Controller Description

The U-PROX IP400 controller is a device designed for managing access to residential and industrial premises, as well as for recording passage times and events.

The controller is supplied in a housing that includes a power supply unit.

The controller operates with two readers that are connected via the Wiegand interface.

The U-PROX IP400 processes the information received from the reader(s) and, using four relays, switches actuating devices (for example, locks, sirens, etc.). The presence of eight additional inputs with various programming options allows continuous monitoring of eight security zones (with current control). The controller can operate both autonomously and as part of a network. An Ethernet interface (wired computer network) is used to interconnect controllers in an access control system (ACS). :contentReference[oaicite:1]{index=1}

The controller features the ability to program network settings and update its firmware via a standard USB port (micro USB B).

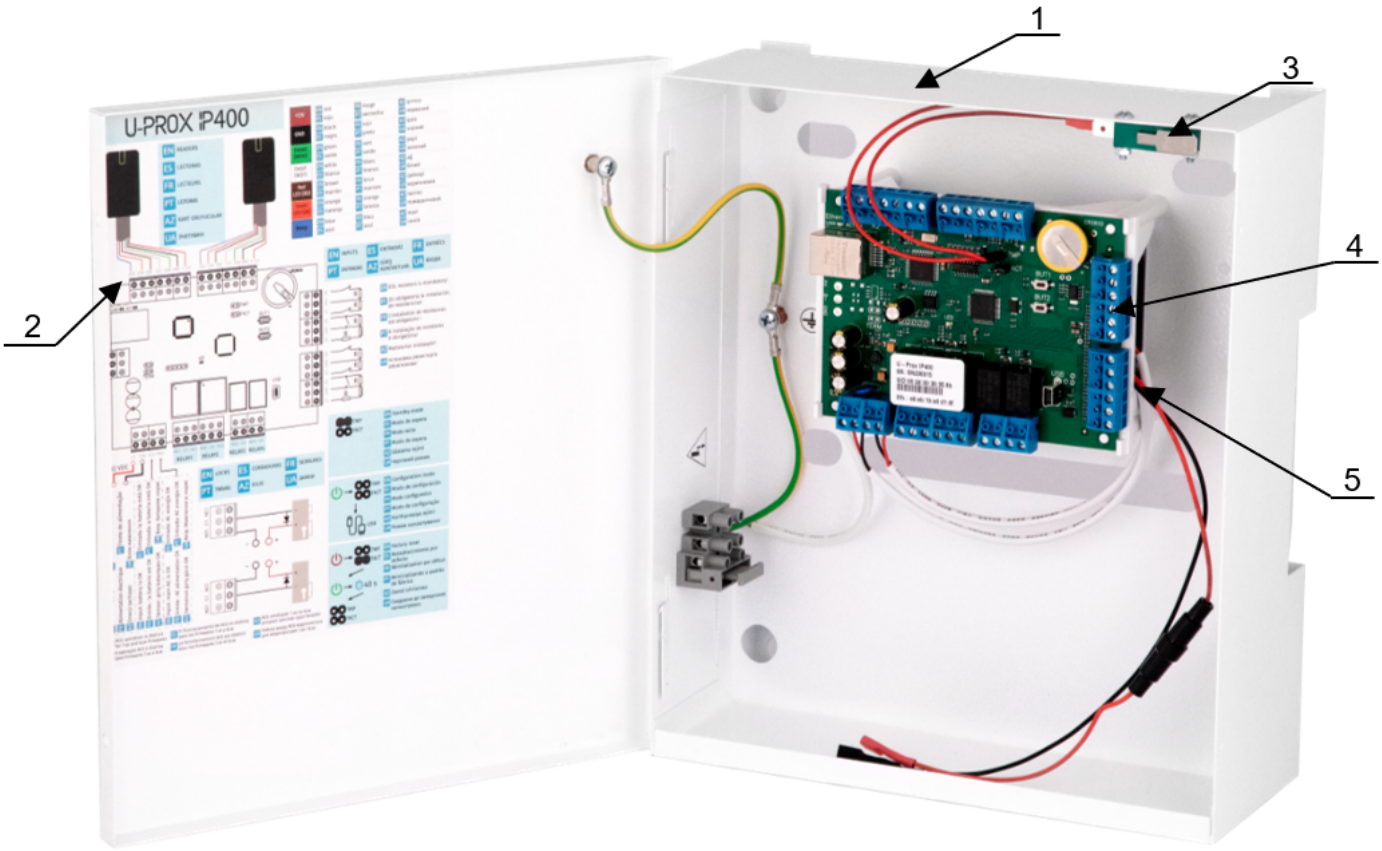
The controller is powered by a 12V source.

Purpose of the Device

The U-PROX IP400 controller is intended for use within access control and management systems (ACS) of various scales—from a small office ACS to the entry system of a large enterprise. In an ACS, controllers are networked together via a computer network. :contentReference[oaicite:2]{index=2}

The controller enables the organization of access to two separate premises or to a single premise with control over both entry and exit, as well as the installation of an alarm system for premises associated with these access points. In cases where both entry and exit of a space are controlled simultaneously, an “Anti-passback” function is provided.

Controller Construction

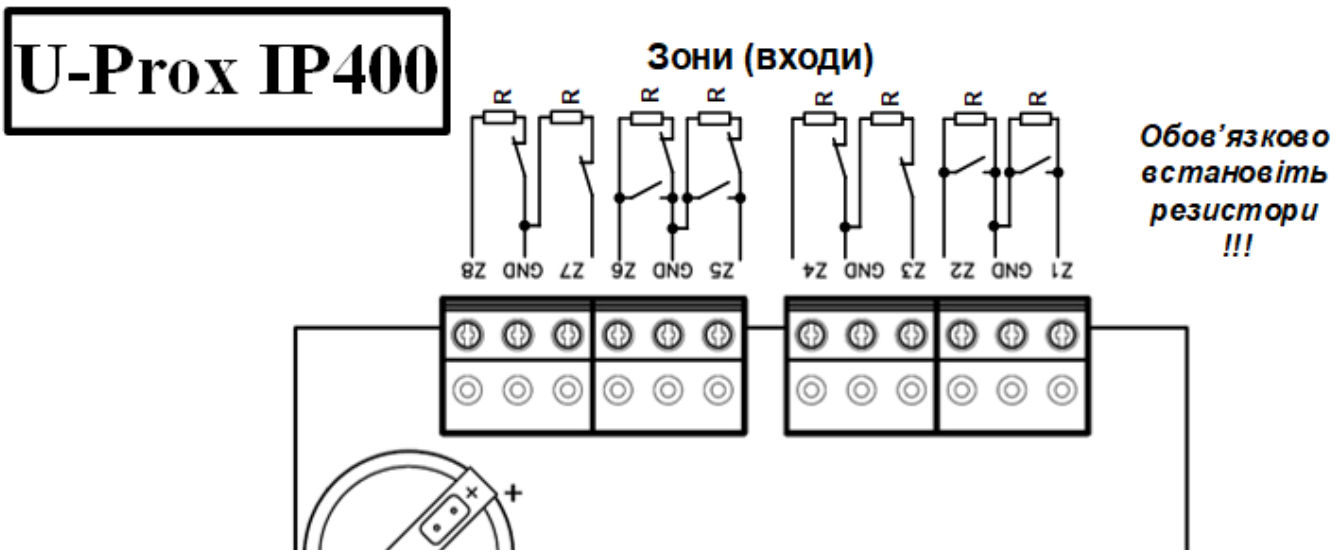


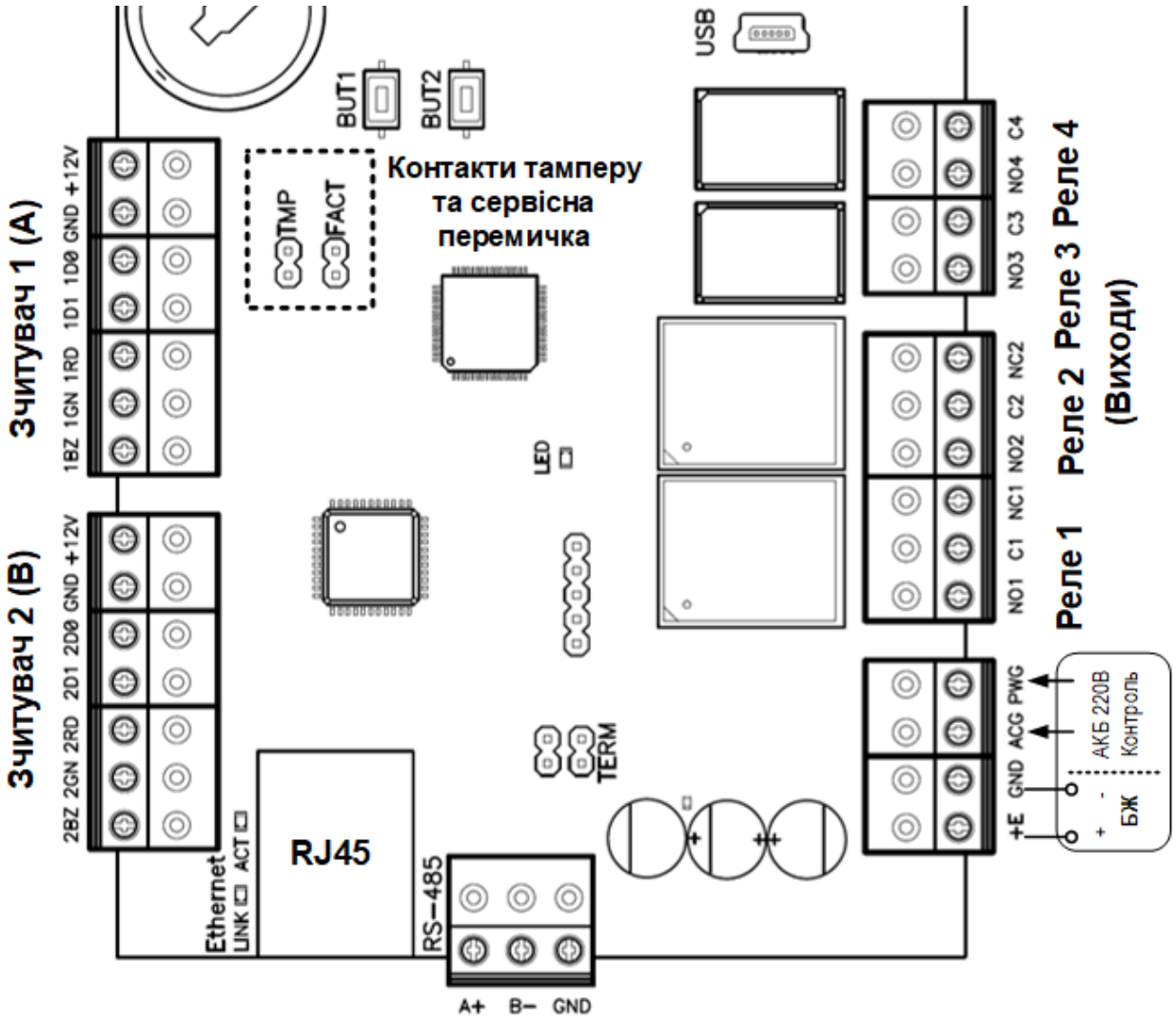
1. Device housing
2. Housing doors
3. Tamper (opening sensor)
4. Controller unit
5. Power supply unit

:contentReference[oaicite:3]{index=3}

Device Diagram

The layout on the controller board of jumpers, buttons, and removable terminal blocks with connectors, and their functions





Подключение считывателей	
№	Wiegand
BZ	Бузер
GN	Зелений світлодіод
RD	Червоний світлодіод
D1	DATA 1
D0	DATA 0
GND	- живлення зчитувача
+12V	+ живлення зчитувача

TMP FACT	**Черговий режим** Корпус приладу закрито (контакти TMP замкнуто)
TMP FACT	**Режим налаштування:** 1. Не вимикаючи живлення, відкрити корпус 2. Під'єднатись по USB
TMP FACT	**Режим зміни мікропрограми:** 1. Відкрити корпус приладу (порушити TMP) 2. Вимкнути пристрій 3. Подати живлення 4. Під'єднатися по USB (доступ дозволено протягом 10 секунд)
TMP FACT	**Скидання до заводських налаштувань:** 1. Відкрити корпус приладу (порушити TMP) 2. Вимкнути пристрій 3. Встановити перемичку FACT 3. Подати живлення 4. Зачекати 40-50 секунд, або, якщо підключені зчитувачі, дочекатися 6 коротких звукових сигналів

:contentReference[oaicite:4]{index=4}

Contact Assignment

Contact	Function
Z1	Input 1, contact for connecting cables
Z2	Input 2, contact for connecting cables
Z3	Input 3, contact for connecting cables
Z4	Input 4, contact for connecting cables
Z5	Input 5, contact for connecting cables
Z6	Input 6, contact for connecting cables
Z7	Input 7, contact for connecting cables
Z8	Input 8, contact for connecting cables
GND	Common contact (ground)
NC1	Relay 1 contacts, normally closed
NO1	Relay 1 contacts, normally open
C1	Relay 1 common contact
NC2	Relay 2 contacts, normally closed
NO2	Relay 2 contacts, normally open
C2	Relay 2 common contact
NO3	Relay 3 contacts, normally open
C3	Relay 3 common contact
NO4	Relay 4 contacts, normally open
C4	Relay 4 common contact
1BZ	Reader 1 connection (access point A), buzzer
1GN	Reader 1 connection (access point A), green LED
1RD	Reader 1 connection (access point A), red LED
1D1	Reader 1 connection (access point A), Data 1
1D0	Reader 1 connection (access point A), Data 0
+12V	Reader 1 connection (access point A), Power
GND	Common contact (ground)
2BZ	Reader 2 connection (access point B), buzzer
2GN	Reader 2 connection (access point B), green LED
2RD	Reader 2 connection (access point B), red LED
2D1	Reader 2 connection (access point B), Data 1
2D0	Reader 2 connection (access point B), Data 0

+12V	Reader 2 connection (access point B), Power
GND	Common contact (ground)
E+	External power source connection (+)
GND	External power source connection (–)
ACG	Battery status: normal
PWG	220V mains: normal
TMP	Housing opening sensor, tamper
FACT	Reset to factory settings
BUT1	Access request button for access point A
BUT2	Access request button for access point B
USB Micro B	USB port used for initial network configuration and firmware updates

Audio-Visual Indication of the Controller

LED	Description
LED, periodic blinking	• 1 short pulse per second – connection with the ACS server is normal; • 2 short pulses per second – connection with the ACS server is absent.
LED, rapid blinking	• Data is being loaded from the server.
Link, lit	• Ethernet cable is connected and functioning.
Link, unlit	• Ethernet cable is missing or faulty.
Act, rapid blinking	• Data exchange is in progress.

Audio-Visual Indication of the Controller Readers

The indication of access modes is performed by the controller's readers. Each controller can have its indication individually configured via the ACS software. The settings are presented in a table showing combinations of sound and light indications. :contentReference[oaicite:7]{index=7}

Controller Operation

Controllers are shipped in an unprogrammed state with factory settings. In this state, the controller's yellow LED blinks once per second. To operate the controller within an ACS, network settings must be loaded into the device using the "Configurator" software. :contentReference[oaicite:8]{index=8}

> It is recommended to install the supplied resistors on all controller inputs.

After the settings are loaded—and provided that all inputs are intact—the controller enters the "Normal" mode.

The controller can manage two independent access points. An access point can be configured in one of four modes: "Normal", "Alarm", "Lockout", and "Free Passage". The highest priority is given to the "Free Passage" mode, as this mode is activated in the event of a fire; followed by "Lockout", "Alarm", and "Normal".

"Normal" Mode

The Normal mode is the controller's primary operating mode. In this mode, the controller either grants or denies access to identifier holders.

Access on Presentation of an Identifier

To gain entry, the user presents a contactless identifier to the reader. If the identifier is registered and access is currently allowed, the door will open (the controller activates the actuating mechanism).

Access on Presentation of an Identifier and PIN Code

After presenting a registered identifier, the controller checks whether a PIN code is required. If so, it enters a state waiting for PIN code entry. Upon correct entry of the PIN code, the access point is opened (the actuating mechanism is activated).

Access via an Access Request Button (Remote Door Opening)

For exit from a premises with a single-sided access point or for allowing visitor entry, an access

request button is used. Pressing and releasing the button opens the access point (activating the actuating mechanism).

Access Denial on Presentation of an Identifier

Access may be denied for the following reasons:

- The controller is in an unprogrammed state;
- The card is not registered in the controller;
- The card's validity period has expired;
- Access is currently prohibited based on the schedule and/or day of the week;
- An attempt is made to re-enter when the "Anti-passback" function is active;
- The presented identifier is registered as lost or blocked;
- The controller is in "Alarm" mode;
- The controller is in "Lockout" mode;
- The validity period for a temporary card has not yet begun;
- The passage counter for a visitor's temporary card has been exhausted.

"Alarm" Mode

An access point enters "Alarm" mode in cases of unauthorized entry (forced entry), tampering with the controller housing, presentation of an identifier marked as lost, if the door remains open too long (exceeding the allowed open time), or if the identifier selection function is activated.

In "Alarm" mode, the controller activates outputs designated as ALARM and SIREN. The alarm output remains active until the "Alarm" mode is deactivated, and the siren output is programmed with a set duration for the siren sound.

If an access point is in "Alarm" mode, passage through it is blocked. The door may only be opened by pressing the exit request button.

"Alarm" mode can be deactivated by presenting an identifier marked for "Alarm Cancellation" or via a command from the computer.

"Free Passage" Mode

There are situations in an ACS when it is necessary to open the door for free passage of people—for example, in the event of a fire, earthquake, or other extreme situations. For such cases, the controller provides a "Free Passage" mode.

An access point enters "Free Passage" mode either by a command from an operator via the computer or by a break in the cable designated as FREE PASSAGE. The access point remains in

“Free Passage” mode as long as the free passage cable remains broken (if the cable is broken, the free passage state cannot be cancelled by operator command).

> The controller allows configuring the cable as a Free Passage function for access point A, access point B, or both (A+B).

While the access point is in “Free Passage” mode, the lock remains open continuously, and the controller logs every identifier presentation and code entry as an “Access Granted” event—regardless of the anti-passback, schedule, and other card attributes. This is used to track personnel presence during extreme situations.

When using locking devices with mechanical reactivation, it is essential to monitor the door status. Such devices are deactivated by an impulse of current and remain open until the door is closed. Upon door closure, the locking device returns to the locked state. In “Free Passage” mode, the controller checks the door contact and, after each door closure, issues another unlocking impulse to the lock.

> When operating the controller without a door contact (reed switch), using an “impulse” output type for unlocking the door is not recommended. In this case, the “Free Passage” mode will not function correctly – it will be impossible to open the door without presenting an identifier.

“Lockout” Mode

If a situation arises that requires the door to be blocked for all system users, the controller enters “Lockout” mode. When an access point is in “Lockout” mode, only identifiers with the “Security Service” attribute are granted access. In this state, the door cannot be opened by pressing the exit request button.

An access point enters “Lockout” mode either by a command from the computer or by a break in the cable designated as LOCKOUT. The access point remains in “Lockout” mode as long as the lockout cable remains broken (if the cable is broken, the lockout state cannot be cancelled by operator command).

> The controller allows configuring the cable for the Lockout function for access point A, access point B, or both (A+B).

Usage Options and Operating Modes of the Outputs

All outputs of the controller can be programmed for various uses: to control a lock, siren, alarm, or as a programmable output. In addition, each output can be programmed with an operating mode: continuous (the output remains active as long as the condition is met, for example, while

in “Alarm” mode), impulse (the output is activated for a set time), trigger (the output is activated on the first event and then deactivated on the next, and so on), or manual (the output is activated or deactivated by separate commands).

Operation of Identifiers (Cards)

Code (Electronic Card Code)

Each card has its unique code assigned during manufacturing. It consists of 10 hexadecimal digits.

PIN Code

This is an additional code assigned to the card. It must consist solely of six decimal digits. It can be used in conjunction with readers that have an integrated keypad.

After presenting the card to the reader’s built-in keypad, the PIN code must be entered and the “#” button pressed. If the correct PIN code is entered, the controller unlocks the door and grants access. Otherwise, the controller issues a warning signal, logs an “Incorrect PIN” event, and the door remains locked.

Validity Period

This is the expiration date of the card’s validity.

Alarm Cancellation

If a card designated for alarm cancellation is presented to a reader at a door in an alarm state, the controller logs an event “Alarm Cancelled” and returns the door to the normal state. If a card without alarm cancellation rights is presented, the door remains in its current state and an event “Access Denied. Alarm State” is recorded.

Security Service

This attribute grants the right to access even through locked doors. If the door is in “Lockout” mode, presenting a regular card will result in an “Access Denied. Lockout State” event. However, if a card with the “Security Service” attribute is presented, the controller grants access and logs an event “Access Granted. Lockout State”.

VIP

This attribute allows access at all times and in all areas, except when the door is in Lockout

mode. A card with this attribute can be assigned any schedule and is not subject to anti-passback or validity period restrictions. It may also include a PIN code. If the door is in “Lockout” mode, even a VIP identifier will not be granted access.

Anti-passback Disabled

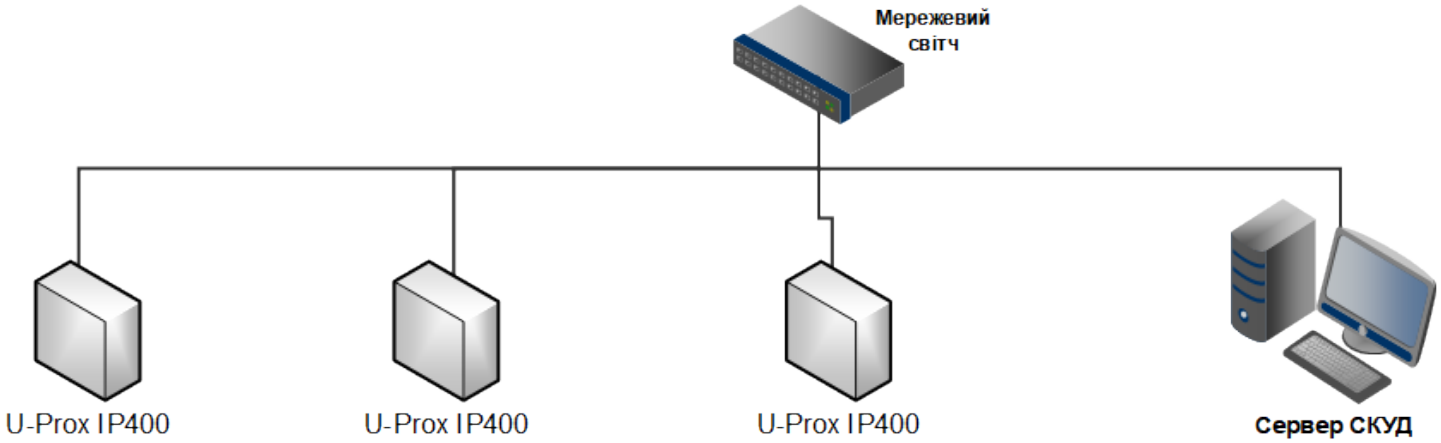
This setting allows access without considering the anti-passback function. Such a card is granted access regardless of the direction of the previous passage, but still subject to the assigned schedule and other card attributes.

Operation of the Communicator

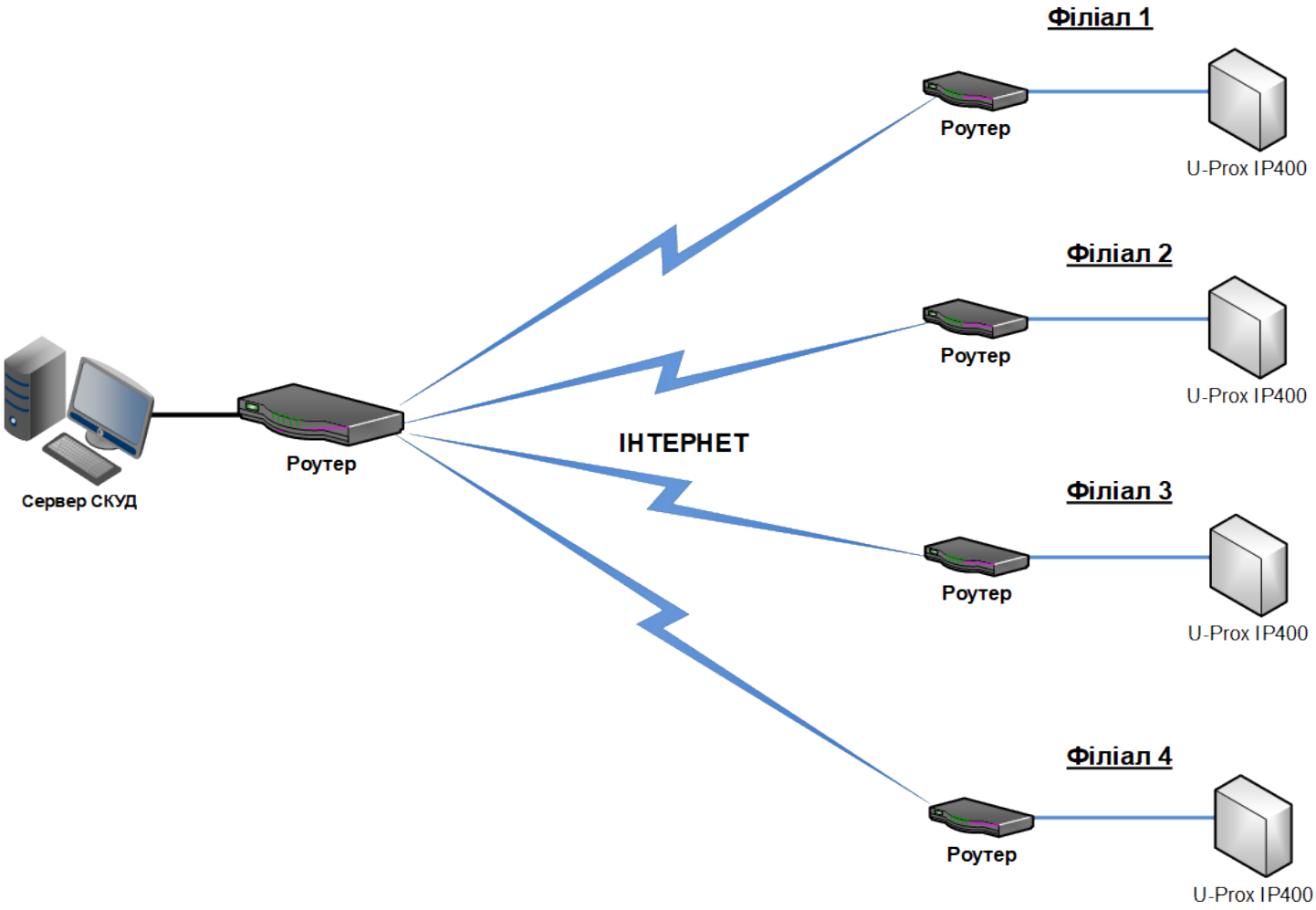
The U-PROX IP400 controller operates in an automatic mode. After loading data from the server, it enforces access rules for the presented cards and sends access event notifications to the ACS server. :contentReference[oaicite:9]{index=9}

The controller’s communicator works in notification mode, meaning that when an event (passage or zone violation) occurs, data is transmitted to the ACS server.

The U-PROX IP400 controller can be connected to a computer network via a wired Ethernet connection. In this case, it supports both operation within the enterprise’s local network, as well as via the Internet.



It also supports Internet connectivity, allowing for distributed access control systems of any scale.



Device configuration can be performed either via auto-configuration or manually from a PC using the “Configurator” software. When properly configured, the following is ensured:

- The device is assigned either a static or dynamic (DHCP) IP address;
- It operates with either an IP address or a DNS (domain name) address for the ACS server;
- It supports Internet operation (for servicing remote branches) with the possibility of redundant Internet paths through a secondary router;

:contentReference[oaicite:10]{index=10}

The controller operates in automatic mode – after loading data from the server, it enforces access rules for the cards and sends corresponding notifications to the server.

The communicator functions in notification mode, meaning that when an event occurs (such as passage or a zone violation), data is transmitted to the ACS server.

When operating on a computer network, the controller ensures protection against unauthorized interference by encrypting data packets using a 256-bit key and by verifying the unique serial number of the device, as well as by monitoring the communication channel through periodic test signals from the device.

Local Network Operation Algorithm

1. Upon power-up, the controller checks whether DHCP is enabled (device IP address is 0.0.0.0) or if the device has obtained a static IP address;
2. If DHCP is enabled, the dynamic IP address assignment procedure is initiated;
3. The IP address status is periodically updated (maintaining the reserved IP address if DHCP is enabled);
4. The availability of the ACS server and the U-PROX IC A controller is determined (via IP or DNS name);
5. Periodic test signals are sent;
6. Access events are transmitted;
7. The controller waits for commands.

Internet Network Operation Algorithm (Local Wired Network)

1. Upon power-up, the controller checks whether DHCP is enabled (device IP address is 0.0.0.0) or if it has obtained a static IP address;
2. If DHCP is enabled, the dynamic IP address assignment procedure is initiated;
3. The IP address status is periodically updated (maintaining the reserved IP address if DHCP is enabled);
4. The possibility of Internet access is determined (by checking the availability of the routers' IP addresses);
5. The availability of the ACS server and the U-PROX IC A controller is determined (via IP or DNS name);
6. Periodic test signals are sent;
7. Access events are transmitted;
8. The controller waits for commands.

:contentReference[oaicite:12]{index=12}

Auto-Configuration of Controllers in a Peer-to-Peer Network

By using the existing network infrastructure and standard network protocols (such as DHCP), the "plug-and-play" principle is implemented. The auto-configuration mode for the server address on the devices greatly simplifies the deployment of the access control system.

1. After power-up, the controller checks whether DHCP is enabled (device IP address is 0.0.0.0) or if it has obtained a static IP address;
2. If DHCP is enabled, the dynamic IP address assignment procedure is initiated;
3. If no ACS server address (IP or DNS name) is set, the controller enters auto-configuration mode:
    a. The device broadcasts data packets announcing itself as a new device on the local network.

b. Upon receiving a packet from a new device, the system operator is notified. The operator must then add the device to the database.
c. After the device is added to the database, it receives a response packet from the ACS server. The server address is then stored in the controller's settings, and the broadcast stops.
d. After the controller's parameters are configured in the database, the operator must load the device. The device will then be linked to that ACS, preventing unauthorized control interception.
e. If the server address changes, the device will re-auto-configure; however, data exchange will only be possible with the ACS to which the device is already bound.

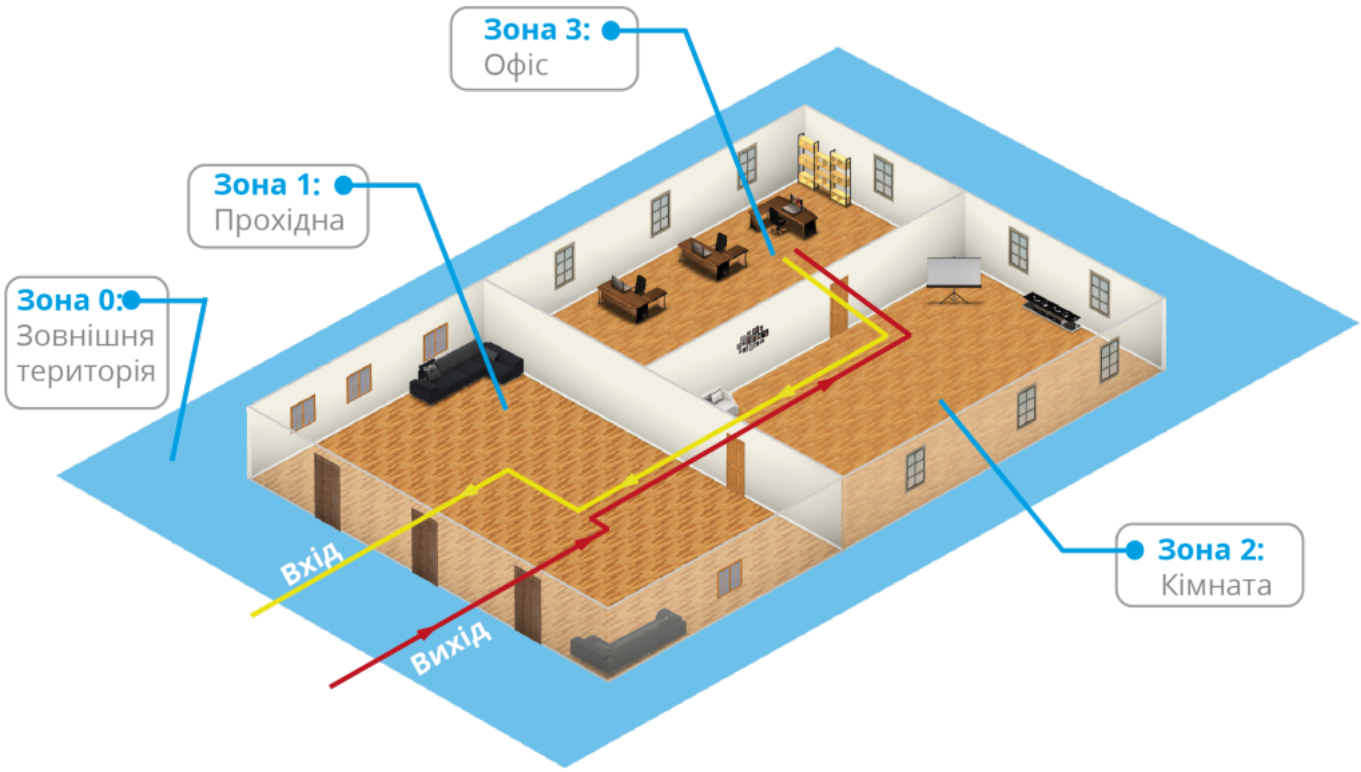
4. If necessary, the controller can be reset to factory settings to cancel its binding.

Although this broadcast is limited to the peer-to-peer local network and active network equipment, for networks with complex topologies the ACS server's IP address must be set manually.

To cancel the controller binding, it must be reset to factory settings.

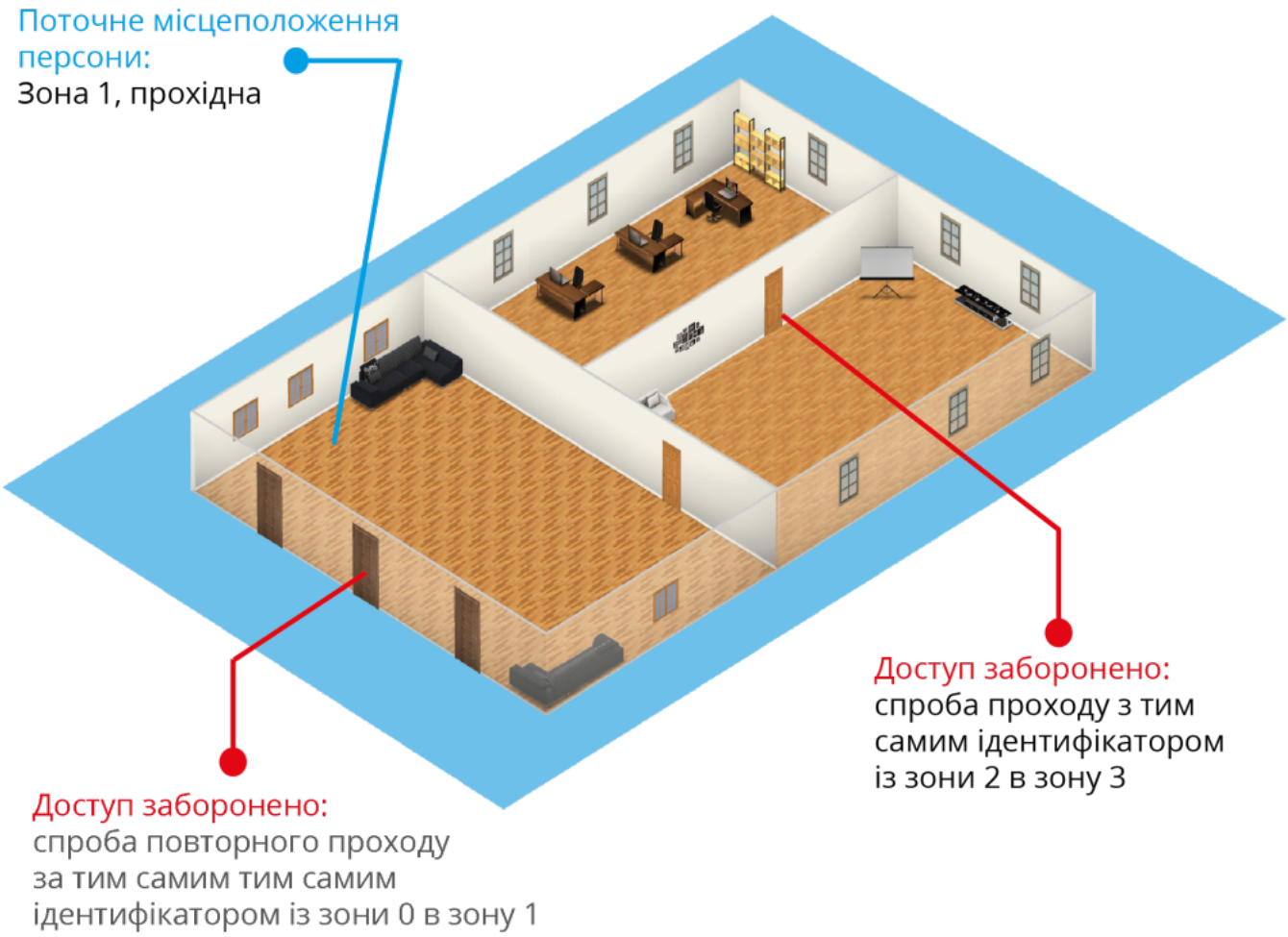
Global Anti-passback

The U-PROX IP400 controller can operate as part of a global anti-passback system. In this case, a master controller of the U-PROX IC A series tracks the location of a person based on their passage through a door, receiving data from U-PROX IP400 controllers. The global anti-passback is based on zone-based anti-passback. The premises are divided into rooms – access zones. With such a division, entering another zone is considered an exit from the previous one. Passage to a zone is possible through different doors. The anti-passback controller tracks employee movements from one zone to another by receiving data from the access controllers.

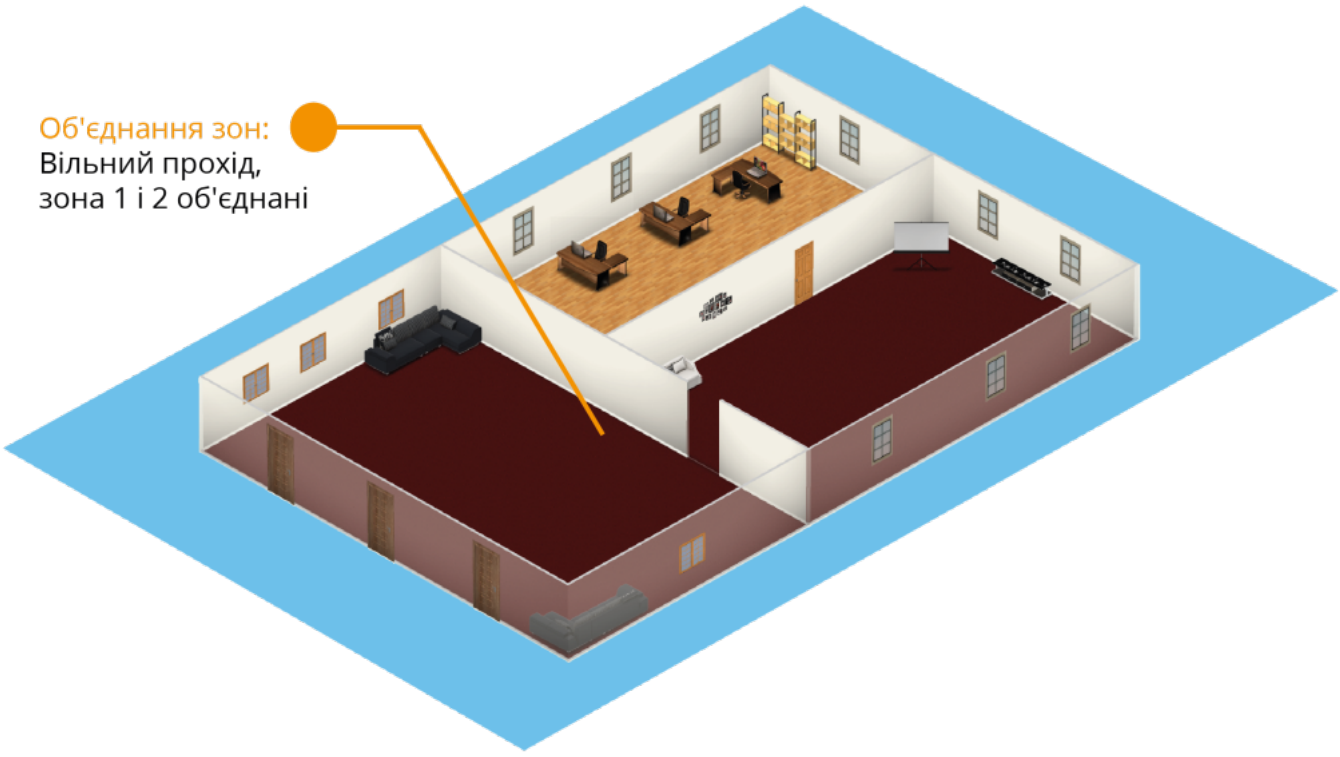


Initially, an employee's location is "Undefined" and only after the first presentation of an identifier to a reader is their location recorded by the U-PROX IC A controller. The "Undefined" status is assigned during the registration of a new employee or after the operator issues a "General Location Reset" command.

Using the global anti-passback system, repeated passages, card duplication, unauthorized entry (unexpected presence inside), sharing of identifiers, etc., can be prevented.



If communication with the ACS controller is lost, if the door is forced open, or if the door switches to free passage, the anti-passback controller groups the access zones into one, assuming that personnel may be present in both zones. When the door or connection is restored, the zones are separated again. The actual location of personnel is then determined by subsequent presentations of the identifier to the reader.



If communication with the U-PROX IC A controller is lost, U-PROX IP400 access controllers can be configured to behave in one of two ways:

- Block all access
- Grant access according to the locally stored person location data from the anti-passback function

Requirements for Configuring the U-PROX IC A Controller

- The controller must have a static (fixed) IP address.

Requirements for Configuring U-PROX IP400 Controllers

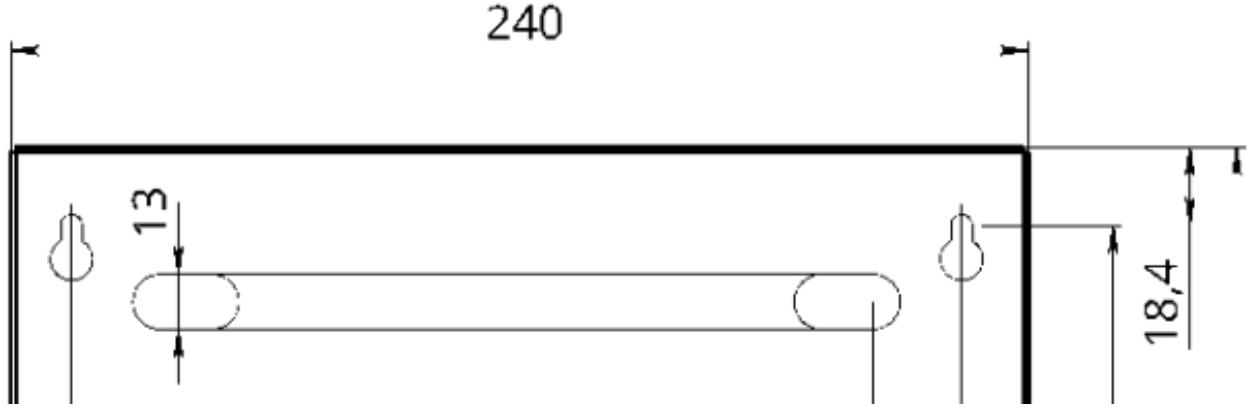
- Only controllers with double-sided doors (entry and exit by identifier presentation) participate in global anti-passback.
- The first ACS server address in the device's communication settings must be the address of the computer running the U-PROX IP server software.
- The second ACS server address in the communication settings must be the address of the U-PROX IC A controller.
- The ACS must have the "General" anti-passback mode enabled for the doors.
- The access controller in the ACS must have the master anti-passback controller specified, along with the corresponding reaction to communication loss.

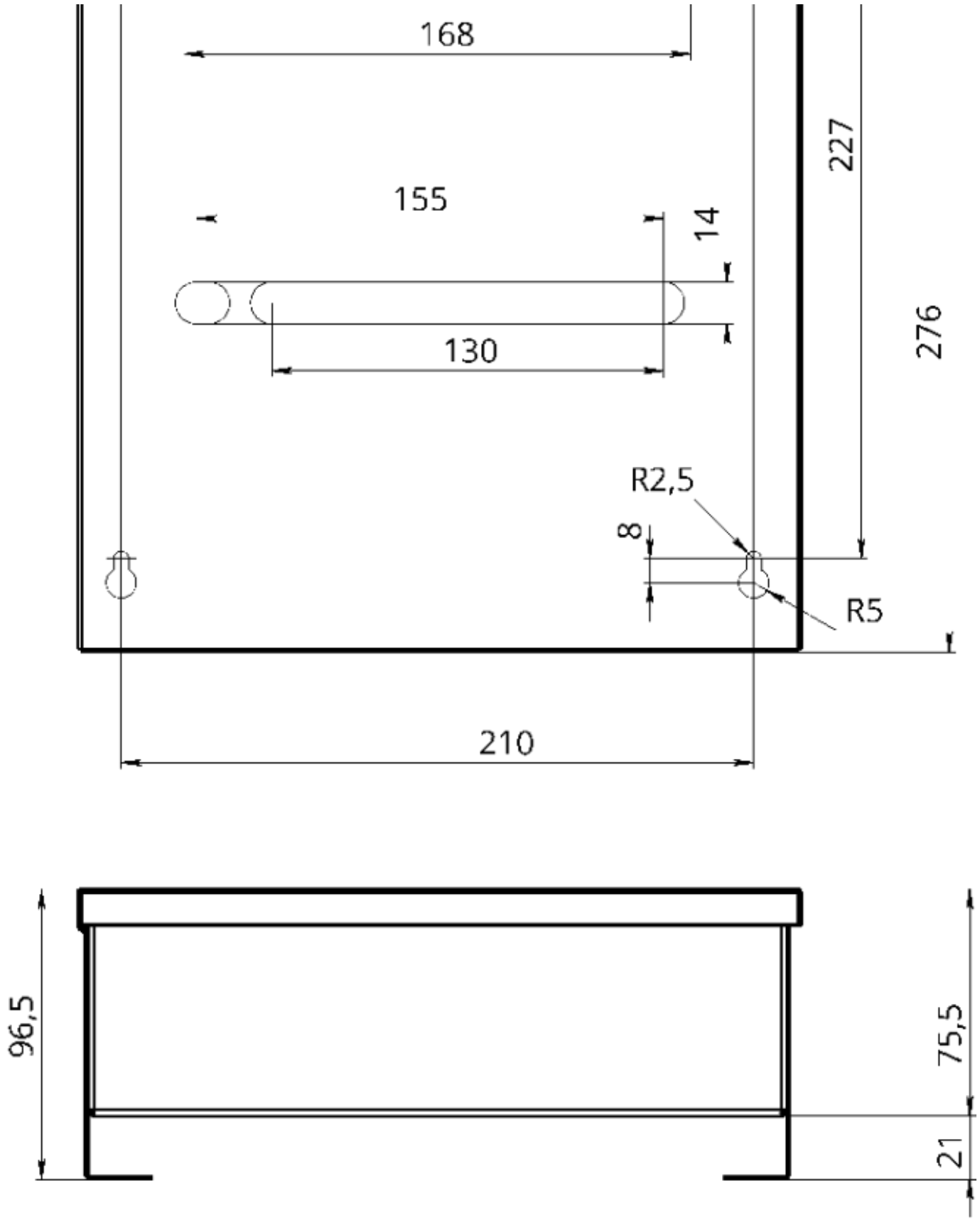
U-PROX IP400 controllers send access event notifications to two addresses simultaneously. The first address is the ACS server, where events are displayed and stored in the application's database. The second address is the U-PROX IC A controller, which responds with a command to either deny or grant access.

> After presenting an identifier, the delay in granting or denying access may be up to 1 second depending on the network topology and bandwidth.

Operating Procedure for the Device

The controller is supplied in a metal housing with its power source. The overall dimensions of the device are shown in the illustration below.





Mounting Recommendations

The controller should be installed in a location that is accessible for maintenance.

To mount the controller on a wall, perform the following steps:

- Open the housing cover, hold the housing against the intended mounting location, and

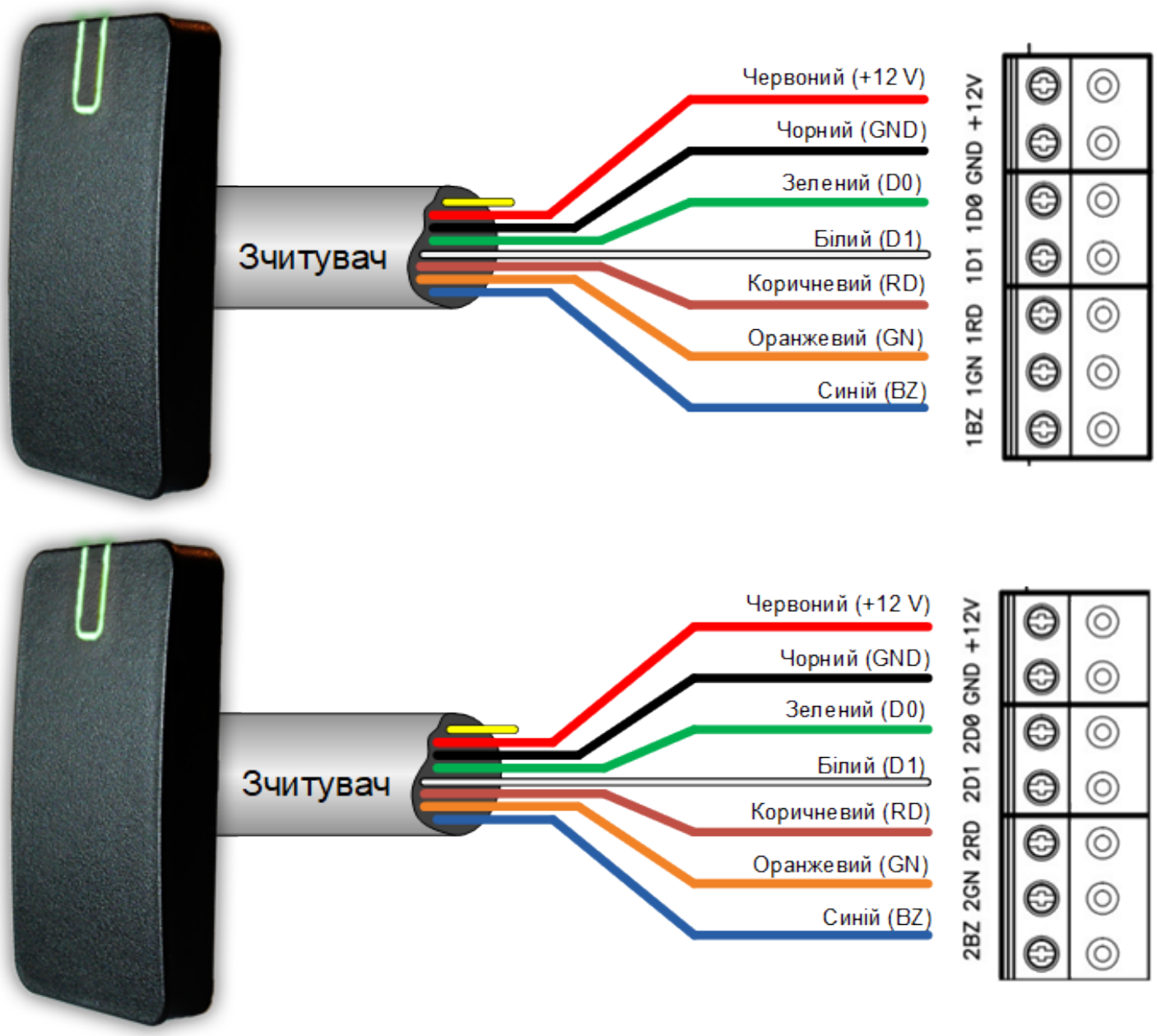
mark the drill holes;
- Run the cables through the holes in the housing wall;
- Secure the controller housing;
- Connect the cables.

Connection Procedure

1. Before installation, perform the initial configuration (set the network parameters) of the controller using the “Configurator” utility via the USB port.
2. At the installation site, prepare by marking and drilling the necessary holes.
3. If required, run the cable from the power supply unit.
4. Connect the cable from the actuating device (lock).
5. Install the external readers and connect their cables.
6. Run the cables from the sensors/buttons.
7. Connect the Ethernet cable.
8. Route the installation cables within the wall.
9. Mount and secure the controller housing.
10. Connect the wiring of the power supply, lock, reader, and controller inputs with cables as specified in the following sections.
11. Connect the Ethernet cable.
12. Close the cover and secure it with a screw.
13. Register the controller in the ACS (according to the ACS instructions).
14. Using the ACS, perform a full load (configure inputs, outputs, schedules, identifiers, etc.) of the controller.
15. The device is now ready for operation.

Connecting the Readers

The controller has two Wiegand interface ports for connecting readers. Readers with a Wiegand interface can work together with the controller.



Wire color correspondence:

- White – Data 1
- Green – Data 0
- Blue – Buzzer activation
- Brown – Red indicator activation
- Orange – Green indicator activation
- Black – GND
- Red – +12V

> When using readers from different manufacturers, the wire colors may differ. Refer to the reader's user manual for the correct color correspondence.

The current consumption of each external reader connected to the "+12V" terminal must not exceed 150 mA. When connecting long-range readers with current consumption above 150 mA,

power must be supplied from a separate source.

Connecting the Cables (Inputs)

The controller has eight inputs for connecting cables with current monitoring. The function of each input is set during the controller's programming. The following functions are possible for the inputs:

- Passage sensor (door contact)
- Exit request button
- Passage sensor (door contact) + exit request button
- Free Passage (A, B, A+B)
- Lockout (A, B, A+B)
- Monitoring the sensor status (alarm sensor)

Below is a description of connecting various input types. After resetting the controller to factory settings, all cables have no assigned function and are not monitored. All cables function as either normally closed or normally open. The use of load resistors is mandatory.

> The normal resistance of the cable should be between 1.4 kΩ and 3 kΩ, a short circuit is less than 1.4 kΩ, and an open circuit is more than 3 kΩ.

Access Request Button

The access request button is used when door passage is controlled from only one side. The door opens when the access request button is pressed and released.

Additionally, the access request button can be used as a remote door opening button (for example, to open the door manually by a receptionist or security guard).

Example: Connecting normally open exit request buttons to inputs Z1 and Z2. In programming, assign:

- Z1 – exit request button for access point A
- Z2 – exit request button for access point B

> Using a door release button on an electric strike or an exit button on a turnstile panel may trigger a DOOR FORCE event.

> For proper operation during programming, the connected cables must be assigned as exit request cables.

Passage Sensor (Door Contact)

A door contact sensor allows the controller to determine the state of the door (open/closed) or the position of a turnstile rotor. In the absence of a door contact, the controller cannot detect unauthorized access or when the door remains open for too long (e.g., when multiple people pass through one turnstile).

Example: Connecting normally closed door contacts to inputs Z3 and Z4. In programming, assign:

- Z3 – door contact for access point A
- Z4 – door contact for access point B

It is recommended that doors controlled by the ACS be equipped with door closers.

For proper operation, the connected door contacts must be assigned as such during programming.

Combined Cable – Exit Request Button and Passage Sensor (Door Contact)

The controller inputs can be configured to serve simultaneously as an exit request button and a door contact sensor. In this configuration, an open circuit indicates a door contact fault, while a short circuit indicates that the exit request button has been pressed.

Example: Connecting combined cables to inputs Z5 and Z6. In programming, assign:

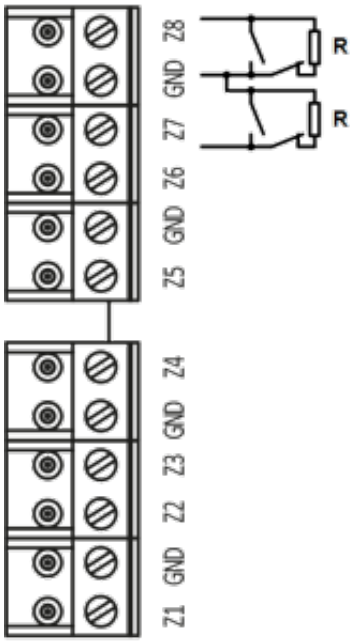
- Z5 – combined door contact and exit request button for access point A
- Z6 – combined door contact and exit request button for access point B

Any of the 8 inputs can be assigned as a combined input for both door contact and exit request functions.

Integration with Fire and Security Alarm Systems

Thanks to the inputs programmed as Free Passage and Lockout, the controller can be fully integrated into a fire and security alarm system.

For joint operation with a fire alarm system, configure one of the inputs as “Free Passage.” An external fire alarm cable or a fire alarm panel output can be connected to this input. In the event of a fire alarm, the cable designated as “Free Passage” is broken, and all doors controlled by the controller automatically unlock, allowing personnel to exit the danger zone.



In programming, assign:

- Z7 – “Lockout A+B”
- Z8 – “Free Passage A+B”

  “Lockout” can be assigned to access point A, access point B, or both (A+B).

  “Free Passage” can be assigned to access point A, access point B, or both (A+B).

  Zones with Lockout and Free Passage types operate on both short-circuit and open-circuit conditions.

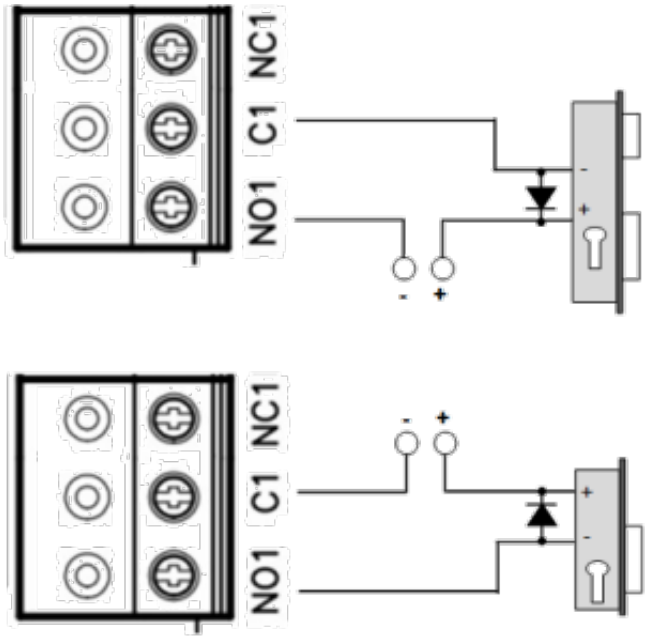
Connecting Actuating Devices

Electric Locks

The availability of normally closed and normally open relay contacts, along with the ability to program the activation time of the lock over a wide range (from 1 to 255 seconds), allows the controller to operate electric locks and strikes of almost any type.

A special case is when the time is set to 0. In this case, a pulse of 200 ms is applied to the relay.

Example: One actuating device opens by applying voltage, while another opens by removing voltage.



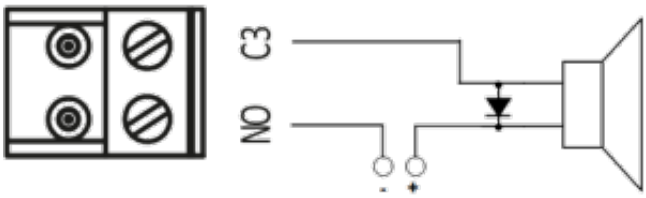
When using relay contacts to switch current through an inductive load (for example, when controlling an electromagnetic lock), high-amplitude electrical impulses may occur. To prevent damage to the relay contacts, the inductive load must be shunted with a diode connected in reverse polarity across the coil's power supply.

Note that inexpensive electromagnetic strikes do not allow prolonged voltage application. For such strikes, program the relay time so as not to overheat the strike coil.

> For proper lock operation, the connected relay outputs must be assigned as lock outputs during programming.

Sirens and Bells

Electric bells, being inductive loads, require the use of a protection diode when connected to a DC source (see the warning about inductive loads above).



> When connecting a siren, follow the siren's user manual. The siren's current draw must not exceed 1 A.

For non-standard actuating devices (such as magnetic starters, turnstiles, etc.), please consult your equipment supplier regarding proper connection methods.

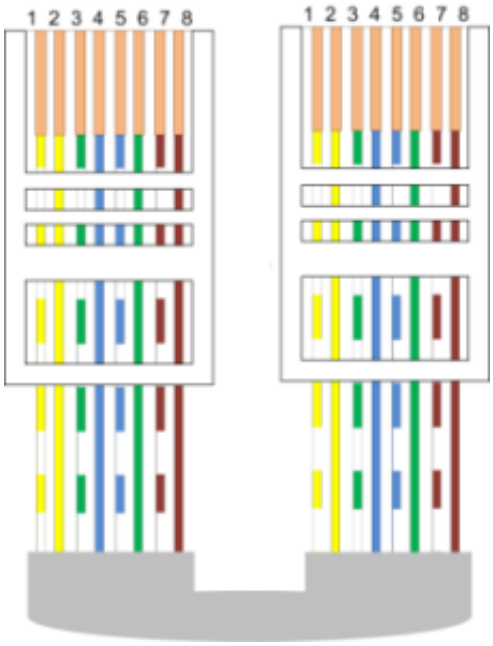
> For proper siren operation during programming, assign the connected relay output

as the siren (or alarm) output.

Connecting Ethernet

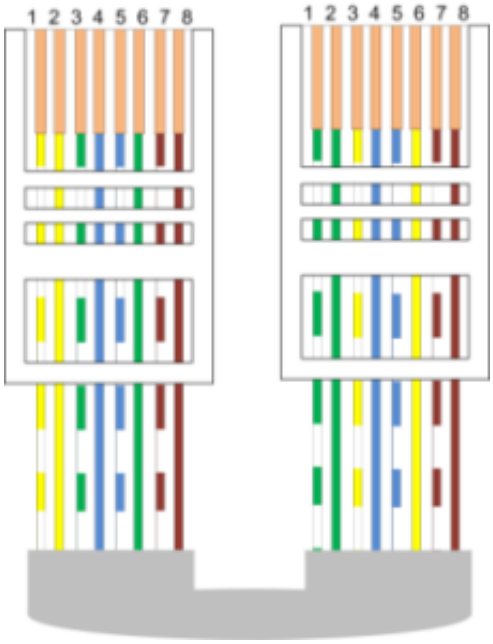
The Ethernet interface is used to network the system components (PC and controllers). The length of an Ethernet cable without additional equipment can be up to 100 meters, with data transmission speeds of up to 100 Mbps.

Direct Crimping – Connection to a Switch or Router:



1. White-yellow – white-yellow
2. Yellow – yellow
3. White-green – white-green
4. Blue – blue
5. White-blue – white-blue
6. Green – green
7. White-brown – white-brown
8. Brown – brown

Crossover Wiring – Connection to a Computer:



1. White-yellow – white-green
2. Yellow – green
3. White-green – white-yellow
4. Blue – blue
5. White-blue – white-blue
6. Green – yellow
7. White-brown – white-brown
8. Brown – brown

Factory Settings

Communicator

DHCP is enabled (the controller does not have a fixed IP address), and the ACS server addresses are not specified.

Inputs (Cables)

Z1 – Z8: Disabled

Outputs

Relays 1 – 4: Disabled

Readers

Wiegand 42bit

Warranty

The warranty period for U-PROX devices (excluding power sources) is 2 years from the date of sale. If the device does not operate properly, please first contact support@u-prox.systems; the issue may be resolved remotely.

Device supply, staff training, installation, commissioning, and warranty service for the U-PROX IP400 controller are performed by the manufacturer or by organizations authorized by the manufacturer.

If commissioning is performed by an organization that is not authorized by the manufacturer, the consumer forfeits warranty service.

Warranty repairs will not be performed if the device fails due to:

- Improper connection,
- Non-compliance with the operating instructions,
- Physical damage,
- Force majeure events.

Warranty and post-warranty service for U-PROX IP400 controllers is provided only by entities or organizations authorized by the manufacturer. The manufacturer reserves the right to make design changes that do not affect the main technical characteristics or reliability of the product.