
ACCESS RIGHT
ACCESS CONTROL SYSTEM
SKIF.
ACS
FINGERPRINT SCANNER
QR CODE
SOFTWARE MODULE
VISIT CONTROL
RECOGNITION
RFID
DATA WAREHOUSE
VISIT CONTROL
FINGERPRINT SCANNER
RECOGNITION
PRESENCE SENSOR
RFID
ACCESS RIGHT
SITE ACCESS
VOICE COMMUNICATION
QR CODE
VIDEO SURVEILLANCE
SITE ACCESS
DATA WAREHOUSE
MONITORING
PLUS

# PURPOSE

Access Control System, ACS (from Eng. Access Control System, ACS) is a set of software and hardware security equipment designed for controlling and registering the entry and exit of objects (people, vehicles) to a given area through the «entrance points:» doors, gates, checkpoints.

The main purpose is to control access to a given area (who and when is allowed to enter, and to which area), including:

- restriction of access to the specified area
- identification of a person with access to the specified area

Other purposes:

- time and attendance;
- payroll accounting (if integrated with accounting systems);
- maintenance of staff/visitors database;
- integration with the security system, for example:
  - with video surveillance system;
  - with security alarm system (SOS);
  - fire alarm system (FAS).

At important facilities, the ACS network is not physically linked to other information networks.

# BARRIER UNITS

## MOUNTED ON DOORS:

Electric strikes are the least protected devices against burglary, and they are usually mounted on the inner doors. Electric strikes, like other types of locks, can be opened and closed by applying pressure.

Almost all electromagnetic locks are locked by applying pressure, so they can be installed on escape routes in case of fire.

Electromechanical locks are quite resistant to burglary, many of them have a mechanical reset (this means that if an opening impulse is given to the lock, it will be unlocked until the door is opened).

## INSTALLED ON THE WALKWAYS/DRIVEWAYS:

Turnstiles are used at the entrypoints of the officebuildings, public interest facilities (stadiums, railway stations, metro, some state institutions) - wherever the control ofcrowds is required. There are two main types of turnstiles: waist-high and full-height.

Man-traps are used in banks, at sensitive sites (in enterprises with high security requirements).

Gates and barriers are mainly installed at the entry points to the company's territory, in parking lots, around the entrance area, in the courtyards of residential buildings. The main requirement is resistance to climatic conditions and the possibility of automated control (using an access control system). When it comes to the access control, the system is subject to additional requirements — increased range of reading marks, recognition of vehicle plate numbers.

Automatic car barriers are used to ensure the prevention of unauthorized entry of vehicles into the protected area. Car barriers are counter-terrorism measures, since passing through a lifted up barrier can damage the vehicle's suspension.

## IDENTIFIER

Main execution types are a card, a keychain, a mark, a QR-code, a digital set, a fingerprint. It is the basic element of the access control system, because it keeps the code for determining («identification») the owner's rights. It can be a Touch memory, proximity card (for example, RFID tag), or an outdated magnetic stripe card. The identifier can also be a code entered on the keyboard, as well as individual biometric personal characteristics.

The reliability (resistance to burglary) of the access control system depends strongly on the type of identifier used. RFID tags with encryption capabilities that can store the card code in a secure storage area provide a fundamentally higher level of security.

## CONTROLLER

This is the «brain» of the system: it is the controller that decides whether to let the identifier owner in or not, because it stores the identifier codes with a list of access rights for each of them in its own non-volatile memory. The network controller is integrated into a single system with other controllers and a computer to provide centralized control and management. In this case, the decision to accessing can be made both by the controller and by software of the mainframe.

If the controller needs to be operated during power outages, its unit is provided by its own battery or an external battery pack.

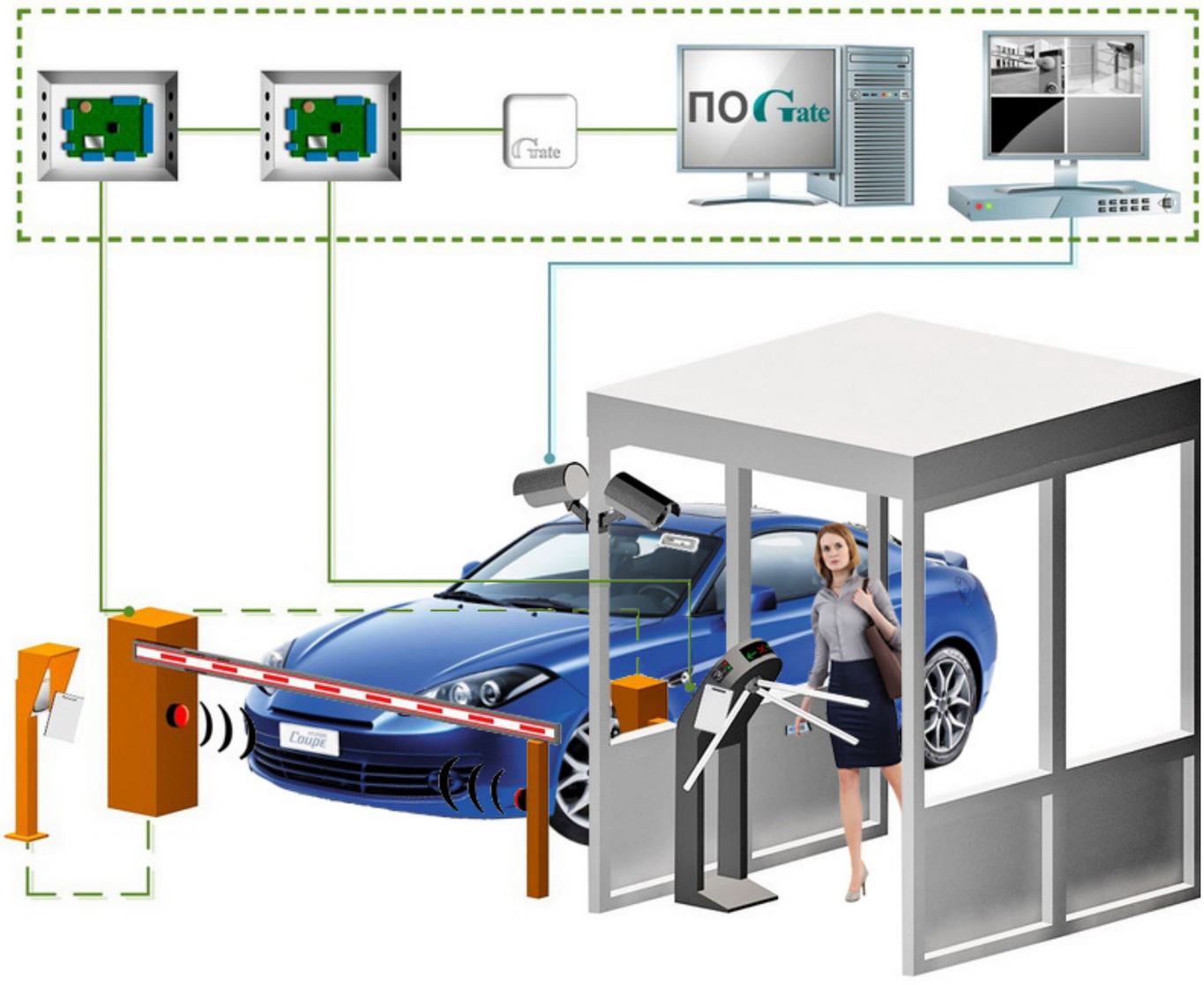
## READER

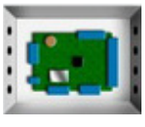
This device receives («reads») an identifier code and transmits it to the controller. Versions of the reader depend on the type of identifier. There are also readers for long-range identification of objects (with identification distance up to 50 m). These systems are good for driveways, parking lots, at the entry to toll roads, etc. Identifiers (marks) for such readers are active as a rule (have a built-in battery).

## MEDIA CONVERTER

They are used to connect the hardware modules of the ACS to each other and to the PC. Some ACS controllers already have a built-in Ethernet interface, which enables connecting to a PC and linking with each other without using any additional devices.

# ACS LINK CIRCUIT



Network access controller

RS-485/USB Converter

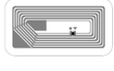
Dashboard camera

Access card reader

RFID card

Smartphone

Video surveillance camera



RFID sticker

Turnstile

Reader stand

Electromechanical barrier

# SOFTWARE

It is used where reporting, information processing on entries is required, or where the networking software installed on one or more PCs connected to the network is required for initial programming, management and collection of information duringthe system operation.

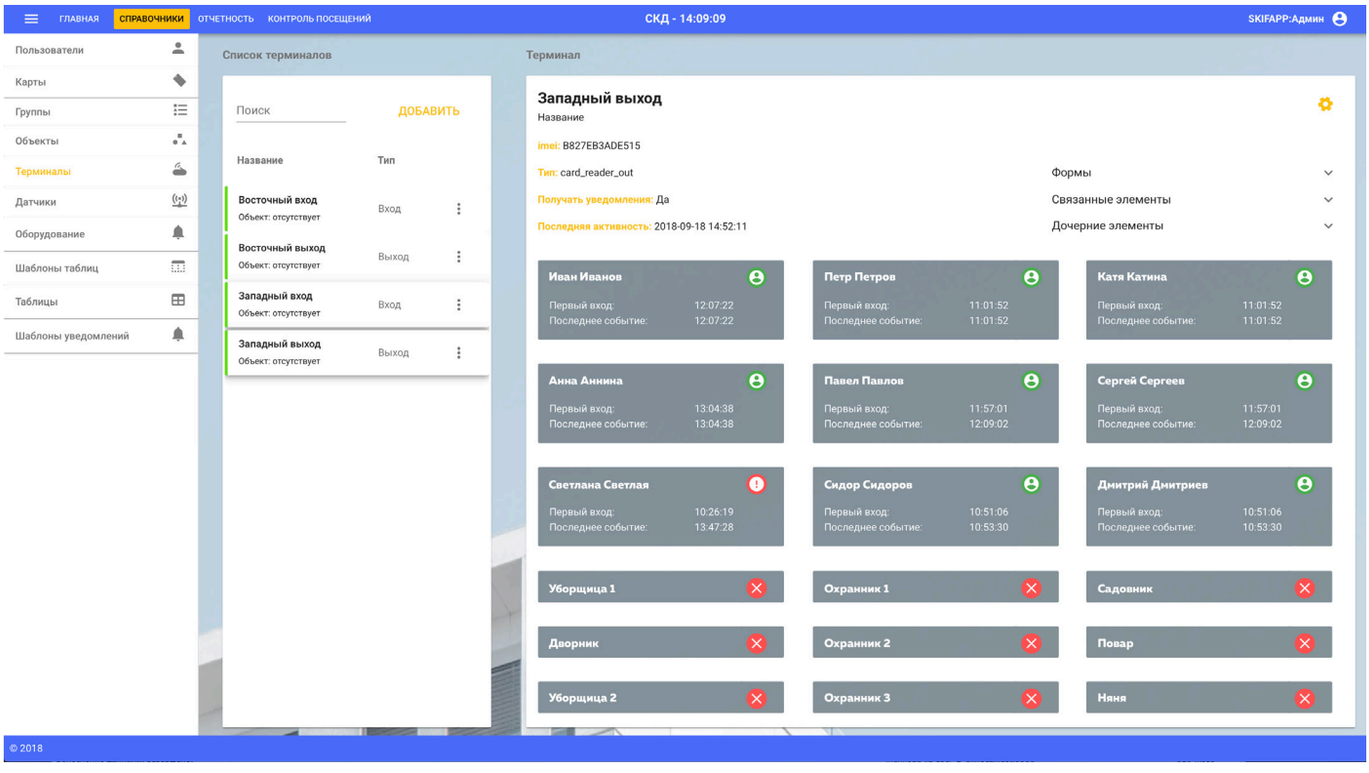
All ACS are divided into two categories: remote and network systems.

## REMOTE SYSTEMS

Remote systems are cheaper, easier to operate, no need to lay hundreds of meters of cable, use of computer pairing devices, or use of any computer. Some of disadvantages of such systems are: you can not create reports, control time and attendance, transmit and summarize information on events, and control remotely. When choosing a remote system with high security requirements, you are encouraged to pay special attention to the following:

- the reader shall be separated from the controller so that the lock can not be opened from the outside through wires.
- the controller must have a backup power supply in case of power failure.
- it would be preferable to use a reader in a vandal resistant housing.

The remote AC system also uses electronic locks that transmit information wirelessly: a mechanical latch with electronic control and a built-in reader is installed in the door. The latch is connected via radio to the hub, which is already exchanging information with the workstation, which have a software installed on.



## NETWORK SYSTEMS

In a network system, all controllers are connected to a computer, which offers many advantages for large companies, but it is not required for a «single-door» ACS. Network systems are good for large objects, as it becomes extremely difficult to control even a dozen doors with a remote system installed on. Network systems are indispensable in the following cases:

- if you need to implement complex algorithms for giving access to groups of employees with varying degrees of privilege to different areas at the enterprise and be able to change them quickly;

- if you need to selectively delete or create passes (marks) for a large number of entrance points or for a large number of employees (high turnover and loss of passes);

- if you need information on previous events (event archive) or require additional real-time monitoring. For example, the network system has a photo verification feature: at the entrance, when a person holds his/her identifier in front of the reader, the employee (door-keeper, guard) can see on the monitor screen a photo of the person to whom the identifier is assigned in the database, and compare with the appearance of the person passing through, that makes the cards non-transferable;

- if you want to control time and attendance and labor discipline;

- if the interaction (integration) with other security subsystems is required, such as video surveillance or fire alarm.

The network system allows not only to control events on all protected territory from one place, but also to centrally manage the rights of users, to maintain a database. Network systems help to arrange multiple work places, sharing the management functions between different employees and services of the company.

Wireless technologies, so-called radio channels, can be used in network access control systems. The use of wireless networks is often situation-specific: it is difficult or impossible to run a wire between objects, budget cuts for installation of the entrance point, etc. There are many options of radio channels, but only some of them are used in the ACS.

# ADDITIONAL FEATURES

- GSM module with SMS notification/alert that contains information on entrance;
- for network ACS - possible to control via the Internet remotely;
- system for plastic cards customization;
- «anti-passback» mode - if a person has already entered to the protected area, he/she cannot gain entry by the same identifier, which will prevent the card from being used by two or more people.

# ACS USERS FIELD

- corporate offices, business centers,
- banks;
- educational institutions;
- industrial enterprises;
- protected areas;
- vehicle parking lots;
- areas, where vehicles driving;
- private houses, housing estate,
- cottages, hotels;
- public institutions.


Russia, 119415, Moscow, Leninsky prospekt, 116, build. 1

**Technical support (free calls for Russia)**
8 (800) 222-02-75

**for stationary phone numbers (Moscow)**
8 (499) 431-70-00

**for mobile phones (Megafon, Russia)**
8 (925) 550-05-33

**Technical support**
zhminda@monitoring-plus.com

**Administration**
graf@monitoring-plus.com

**Website::**
www.monitoring-plus.ru