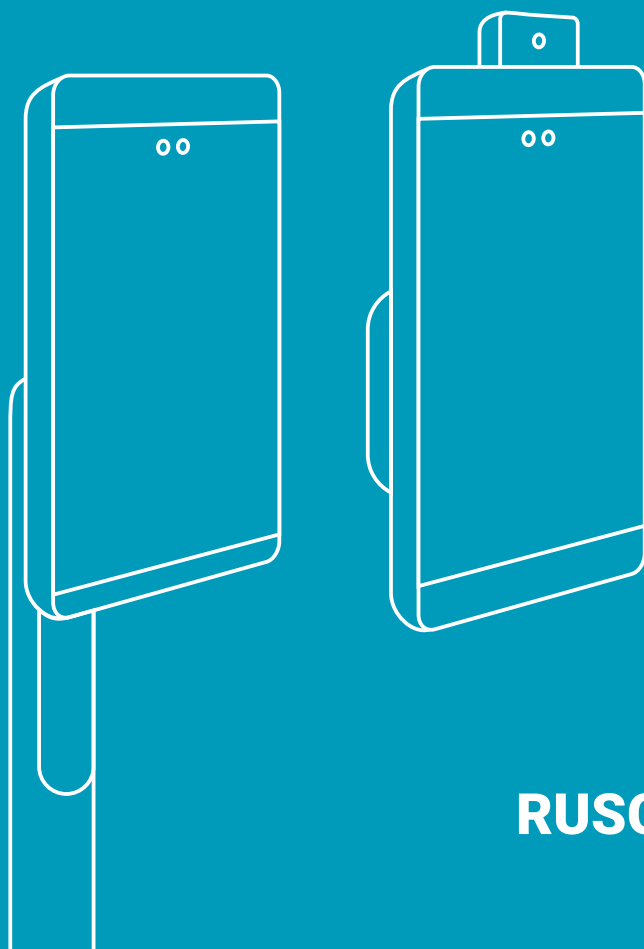


OPERATIONS MANUAL

FACE RECOGNITION TERMINALS

R20-FACE (8W/8T/Thermometer/SE)



RUSGUARD

General characteristics

The R20-Face is designed to identify a user by reading his biometric data (face). Double user identification is possible in the **Card and Face** mode. Terminals with built-in thermometer perform non-contact temperature measurement and mask check.

Terminal should be connected to the RusGuard access control panel via the RS-232 interface to run the “Card and Face” mode. Check the availability of these interfaces when ordering the access control panel.

Depending on the functionality and installation location, the R20-Face is available in the following modifications:

Name	Mount	Thermometer	Expanded memory
R20-Face (8W)	Wall		
R20-Face (8T)	Fare gate		
R20-Face (8W) Thermometer	Wall	Yes	
R20-Face (8T) Thermometer	Fare gate	Yes	
R20-Face (8W) SE	Wall		Yes
R20-Face (8T) SE	Fare gate		Yes
R20-Face (8W) Thermometer SE	Wall	Yes	Yes
R20-Face (8T) Thermometer SE	Fare gate	Yes	Yes

Terminal-controller communication interface: Wiegand 26/34/50, RS-232.

Terminal-server communication interface: Ethernet 10/100 BASE-T.

Default settings: Password – 12345678, IP address – 10.0.0.150.

Face identification distance	Adjustable within 0.5–4m
Face identification speed	<1s
Non-volatile memory	Up to 50,000 users Up to 100,000 users (SE model)
Screen	8" IPS LCD anti-glare touchscreen Resolution 1080x800 pixels, viewing angle 170 °
Backlight	Built-in, with white and infrared light
Camera (2 pcs.)	2.0 MP, viewing angle 95.8 °, focal length 5.75mm, aperture F2.7, WDR
Interfaces	RS-232, Wiegand 26/34/50, Ethernet, Wi-Fi
Power / Consumption	DC12V / 1A
For models with thermometer:	
Temperature measurement range	+34...+42 °C
Measurement accuracy	±0.3 °C
Measurement range	15–30cm
Operating temperature	-10...+50 °C
Humidity	Up to 90%
Ingress protection rating	IP54
Complete set	Terminal with bracket, 220V power supply, mounting kit, operations manual, packaging
For models:	
Dimensions and weight:	with bracket / without bracket / weight:
R20-Face (8W)	133x272x85.5mm / 133x272x23mm / 1.1kg
R20-Face (8W) with thermometer	133x298x85.5mm / 133x298x23mm / 1.1kg
R20-Face (8T)	126x448x113mm / 126x231x23mm / 1.5kg
R20-Face (8T) with thermometer	126x475x113mm / 126x258x23mm / 1.5kg

Dimensions, installation diagrams

All dimensions are in millimeters.

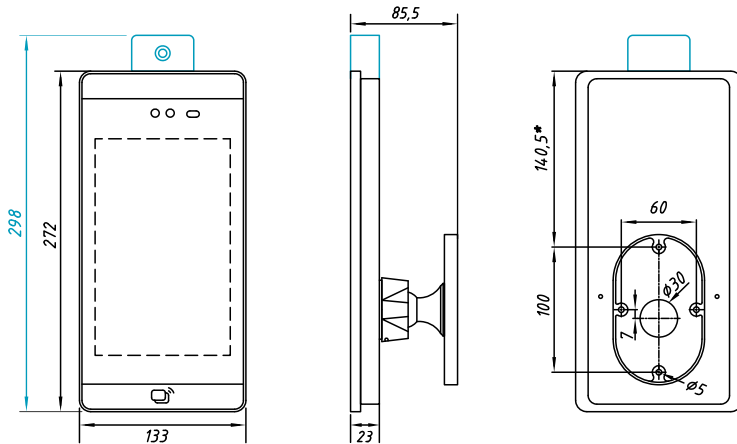


Fig. 1. Dimensions and mounting holes marking for any R20-Face (8W) modification

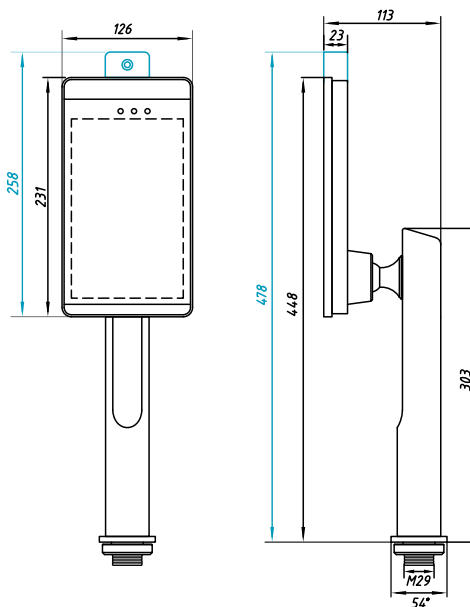


Fig. 2. Dimensions and mounting holes marking for any R20-Face (8T) modification

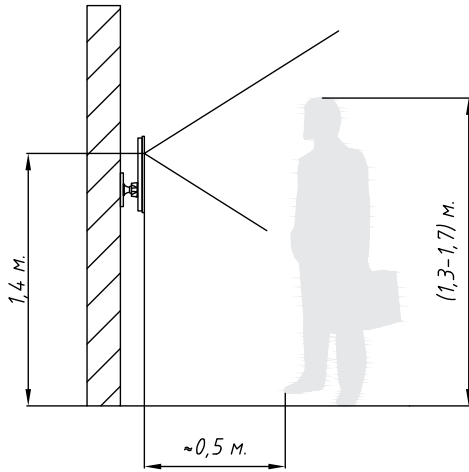


Fig. 3. Recommendations for installation of wall-mounted modifications of R20-Face terminal

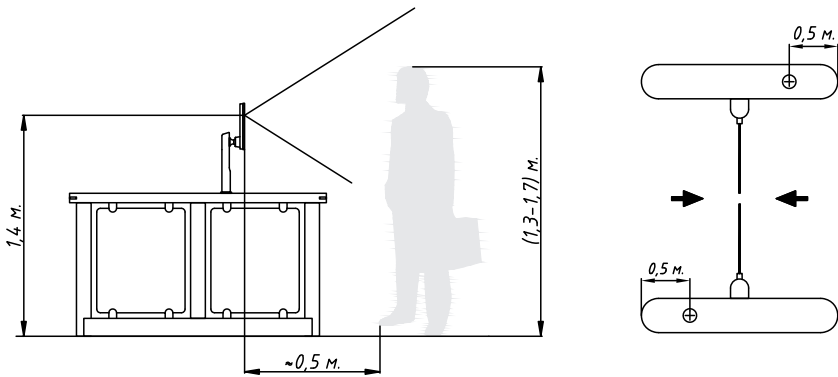


Fig. 4. Recommendations for installation of fare gate-mounted modifications of R20-Face terminal

The distance from the fare gate edge to the terminal location point is reference and may vary depending on the specific model of the fare gate.

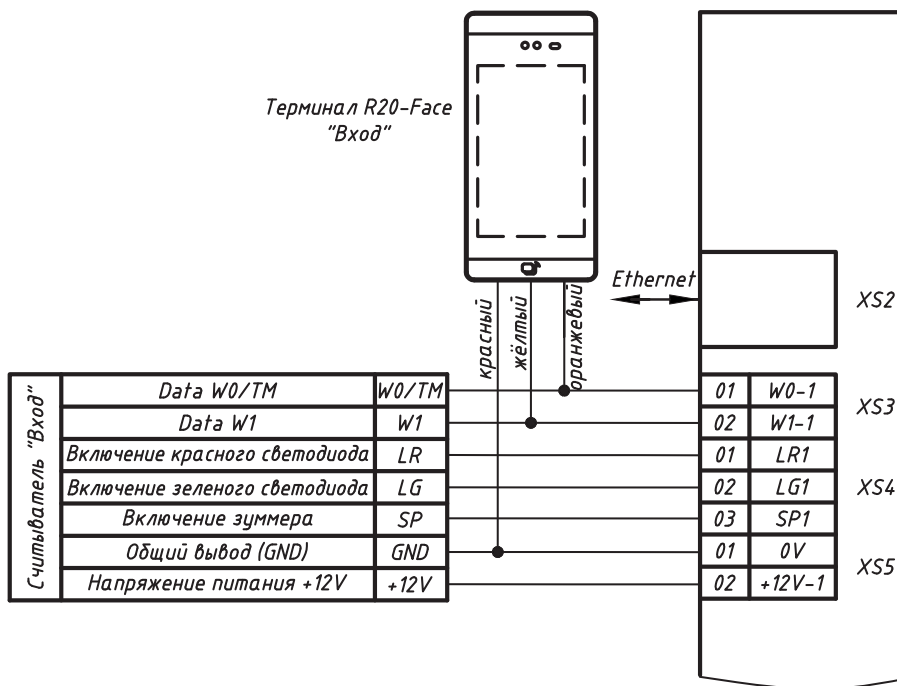
To install terminals on fare gates without a horizontal surface, it may be necessary to make individual brackets on your own.

Connection diagrams

To reduce the interference effect on the Wiegand line, the UTP 4x2x0.52 cable type is recommended.

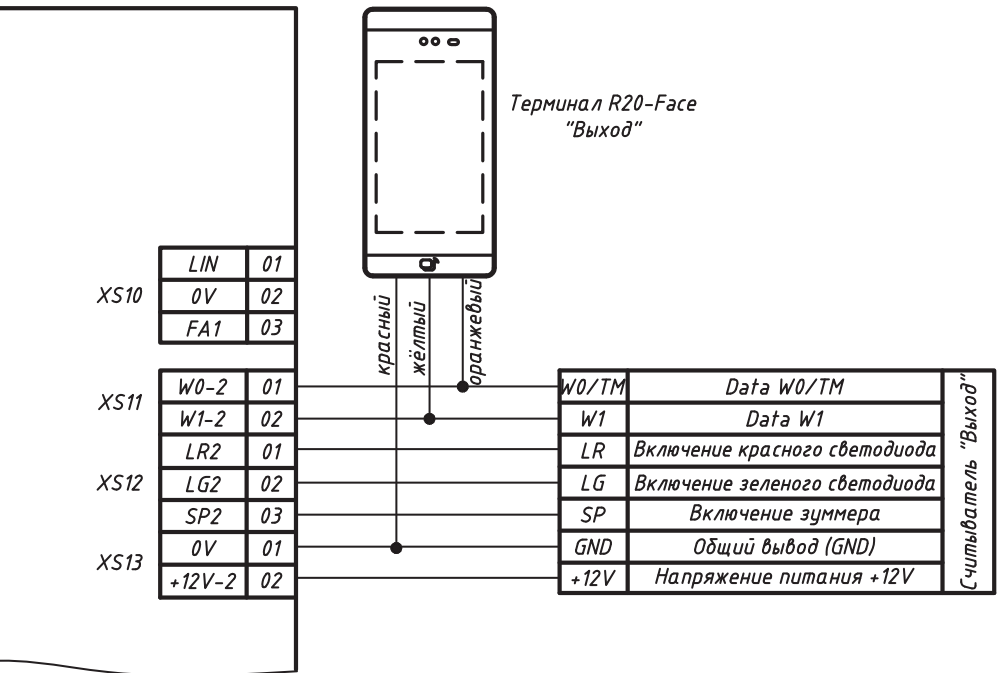
When the terminal is powered from an external power supply, it is recommended to use a cable with a cross-section not thinner than ШВВП (flat copper two-core cable with PVC insulation) 2x1.5 or analog. After turning on the terminal, make sure that the voltage is 12-12.2V. In case the voltage is less, increase it at the power supply or use a cable with a larger cross-section.

Do not forget to connect the terminals to the Ethernet network and configure the network parameters (see Configuring network parameters).

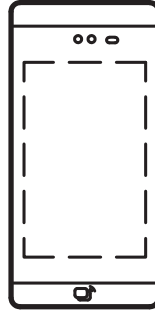


Connection diagram to access control panel
ACS-102-CE / ACS-105-CE / ACS-202-CE
 via Wiegand interface

To reduce the interference effect on the Wiegand line,
 the UTP 4x2x0.52 cable type is recommended



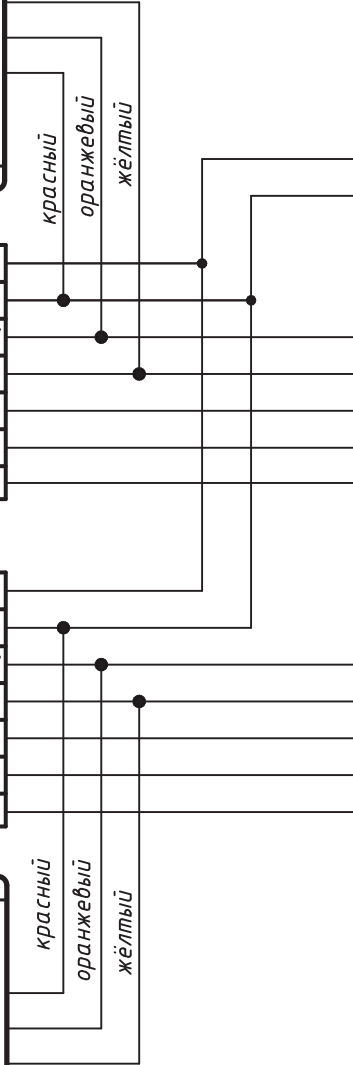
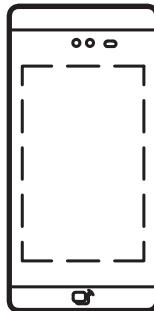
Терминал R20-Face
"Вход"



Считыватель "Вход"	Напряжение питания +12V	+12V
	Общий вывод (GND)	GND
	Data W0/TM	W0/TM
	Data W1	W1
	Включение красного светодиода	LR
	Включение зеленого светодиода	LG
	Включение зуммера	SP

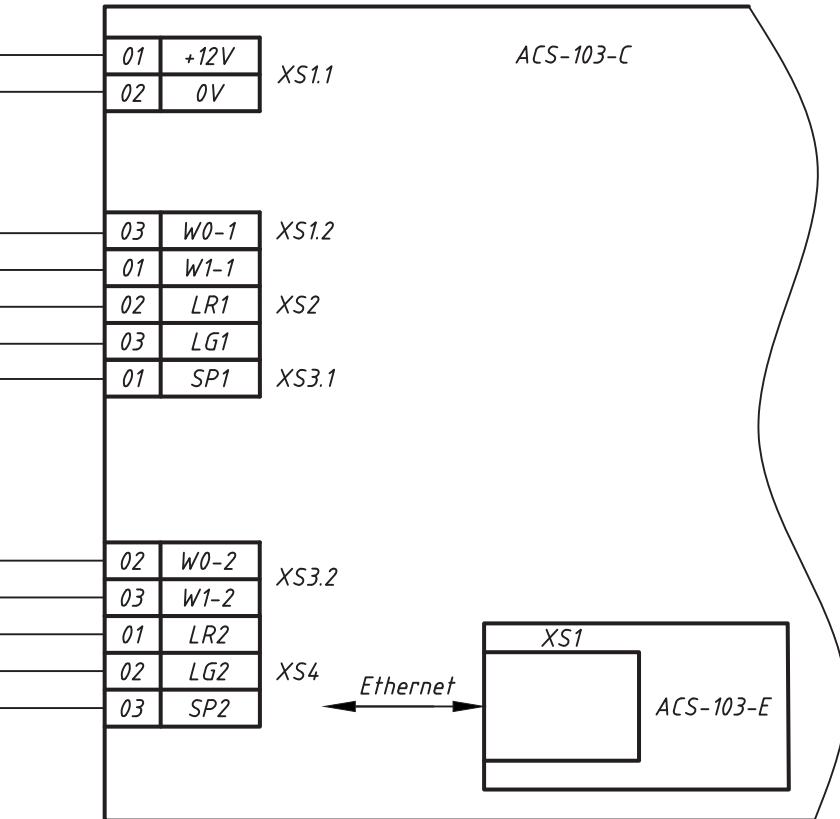
Считыватель "Выход"	Напряжение питания +12V	+12V
	Общий вывод (GND)	GND
	Data W0/TM	W0/TM
	Data W1	W1
	Включение красного светодиода	LR
	Включение зеленого светодиода	LG
	Включение зуммера	SP

Терминал R20-Face
"Выход"



Connection diagram to access control panel

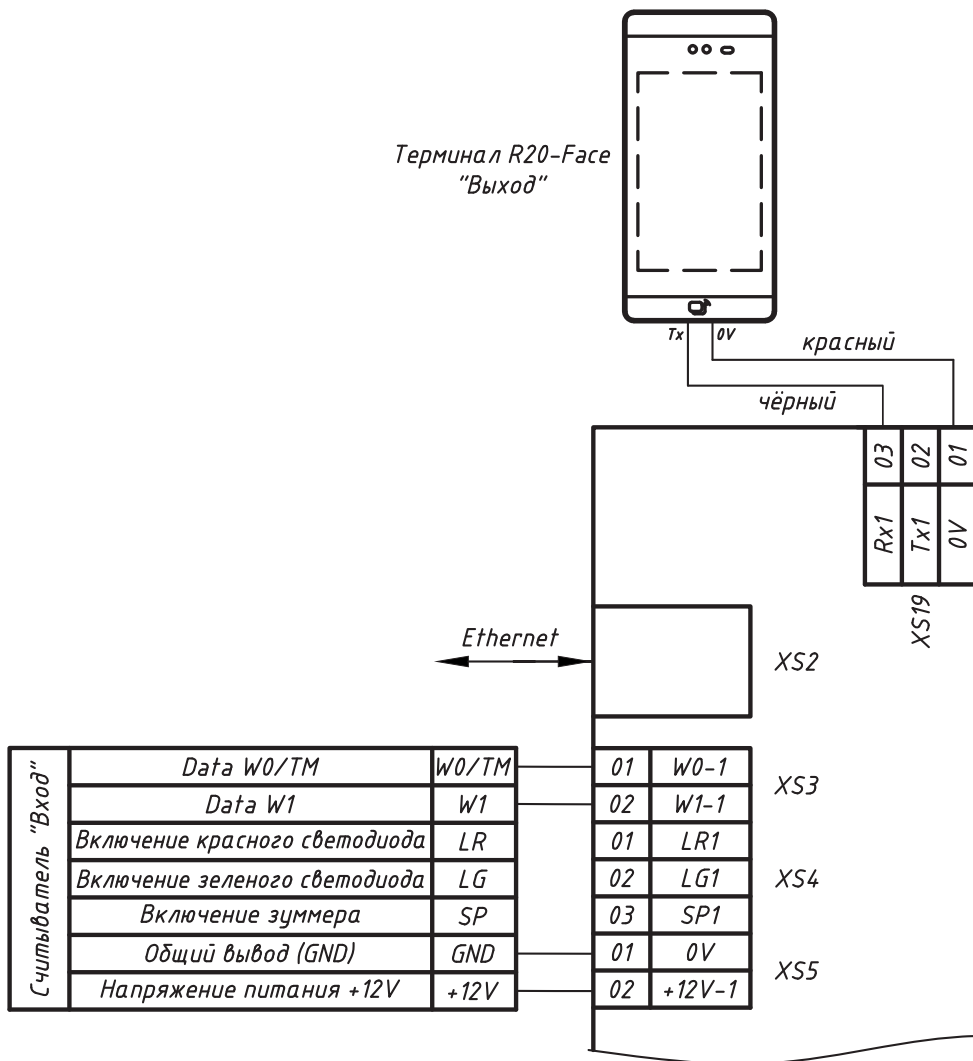
ACS-103-CE via Wiegand interface



To reduce the interference effect on the Wiegand line,
the UTP 4x2x0.52 cable type is recommended

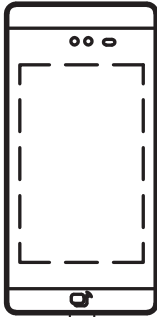
Connection diagram to access control panel

ACS-102-CE, ACS-105-CE, ACS-202-CE via RS-232 interface

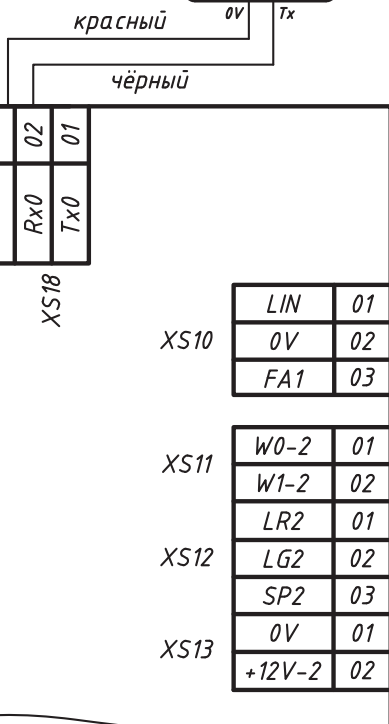


Not all modifications of RusGuard access control panels are equipped with RS-232 port.
Check the availability of these interfaces when ordering the panels.

To reduce the interference effect on the Wiegand line,
the UTP 4x2x0.52 cable type is recommended



Терминал R20-Face
"Вход"



W0/TM	Data W0/TM	"Выход"
W1	Data W1	
LR	Включение красного светодиода	
LG	Включение зеленого светодиода	
SP	Включение зуммера	
GND	Общий вывод (GND)	
+12V	Напряжение питания +12V	

Setting-up procedures

Mount the terminal following the recommendations.

Connect the terminal to the Ethernet network, to the access control panel via Wiegand or RS-232 and supply power to it.

After loading, the terminal operating interface will be displayed on the screen.

Configuring network parameters

The terminal default IP address is 10.0.0.150. There are two ways to change settings: via the terminal OSD menu or using the configuration utility.

Changing network settings via OSD (on-screen display)

1. To enter the configuration menu, click the ☼ icon in the lower right corner of the screen.
2. Enter the default password – 12345678.
3. Go to the **Network Config**, in the **Current connection**, click on **(!)** and by clicking on the **IP Addr**, specify the necessary network settings. When finished, click **Save** to save the data.
4. Please change the access code for security reasons! For this, go to **System Settings – Password Settings** and set a new password.

Changing network settings with the configuration utility

1. Download the utility from www.rgsec.ru/files/ftp/RusGuardFaceConfig.zip
2. Configure the 10.0.0.x network on the PC.
3. Connect the PC to the terminal or to the same network.
4. Run the utility, click **Check**. the “Serial number” should display the serial number of the terminal.
5. Set new network settings and click **Set**.
6. It is recommended to change the factory access password. Enter it in **New password** and click **Save**. Please note that after changing the terminal network settings, it is necessary to change the corresponding settings on the PC, and enter the new (assigned) IP address of the terminal in the utility.

Be sure to save the password if you change the preset one. In case of password loss, it can be reset only at the RusGard service center. This procedure cannot be done remotely.

Terminal configuration in RusGuard Software

System requirements for the correct operation of all terminal modes:

1. RusGuard Software version 2.4.5 or higher: www.rgsec.ru/support/software/programm
2. The access control panel firmware version is not lower than 5.05 (relevant when the terminal is connected via RS-232 interface): www.rgsec.ru/files/ftp/RusGuardControllerConfig.zip
3. Quickly configure the terminal in RusGuard Software following the detailed video instructions: www.rgsec.ru/face-recognition#settings

In the System **Administration** module, in the **System Configuration** section, check the following boxes:

1. In the “Photos and Images” section through the “Edit” button, check the box for the employee’s photo that will be used for face recognition (Fig. 5). Check only one photo.
2. In the “Biometrics” section through the “Edit” button, check the box next to “No card types” if your facility does not have separation of employee card types, or select the desired type of key that will be used for biometrics (Fig. 6). If you use one key for an employee and do not use the Type assignment to him, then select “No key type” in the biometrics settings. If you use several keys for an employee, for example Card and Mobile ID, then it is advisable to assign a Type to the main key, which should be selected when setting up biometrics.

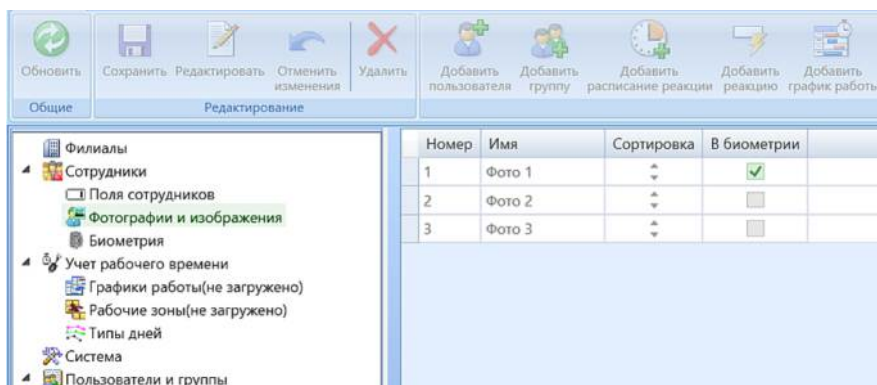


Fig. 5. Selecting a reference employee photo for recognition

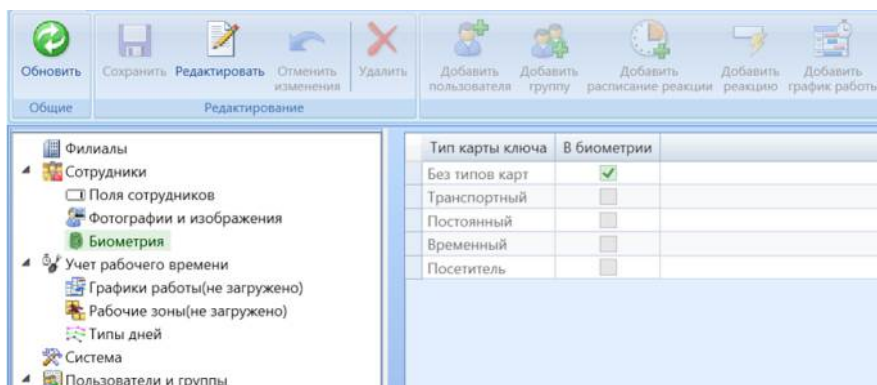


Fig. 6. Configuring recognition without using employee card types

Go to the **Hardware configuration**, select the controller to which the terminal is connected, and open the access point settings tab:

1. by **Edit** button, check the box next to the “Biometric reader” item and specify the IP address of the terminal connected to this controller (Fig. 7);.
2. when connecting the terminal via the Wiegand interface, set **Default** in the **Reader interface** setting. When connecting the terminal via RS-232 – select the **RS-232** item.
3. if necessary, configure other terminal settings such as **Recognition type**, **Recognition distance**, **Recognize among multiple faces**, etc.

Be sure to complete all actions with the **Save** button.

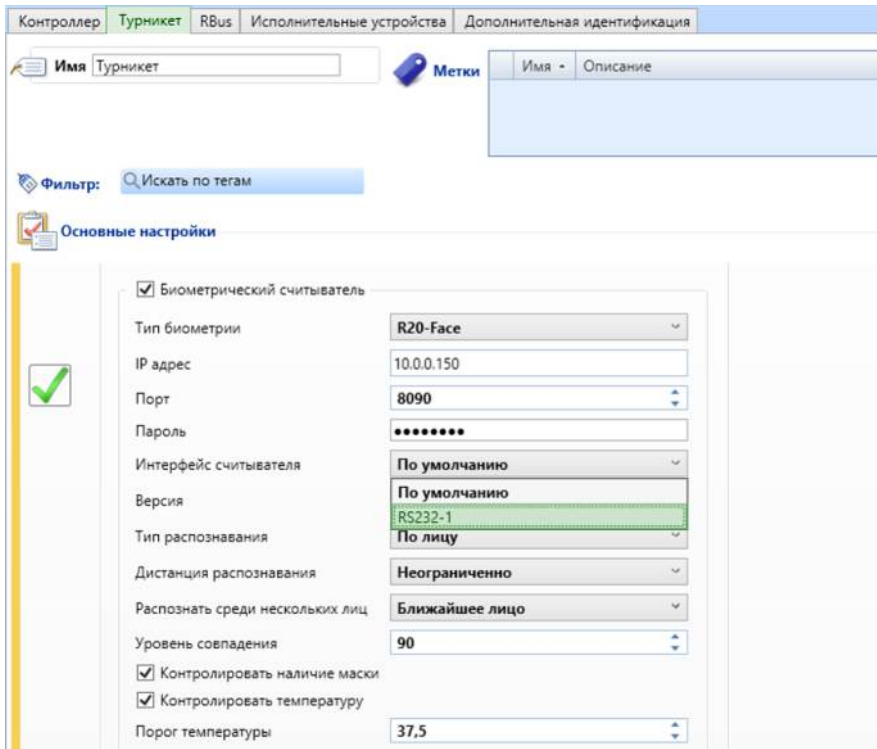


Fig. 7. Configuring the terminal connected to a specific panel

To check the correctness of terminal determination in the system, go to the **Service functions** tab, select the access point section and make sure that the terminal is connected (Fig. 8).

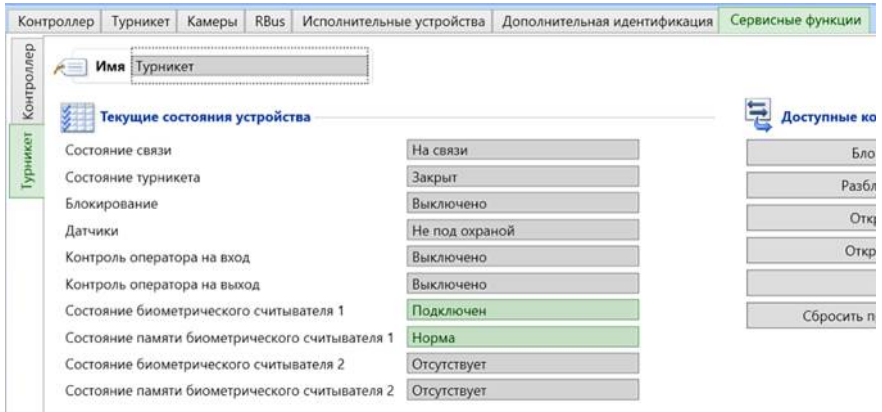


Fig. 8. Checking the terminal connection to the system

For a terminal connected via a Wiegand interface, no further configuration is required. If the terminal is connected via the RS-232 interface, it is necessary to make additional settings for the Access level:

1. Go to the **ACS (Access Control System) configuration, Schedules**. Draw up a custom schedule such as Pass 0-24 (Fig. 9).
2. Go to the **Access levels** section. Create a new access level and open the **Add Access Point** dialog. Select the drawn up **Pass** schedule and enable the **Multi-Factor Authentication** option.
3. For the **Card or Face** mode, add **By face (controller)** to the **Identification** section (Fig. 10). For the **Card and Face** mode, add **By face** to the **Controller** section (Fig. 11).
4. Save the access point settings.
5. Assign the created Access Level to Employees or Employee Groups.

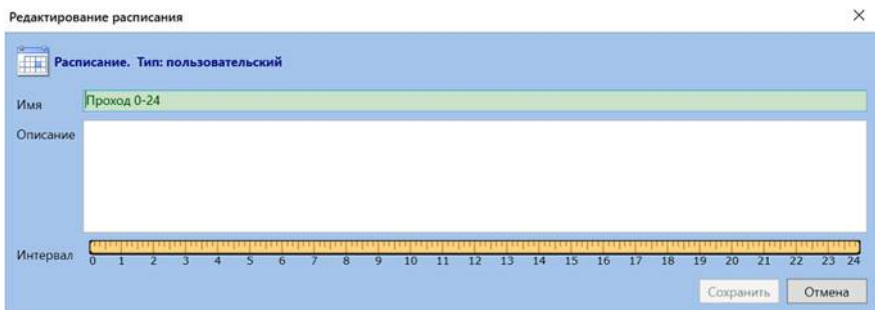


Fig. 9. Drawing up a custom schedule

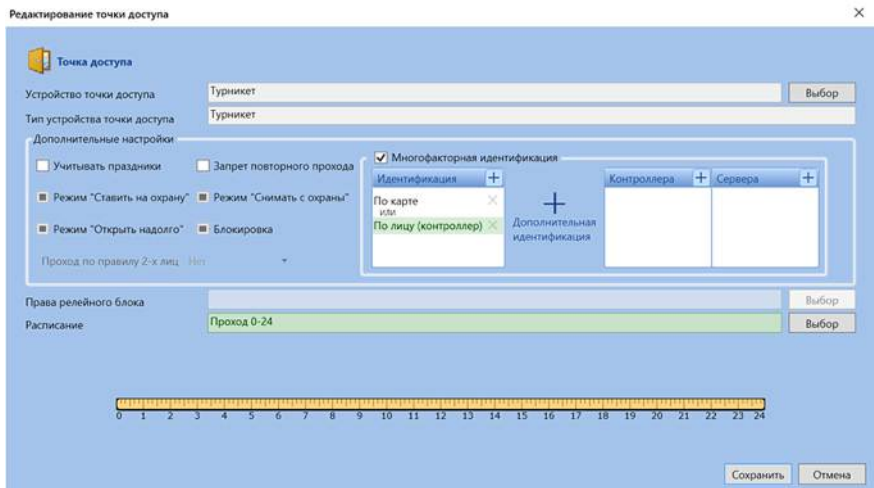


Fig. 10. Access level settings for **Card and Face** mode

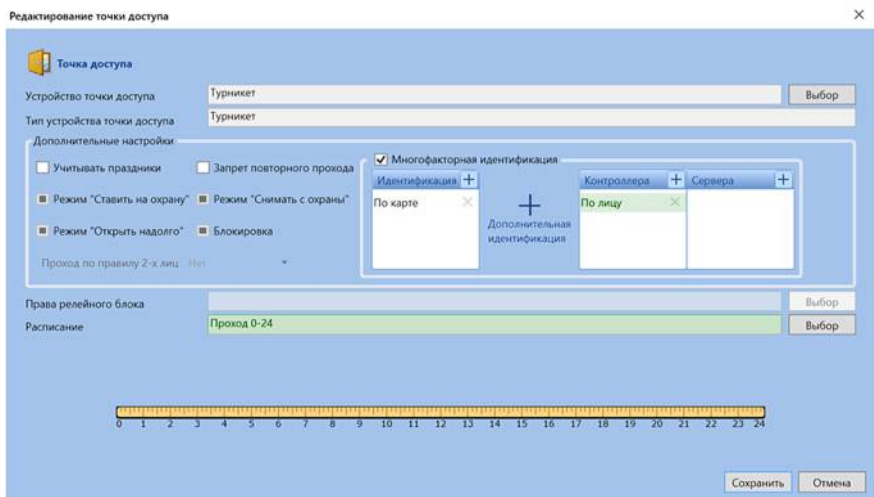


Fig. 11. Access level settings for **Card and Face** mode

Recommendations for quality of photos used for identification

Portrait photos taken on a solid background are best suited for identification, observing the following guidelines:

- the size of photos used should not exceed 1.3 MB
- the minimum resolution of the face area in the photo is not less than 320x240;
- the distance between the pupils is not less than 60 pixels;
- the recommended head size in the frame is 70% horizontally, subject to the recommended minimum resolution of the face area;
- head deviation – not more than 15 degrees vertically and horizontally;
- processing by any photo editors for correction (retouching of skin, lighting, background, etc.) is not recommended;
- photos should be taken with open eyes, gaze directed towards the camera, mouth closed.

Certificates

R20-Face terminals comply with the requirements of state standards and have the following certificates:



Certificate of Conformity No. РОСС.RU.HB25.H00091 No. 0473446 issued by the Rus-Test Limited Liability Company, 121357, Moscow, 67, Kutuzovsky prospect, building 2, apartment V, room 6, office 27.



Declaration of Conformity to the requirements of Eurasian Economic Union technical regulations EAEU N RU Д-RU.HA66.B.00720/19 dated October 25, 2019, issued by the Testing Laboratory of the PLANTEST Limited Liability Company, accreditation certificate РОСС RU.33071.ИЛ.000014.



Certificate of Conformity of technical arrangements of transport security to the requirements for their functional properties No. МВД РФ.03.000460 dated October 29, 2019, issued by the Certification Body for technical arrangements of transport security of Federal Government Institution “Scientific and Production Association “Special Equipment and Communication” of the Ministry of Internal Affairs of Russia.

Warranty

The product warranty is 1 year from the date of sale. The warranty is valid with a completed warranty card and a seal of the trading organization.

The reasons for warranty obligations termination may be:

- non-observance of operation rules, including installation and connection rules;
- mechanical damage or traces of exposure to water and/or aggressive substances;
- damage caused by careless storage or transportation through the buyer's fault;
- traces of unskilled interference in the device circuit.

During the warranty period, the manufacturer will fix the arisen faults free of charge. Repairs are performed in the manufacturer's workshop

Manufacturer: RusGuard JSC
Russian Federation, 127273, Moscow, 19, Signalniy proezd.
Tel: +7 (495) 369-09-90
Info@RgSec.ru
www.RgSec.ru

Acceptance and packing certificate

- R20-Face (8W)
- R20-Face (8T)
- R20-Face (8W) Thermometer
- R20-Face (8T) Thermometer
- R20-Face (8W) SE
- R20-Face (8T) SE
- R20-Face (8W) Thermometer SE
- R20-Face (8T) Thermometer SE

Manufacturing number _____

Day/Month/Year _____