional tension. So, when reading aloud sitting energy consumption increased by 48%, with a public lecture speech - na94%, the operator of computers – 60-100%. Increased metabolism and energy consumption during operation results in an increase of heat. When heavy physical work the body temperature may rise to 1-1,5 ° C.

The level of energy can serve as a criterion for severity and intensity of work that are important to optimize working conditions and rational organization. The level of energy consumption was measured by indirect calorimetry, t. E. A complete gas analysis (taking into account the amount of oxygen consumption and carbon dioxide emissions). With increasing severity of labor significantly increases the amount of oxygen consumption and energy expenditure, hence there are various daily energy person:

- intellectual workers (engineers, doctors, teachers, etc.): 10.5-11.7 MJ;

- employees of mechanized labor and service (nurses, salespeople, workers, machines and serving others.): 11.3-12.5 MJ;
- workers who perform work of moderate severity (machine operators, drivers, surgeons, printers, casters, agricultural workers and others.): 12.5-15.5 MJ;
- workers performing heavy work (loggers, porters, miners, steelworkers and others.): 16.3-18.0 MJ;

3.3. **Technical measures for the dispersion of emissions into the atmosphere**.

Air protection - a system of measures implemented by public authorities, local governments, corporations and individuals in order to improve air quality and prevent its harmful effects on the health and living conditions of people and the environment.

The system of measures to protect the air pollution in the first place should be put technological measures, the implementation of which is capable of fully and fundamentally solve the contradiction between the production of goods for the person and the state of its habitat. However, as always in life, to achieve the ideal, in this case the complete elimination of emissions from the process cycle is not possible. Therefore, along with technological activities aimed at maximum reduction of emissions, often have to resort to reduce the harmfulness of emissions, or cleaning that is carried out by sanitary measures. For the purpose of the spatial separation of the emission source to the human environment necessarily conducted planning activities.

The system of measures to protect the air pollution also includes a group of administrative measures, one of whose aims is to limit the anthropogenic pressure on the entire natural environment, including the human environment, in times of unfavorable synoptic situation when reduced eliminates nature's ability to respect emissions into the air. Administrative measures are also designed to facilitate the timely implementation of the above activities, arranging social relations.

In the specific sanitary situation for the protection of air pollution must be integrated use of these measures in order to achieve maximum impact at the lowest cost. Effective solution of this problem is possible, as a rule, only a large-scale territorial industrial complex, and not on the scale of the enterprise. For competent assessment of the projected measures for the protection of air ambulance doctor should be familiar with the principles and methods of limitation of anthropogenic impact on the atmosphere of the settlement.

Technological and technical measures are implemented at the source of air pollution. These include the replacement of power sources less harmful raw materials - less toxic, pretreatment of fuel or raw materials to reduce the harmfulness of emissions, improving the process to reduce emissions or hazards (using wet instead of dry processes). Of great importance is also sealing the process equipment, instruments, interdepartmental transport, recovery (return process) volatiles.

Sanitary measures, their purpose is to removing or neutralizing the emissions of components which are in a gaseous, liquid or solid form, from organized stationary sources. Caught components can be returned later to the same production, used as raw materials or additives in other enterprises or buried in landfills of industrial solid waste in ash dumps.

Requirements for the abatement of dust and gas are presented, taking into account the large variety of components of air emissions, their qualitative features. Methods for cleaning up emissions can be divided into two groups.

Physical methods are used to extract solid and liquid impurities - dust, smoke, mist or spray of droplets. This so-called dust removal. This includes mechanical and electrostatic cleaning methods.

Physicochemical cleaning methods for extraction and utilization of certain impurities from the flue gas - gas cleaning.

Technological and sanitary-technical measures can not always ensure the quality of the release, in which the observed composition of atmospheric air of settlements in the level of requirements of sanitary rules and norms. In this case, there is the need for planning actions. Among the most important are the functional zoning of the territory of the settlement plan living areas, landscaping settlements, organization of sanitary protection zones, increasing the height of the flue or vent pipe business.

Sanitary Protection Zone (SPZ) is the area around the industrial plant of a technical object, which is the source of the impact on the environment and human health, measures that reduce the levels of exposure to workplace factors (air emissions, noise, vibration, electromagnetic and ionizing radiation and so on.) in residential and recreational areas to the limits permitted by the sanitary rules, hygienic and ecological norms.

Pressures on the environment and human health are man-made objects, the levels of production factors which are outside the industrial site exceed the hygienic standards (MPC or the maximum permissible level) for populated areas or whose contribution to the pollution of residential areas exceed 0.1 MPC.

SPZ organization is necessary in case after the company all the technological and technical measures for the treatment and disposal of air emissions, limit the spread of man-made physical factors developed at the level of advanced science and technology, can not be achieved reducing the levels of exposure to the residential area and recreational areas to acceptable sanitary rules and hygienic standards. On this basis, we can formulate the goal of SPZ: source separation space impacts on the environment and the territory of the residential and recreational areas for the creation of conditions for dispersion of industrial emissions into the atmosphere to ensure compliance with hygienic standards in the area of residential and recreational areas.

The SPZ are not allowed collective and individual cottage and garden plots; enterprises for the production of medicines, pharmaceutical companies warehouses, food industry, wholesale food raw materials and food, a complex of buildings for the preparation and storage of drinking water, sports facilities, parks, educational, children's, medical and Wellness-lision institutions.

On the territory of the SPZ it can be permitted occupancy of farmland for the cultivation of industrial crops not used for food and pet food. Accommodation of fire stations, laundries, garages and parking areas for public and private transport, auto-gas stations and related maintenance of the buildings of the enterprise management, design offices, clinics. Sanitary Regulations also allowed the placing on the territory of the SPZ smaller enterprises hazard class. However, with the concurrence of such a project is necessary to ensure that employees of the enterprises are not subject to negative impact on health of factors of production, for the neutralization of which was organized by the SPZ.

The height of the chimney or vent pipe. One of the planning of measures to protect air settlements is to regulate the conditions for dispersion of pollutants in the atmosphere by increasing the height of the output (the height of the flue or vent pipe). Often it concerns the height of the pipe thermal power enterprises state district power plants and total energy power stations. Regular chimney height of 100-120 m businesses. The radius of the smoke zone, where surface concentrations exceed the MAC level is 2-2.5 km. By increasing the height of the pipe to 180-240m, and in some cases up to 300 m radius zone smoke increases to 5-10 km, but the surface concentrations of impurities are significantly reduced. This is due to two factors: the expansion of the opening angle of the torch emissions and improve the turbulence due to higher wind speeds at a height. However, experts believe that the use for urban development areas within the area of smoke, is not justified, even if the calculations show that the surface concentrations do not exceed the maximum permissible concentration. There is a danger of falling into such territories unfavorable sanitary conditions during periods of declining terms of dispersion in a calm and temperature inversion, fogging, and also in connection with a possible further expansion of thermal power (electricity) station. Thus, increasing the height of the pipes at power stations are not accompanied by a reduction in emissions or reduce harm; it merely reduces the surface concentrations of the components. However, an increasing number of people living in the zone of influence of emissions. Therefore, increasing the height of the pipe can not be regarded as a measure compensating for known but not available on this site abatement techniques. In large cities with more diverse sources of air pollution and emissions of multicomponent composition, increasing the height of the pipe will not improve sanitary conditions. Construction of tall chimneys at power stations expediently at their location in areas with low population density, provided a full range of technological and sanitary measures and the absence of other serious near pollution sources.

To remove harmful gas impurities dry and wet type precipitators are used.

For the dry type dust collector cyclones are different kinds - single, group, battery. Cyclones in the change in the concentration of dust at the entrance to 400 g/m3 gas at temperatures up to 500 ° C.

The widespread use of the technique found dedusting filters that provide high collection efficiency of large and small particles. Depending on the type of filter material filters are divided into tissue, fibrous and granular. For cleaning large volumes of gas with highly efficient electrostatic precipitators.

Wet type dust collectors are used to clean high-temperature gases, trapping fire and explosion hazardous dusts and when, along with dust collection is required to capture the toxic trace gases and vapors. Devices called wet-type scrubbers.

To remove harmful gases from exhaust gas impurities used absorption, chemisorption, adsorption, thermal post-combustion, catalytic reduction.

Absorption - dissolution of a harmful gas impurities sorbent, usually water. Method chemisorption is. purging gas irrigation solution reagents entering into a chemical reaction with harmful impurities to form a non-toxic, low-volatile or insoluble chemical compounds. Adsorption - capturing surface of the microporous adsorbent (activated carbon, silica gel, zeolites) molecules of harmful substances.

Thermal afterburning - oxidation of harmful substances atmospheric oxygen at high temperatures (900-1200 ° C). Catalytic achieved using catalysts - materials that accelerate the reaction or make it possible at much lower temperatures (250-400 ° C).

Disposition of the territory of the settlement. Some planning activities in the territory of the residential areas are aimed mainly at reducing the hazard of vehicles as a source of air pollution. In addition to the above-mentioned health gaps between highways and residential area and landscaping, reducing the concentration of exhaust gas combustion engine in a residential area can be achieved and some planning methods.

Given that the non-uniformity of the internal combustion engine (frequent stops, idling, frequent switching speeds, etc.) is the leading cause of rising emissions, a major role in improving the atmosphere of cities plays a rationalization of the road network. By the methods of rationalization of the road network include the organization of road junctions without traffic lights through the construction of underground tunnels, elevated platforms. Construction of bypasses or ring roads gives a great effect to exclude transit traffic of vehicles through urban areas. Administrative measures aimed at air protection settlements is to organize one-way traffic on the narrow streets, pedestrian zones, which prohibited the movement of vehicles, equipment and ride parking lots at the end subway stations and other methods of regulating traffic flows. construction of bypasses or ring roads gives a great effect to exclude transit traffic of vehicles through urban areas.

Measures aimed at control of the internal combustion engine, not less effective: the deadlines and maintenance program, schedule maintenance vehicle traffic police authorities, the introduction of penalties for violation of these terms.

Particular note is introduced administrative time limit power businesses with emissions for the period of the forecast hazardous weather (temperature inversions deep, prolonged calm and so on.).

Conclusion

According to the results of this final qualification work we can conclude following:

1. To create an access control system it is necessary to study the theoretical basis
2. Before the start of the development of ACS, it is necessary develop a list of requirements and the required functionality
3. After compiling the list of features, it is important to choose the right hardware base
4. In the development, it is desirable to split the whole system into independent modules
5. Testing is an important stage in the development of ACS
6. In the development of such systems it is necessary consider the Safety of vital activity requirements

Bibliography

1. The resolution of the President of Republic of Uzbekistan "On measures for further implementation and development of modern information and communication technologies» № PP-1730 on March 21, 2012.
2. Системы контроля и управления доступом / В. А. Ворона В. А. Тихонов, Москва, Горячая линия – Телеком, 2010
3. https://www.arduino.cc/en/Tutorial/LiquidCrystal./ - How to use 16x2 LCD with Arduino board
4. http://en.wikipedia.org/wiki/Serial_Peripheral_Interface_Bus/ - SPI description
5. http://geraintw.blogspot.com/2014/01/rfid-and-raspberry-pi.html/ - RC522 RFID reader and Raspberry Pi connection
6. https://www.cl.cam.ac.uk/projects/raspberrypi/tutorials/robot/buttons_and_switches/ - Buttons and switches, safe connection to Raspberry Pi
7. RT1602M datasheet – 16x2 LCD datasheet
8. The manual of 2081EJ electric strike

Appendix