



# **Gate-IP100**

**КОНТРОЛЛЕР**

**СКУД GATE-IP**

Паспорт и инструкция по  
эксплуатации

## Права и их защита

Всеми правами на данный документ обладает компания «Равелин Лтд». Не допускается копирование, перепечатка и любой другой способ воспроизведения документа или его части без согласия

## Об этом документе

Настоящее руководство по эксплуатации описывает порядок установки, подключения и эксплуатации контроллера системы управления доступом Gate-IP100 (в дальнейшем контроллера). Перед монтажом контроллера тщательно изучите данную инструкцию. Характеристики и параметры контроллера описаны в разделе **Характеристики**. В разделе **Термины** дается объяснения встречающихся в данном документе терминов. Внешний вид контроллера, описание контактов и режимов работы приводится в разделе **Описание и работа**. Порядок монтажа, подключения внешних устройств и настройка контроллера описаны в разделе Порядок работы с устройством

**Внимание!** Перед монтажом и подключением контроллера следует внимательно изучить настоящее руководство по эксплуатации. Выполнение монтажа, подключения контроллера допускается только лицами или организациями, имеющими соответствующие полномочия от производителя.

## Обучение и техническая поддержка

Курсы обучения, охватывающие вопросы установки и использования контроллера Gate-IP100, проводятся компанией «Равелин ЛТД».

Вся техническая информация доступна на сайте компании <http://skd-gate.ru>

Там же можно подписаться на рассылку новостей и задать вопрос группе технической поддержки.

## Содержание

Краткое описание контроллера .....	4
Назначение прибора .....	5
Характеристики .....	5
Термины .....	6
Описание и работа .....	9
Устройство контроллера .....	9
Назначение контактов контроллера .....	10
Перемычки .....	12
Светозвуковая индикация платы контроллера .....	12
Светозвуковая индикация считывателей контроллера .....	13
Работа контроллера .....	13
"Дежурный" режим .....	13
Режим "Тревога" .....	14
Режим "Свободный проход" .....	15
Режим "Блокировка" .....	15
Свойства идентификаторов (карточек) .....	16
Варианты использования и режимы работы выходов .....	17
Работа коммуникатора .....	17
Глобальный антипассбэк .....	22
Порядок работы с устройством .....	25
Порядок подключения .....	25
Рекомендации по монтажу .....	26
Подключение внешнего считывателя .....	26
Подключение шлейфов .....	27
Кнопка запроса прохода .....	28
Датчик прохода (Дверной контакт) .....	29
Комбинированный шлейф - кнопка запроса на выход и датчик прохода (дверной контакт) .....	30
Интеграция с охранно-пожарной сигнализацией .....	31
Исполнительные устройства .....	32
Электрозамки .....	32
Сирены и звонки .....	33
Коммуникация .....	33
Проводная компьютерная сеть (Ethernet) .....	34
Беспроводная компьютерная сеть (Wi-Fi) .....	35
Порядок программирования контроллера .....	36
Подключение контроллеров Gate-4000, Gate-8000 и Gate-P-4000 по шине RS-485 .....	37
Установка ID на шине данных для контроллеров Gate-4000, Gate-8000 и Gate-P-4000 .....	38
Сервисное обслуживание .....	39
Сброс в заводские установки .....	39
Переход в режим программирования .....	39
Замена микропрограммы устройства .....	39
Заводские настройки .....	39
Техническое обслуживание и ремонт .....	40
Хранение .....	40
Транспортирование .....	40
Маркировка .....	40
Комплектность поставки .....	41
Гарантийные обязательства .....	41

## Краткое описание контроллера

Контроллер Gate-IP100 – устройство, предназначенное для управления доступом в жилые и производственные помещения, учета времени прохода и событий.

Контроллер в штатном исполнении работает с двумя считывателями, подключаемыми к контроллеру по интерфейсу Wiegand.

Gate-IP100 обрабатывает информацию, поступающую со считывателя (считывателей), и с помощью четырех реле осуществляет коммутацию исполнительных устройств (например, замков, сирены и т.д.).

Наличие восьми дополнительных входов с различными вариантами их программирования позволяет круглосуточно контролировать восемь охранных зон (с контролем по току).

Контроллер может работать как автономно, так и в составе сети. Для объединения в сеть СКУД служат интерфейсы Ethernet (проводная компьютерная сеть) или Wi-Fi (беспроводная компьютерная сеть).

В контроллере предусмотрена функция программирования сетевых настроек и обновления его микропрограммы через стандартный порт USB (mini USB B).

Контроллер Gate-IP100 имеет развитые аппаратные возможности и интеллектуальные функции для управления двумя точками доступа с одним считывателем и кнопкой запроса прохода (две односторонних точки доступа) или одной точкой доступа с двумя считывателями (двусторонняя точка доступа). Большой объем энергонезависимой памяти позволяет использовать контроллер для организации СКУД предприятия с количеством сотрудников до 31 768 человек и до 1000 посетителей.

Тщательно продуманные технические и конструкторские решения, коммуникация по компьютерной сети Ethernet или беспроводной сети Wi-Fi, энергонезависимая память и часы, защита коммуникационных портов и портов считывателей от короткого замыкания, перенапряжения и переполюсовки – все это позволяет использовать контроллер для построения самых различных систем управления доступом – от системы для малого офиса до проходной большого предприятия.

Доступно только в платной версии



В составе СКУД «Gate-IP» полной (платной) версии контроллер Gate-IP100 может служить для подключения до 32х контроллеров Gate-4000, Gate-8000 и Gate-P-4000 работающих по шине RS-485. При этом контроллер Gate-IP100 в полной мере продолжает выполнять свои функции, как контроллер доступа.



Доступно только в платной версии

## Назначение прибора

Контроллер Gate-IP100 предназначен для работы в составе системы контроля и управления доступом Gate-IP. Контроллеры объединяются по компьютерной сети Ethernet или беспроводной сети Wi-Fi.

Контроллер позволяет организовать доступ в два разных помещения либо в одно помещение, но с контролем, как входа, так и выхода, а также систему сигнализации помещений, связанных с данными направлениями прохода. В случае одновременного контроля входа и выхода из помещения обеспечивается функция запрета повторного прохода ("Антипассбэк").

## Характеристики

- Ток потребления от источника 12 В (при отключенных нагрузках), не более 160 мА
- Амплитуда пульсаций источника питания постоянного тока, не более 500 мВ
- Возможность подключения внешних считывателей бесконтактных идентификаторов, работающих в протоколе Wiegand 26, 37, 42.
- Восемь входов для подключения шлейфов с контролем по току (оконечный резистор - 2 кОм)
- Два реле (контакты NO, NC, COM) 5 А @ 24 В
- Два реле (контакты NO, COM) 1 А @ 24 В
- Один порт USB для конфигурации сетевых настроек и обновления микропрограммы контроллера.
- Контроль вскрытия корпуса прибора
- Порт Ethernet (4 wire)
- Wi-Fi коммуникатор. Поддержка WEP/WPA/WPA2.
- Полная конфигурация выполняется с помощью ПО СКУД через компьютерную сеть
- Часы реального времени
- Функция "антипассбэк"
- Энергонезависимая память:

Идентификаторов	31768 (с версий микропрограммы 6.xx)
Событий	47290
Тайм-зон	250
Недельных расписаний	250
Праздников	250
Временных идентификаторов	1000

- Габаритные размеры корпуса прибора – 210x168x43 мм
- Климатическое исполнение – УХЛ 4.2 по ГОСТ 15150-69 в диапазоне температур окружающего воздуха от 0 до +55 °С
- Контроллер обеспечивает работоспособность при относительной влажности до 80 % без конденсации влаги

## Термины

### Идентификаторы

В системах управления доступом каждый пользователь имеет идентификатор с уникальным кодом. Идентификаторы могут иметь вид пластиковой карточки, брелока и др.

### Считыватель

Для чтения кодов идентификаторов предназначены считыватели, подключаемые к контроллеру СКУД.

Существует несколько распространенных типов идентификаторов и считывателей для них. При подключении к контроллеру важно, чтобы соответствовал тип интерфейса между считывателем и контроллером. Для подключения к контроллеру Gate-IP100 используется интерфейс Wiegand.

### PIN код

Если считыватели имеют встроенную клавиатуру, то в качестве идентификатора может выступать код, вводимый с клавиатуры. Обычно этот код называют PIN кодом, он может являться самостоятельным идентификатором или служить дополнением к карточке или брелоку, тогда после предъявления карточки считыватель "ожидает" ввода PIN кода.

### Точка доступа

Место, где непосредственно осуществляется контроль доступа (например, дверь, турникет, кабина прохода, оборудованные необходимыми средствами контроля).

### Направление прохода

Направление прохода – это логическая единица СКУД, управляющая проходом через точку доступа в одном направлении и включающая в себя считыватель, контроллер (или часть контроллера), исполнительный механизм. Таким образом, турникет с контролем прохода в обе стороны составляет два направления прохода, а дверь со считывателем только с одной стороны – одно направление прохода. Точка доступа, состоящая из двух направлений прохода, называется двусторонней, а точка доступа, состоящая из одного направления прохода – односторонней.

### Кнопка запроса на выход

В случае односторонней точки доступа для выхода из помещения используется кнопка, подключенная к контроллеру – кнопка запроса на выход. Открытие точки доступа любым другим способом: нажатием кнопки на электрозамке, с помощью ключа и т.д. – приводит к возникновению события ВЗЛОМ ТОЧКИ ДОСТУПА.

Кнопка запроса на выход может также использоваться для дистанционного открывания точки доступа.

### **Датчик прохода (Дверной контакт)**

При использовании датчиков прохода СКУД может контролировать состояние точек доступа: положение дверного полотна, стрелы шлагбаума, ротора турникета и т.д. и получать информацию о фактах прохода.

Для этих целей к входу контроллера подключается магнитный датчик закрытия двери, датчик положения ротора турникета, датчик положения стрелы шлагбаума. Вход, к которому подключаются эти датчики, называется вход для датчика прохода (или дверного контакта).

### **Антипассбэк (AntiPassBack)**

Для предотвращения ситуации, когда один пользователь, пройдя через точку доступа, управляемую СКУД, в одном направлении, передает свой идентификатор другому, в контроллере предусмотрена функция антипассбэк. Если эта функция включена, то контроллер отслеживает положение идентификатора – внутри/снаружи. При попытке повторного прохода в одном направлении контроллер СКУД отказывает в доступе и генерирует сообщение В ДОСТУПЕ ОТКАЗАНО, АНТИПАССБЭК.

Включить функцию антипассбэк можно, только если контроллер управляет двусторонней точкой доступа.

### **Глобальный антипассбэк (AntiPassBack)**

Отслеживание перемещения идентификатора через все подконтрольные точки доступа. При глобальном антипассбэке выполняется разделение объекта на зоны доступа, проход в которые возможен через несколько точек доступа. При попытках повторного прохода, несанкционированного использования идентификатора в данных зонах контроллеры СКУД отказывают в доступе и генерируют сообщение ГЛОБАЛЬНЫЙ АНТИПАССБЭК: В ДОСТУПЕ ОТКАЗАНО.

### **Групповой доступ**

Для доступа в помещения с повышенной степенью защищенности можно потребовать предъявления идентификаторов двух и более человек из различных групп, например, работника учреждения и работника вневедомственной охраны.

### **Интервал "время прохода"**

При нарушении дверного контакта, соответствующее направление прохода переходит в режим "Тревога" (см. Режим "Тревога" ниже). Тревога не включается, если контакт нарушен во время интервала "время прохода". Интервал начинается, когда контроллер разрешает проход пользователю. Длительность интервала задается при программировании. Также время прохода заканчивается при нарушении и последующем восстановлении дверного контакта.

### **Попытка подбора идентификатора**

В контроллере предусмотрена функция, включающая режим тревоги, если несколько раз подряд был предъявлен не зарегистрированный в системе идентификатор. Предъявление зарегистрированного идентификатора сбрасывает счетчик количества попыток подбора идентификатора. При программировании контроллера можно включить эту функцию и задать количество предъявлений.

### **Расписания**

При настройке прав доступа пользователей указываются интервалы времени и даты, по которым разрешается проход.

В контроллере, в зависимости от модификации, может храниться до 250 временных интервалов, из этих временных интервалов можно составить до 250 недельных расписаний.

Кроме того, существуют праздничные дни, встречающиеся раз в году, таких дат в контроллере может быть задано до 250.

### **Таймзоны (временные интервалы)**

Таймзона является составной частью расписания, и служит для организации временных интервалов и связывания их с правами доступа. Служат для проверки прав доступа и авторизации пользователя, для выполнения других функций, основанных на расписаниях.

### **Загрузка**

После программирования входов, выходов, прав доступа для владельцев идентификаторов и других параметров контроллера, необходимо выполнить загрузку контроллера. При загрузке данные о настройках попадают из компьютера в контроллер.



## Описание и работа

### Устройство контроллера

Внешний вид контроллера представлен на рис. 1.

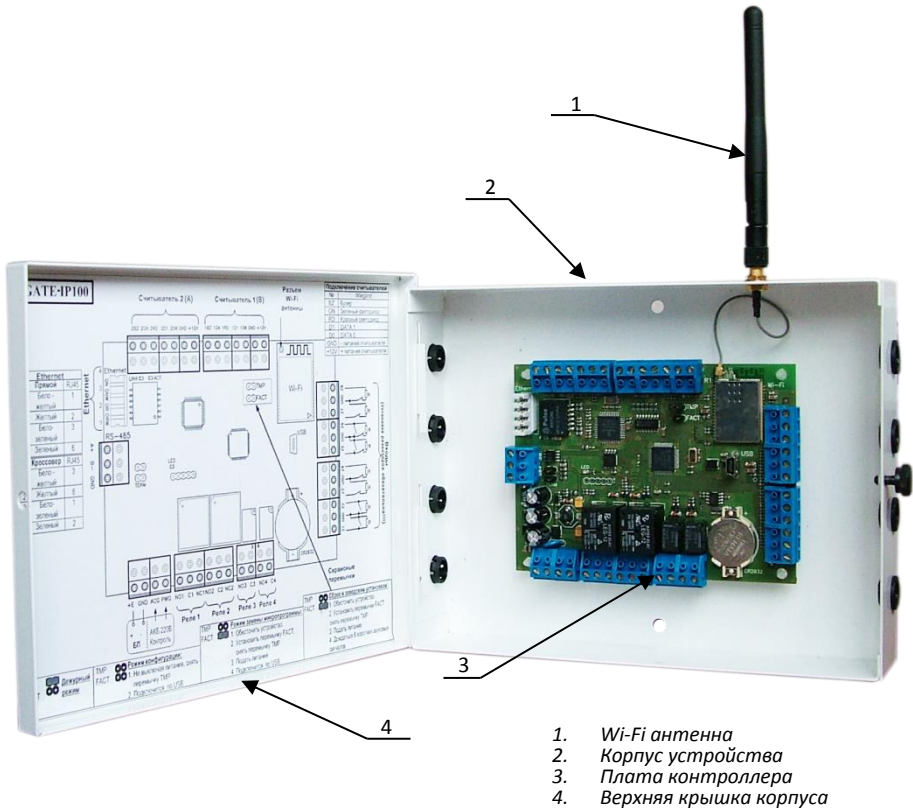


Рис. 1. Внешний вид Gate-IP100

Расположение на плате контроллера перемычек (джамперов) и съемных колодок с разъемами и их назначение показано на рис. 2.

## GATE-IP100

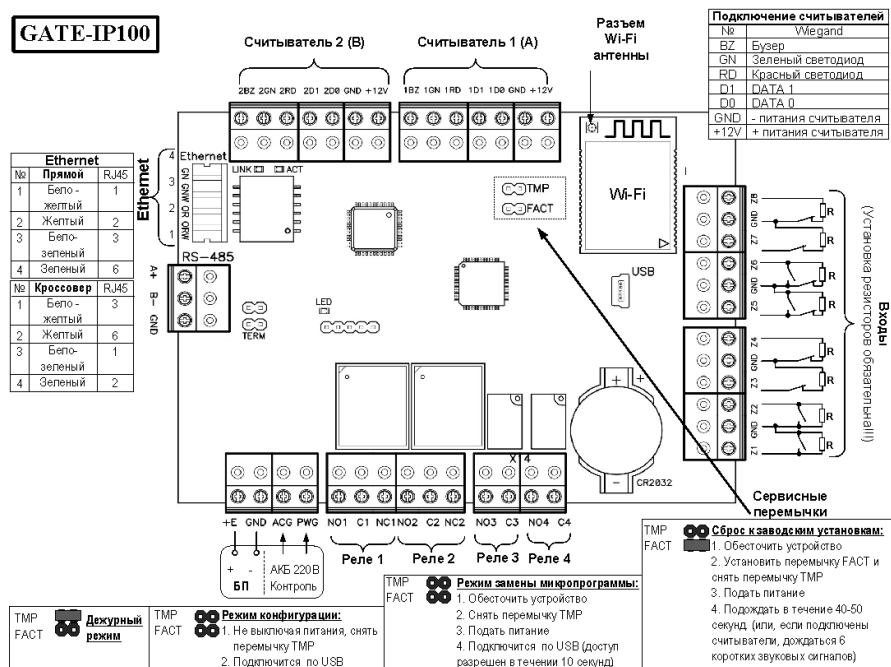


Рис. 2. Внешний вид платы контроллера

## Назначение контактов контроллера

Контакт	Название	Назначение
Z1	Z1	Контакты для подключения шлейфов
Z2	Z2	
Z3	Z3	
Z4	Z4	
Z5	Z5	
Z6	Z6	
Z7	Z7	
Z8	Z8	
GND	GND	Контакты реле 1
NC1	нормально замкнутый	
NO1	нормально разомкнутый	
C1	общий	

NC2	нормально замкнутый	Контакты реле 2
NO2	нормально разомкнутый	
C2	общий	
NO3	нормально разомкнутый	Контакты реле 3
C3	общий	
NO4	нормально разомкнутый	Контакты реле 4
C4	общий	
1BZ	зуммер	Подключение выносного считывателя 1 (Направление прохода A)
1GN	зеленый светодиод	
1RD	красный светодиод	
1D1	Data 1	
1D0	Data 0	
+12 V	Питание	
GND	GND	
2BZ	зуммер	Подключение выносного считывателя 2 (Направление прохода B)
2GN	зеленый светодиод	
2RD	красный светодиод	
2D1	Data 1	
2D0	Data 0	
+12 V	Питание	
GND	GND	
A+	RS-485 A+	Порт RS485, для подключения шины данных с контроллерами Gate-4000, Gate-8000, Gate-P-4000
B-	RS-485 B-	
GND	RS-485 GND	
E+		Подключение внешнего источника питания
GND		
ACG	Аккумулятор в норме	Сигналы от источника питания
PWG	Сеть 220В в норме	
<b>Разъем USB</b>		
USB Mini B	USB разъем	Используется для начальной конфигурации сетевых настроек и обновления микропрограммы
<b>Разъем Ethernet</b>		

1	<b>TX+</b>	Подключение Ethernet кабеля. Клеммы отсчитываются от клеммной колодки RS-485
2	<b>TX-</b>	
3	<b>RX+</b>	
4	<b>RX-</b>	
<b>Разъем Wi-Fi антенны</b>		
Wi-Fi	<b>ANT</b>	Используется для подключения антенны Wi-Fi

### Перемычки

#### Сервисные

- TMP – тампер (датчик вскрытия корпуса)
- FACT - сброс в заводские установки

#### Светозвуковая индикация платы контроллера

Желтый светодиод - LED:

- **дежурный режим (периодическое мигание):**
  - **1 короткий импульс раз в секунду** – связь с сервером СКУД в норме;
  - **2 коротких импульса раз в секунду** – связь с сервером СКУД отсутствует
- **частое мигание** – происходит загрузка данных с сервера
- **режим загрузчика:**
  - **светодиод включен в течение 5 секунд** - детектирование снятой перемычки TMP, вход в режим загрузчика
  - **частое мигание** – ожидание в режиме загрузчика (одета перемычка FACT), также такая индикация устанавливается при неудачной попытке обновления микропрограммы
  - **6 коротких звуковых сигналов** - успешная загрузка микропрограммы
  - **2 коротких звуковых сигнала** – выход из режима загрузчика
- **6 коротких звуковых сигналов** (при снятой перемычке TMP и закороченной перемычке FACT) – произведен сброс в заводские установки

Светодиод **Link**:

- светится - Ethernet кабель исправен

Светодиод **Act.:**

- частое мигание – происходит обмен данными

### Светозвуковая индикация считывателей контроллера

Индикация режимов доступа выполняется с помощью считывателей контроллера. Для каждого контроллера может быть выполнена индивидуальная настройка индикации из программного обеспечения СКУД. Настройки представлены в виде таблицы с комбинациями звуковой и световой индикации.

Значения индикации по умолчанию:

<i>Режим</i>	<i>Индикация считывателей</i>
Дежурный режим	Без звука, мигание красным 1 раз в секунду
Контроль PIN-кода включен	Без звука, мигание красный-зеленый 1 раз в секунду
Свободный проход	Без звука, мигание зеленый-желтый 1 раз в секунду
Блокировка	Без звука, мигание красный-желтый 1 раз в секунду
Тревога	Без звука, красный непрерывно
Регистрация карточки	Без звука, мигание зеленый 1 раз в секунду
Инициализация	Без звука, без световой индикации
Загрузка	Без звука, красный непрерывно
Ожидание ввода PIN-кода	Без звука, мигание желтый 1 раз в секунду
Доступ разрешен	Без звука, зеленый непрерывно
Доступ запрещен	Звук непрерывно, красный непрерывно

### Работа контроллера

Контроллеры поставляются в незагруженном состоянии, в заводских настройках. В этом состоянии желтый светодиод на контроллере мигает 1 раз в секунду. Для работы контроллера в СКУД необходимо загрузить в него сетевые настройки с помощью программы "Конфигуратор".

**Внимание!** Настоятельно рекомендуем установить на все входы контроллера резисторы (из комплекта).

После загрузки настроек в контроллер, и при условии не нарушенных входов, контроллер переходит в режим **"Дежурный"**.

Сброс контроллера в незагруженное состояние производится только командой с компьютера, см. инструкцию по программированию.

Контроллер может управлять двумя независимыми направлениями прохода. Направление прохода может находиться в четырех режимах: **"Дежурный"**, режим **"Тревога"**, режим **"Блокировка"** и **"Свободный проход"**. Самый высокий приоритет у режима **"Свободный проход"**, так как этот режим включается в случае пожара, затем идут режимы **"Блокировка"**, **"Тревога"** и **"Дежурный"**.

### "Дежурный" режим

Дежурный режим – это основной режим работы контроллера. В этом режиме контроллер предоставляет или отказывает в доступе владельцам идентификаторов.

**Проход при предъявлении идентификатора**

Для прохода через точку доступа пользователь подносит бесконтактный идентификатор к считывателю. Если идентификатор зарегистрирован и в данное время проход разрешен, то точка доступа открывается (контроллер активирует исполнительный механизм).

**Проход при предъявлении идентификатора и PIN кода**

После предъявления зарегистрированного идентификатора контроллер проверяет, требуется ли ввод PIN кода и, если требуется, то включается ожидание ввода PIN кода. После ввода правильного PIN кода открывается точка прохода (активируется исполнительный механизм).

**Проход по кнопке запроса прохода (дистанционного открытия двери)**

Выход из помещения с односторонней точкой прохода или пропуск посетителей происходит с использованием кнопки запроса прохода. Нажатие и отпускание кнопки запроса прохода открывает точку прохода (активируется исполнительный механизм).

**Отказ в доступе при предъявлении идентификатора**

Владельцу идентификатора может быть отказано в доступе по следующим причинам:

- контроллер находится в незагруженном состоянии,
- карточка не зарегистрирована в контроллере,
- срок действия карточки истек,
- в данное время и/или день недели доступ запрещен,
- попытка повторного прохода при включенной функции "Антипассбэк",
- предъявлен идентификатор, зарегистрированный как утерянный или заблокированный,
- контроллер находится в режиме "Тревога",
- контроллер находится в режиме "Блокировка",
- срок начала действия временной карточки еще не наступил.

**Режим "Тревога"**

Направление прохода переходит в режим "**Тревога**" при несанкционированном проходе (взлом прохода), вскрытии корпуса контроллера, предъявлении идентификатора, записанного как утерянный, в случае если точка доступа открыта слишком долго (превышено время открытого состояния точки доступа) и, если включена соответствующая функция, в случае подбора идентификатора.

В режиме "**Тревога**" контроллер активирует выходы, назначенные как ТРЕВОГА и СИРЕНА. Тревожный выход остается активированным до выключения режима "**Тревога**", а для выхода, назначенного как СИРЕНА, программируется время звучания сирены.

Если направление прохода находится в режиме "**Тревога**", то проход через него заблокирован. Точка доступа может быть открыта нажатием кнопки запроса на выход.

Выключить режим "**Тревога**" можно предъявлением идентификатора, имеющего признак "**Снятие тревоги**" или по команде с компьютера.

#### Режим "**Свободный проход**"

При эксплуатации СКУД бывают ситуации, когда необходимо открыть точки доступа для свободного прохода людей, например в случае пожара, землетрясения или другой экстремальной ситуации. Для этого случая в контроллере предусмотрен режим "**Свободный проход**".

Направление прохода переходит в режим "**Свободный проход**" по команде оператора с компьютера или нарушением шлейфа, назначенного как СВОБОДНЫЙ ПРОХОД. Направление прохода остается в режиме "**Свободный проход**" до тех пор, пока нарушен шлейф СВОБОДНЫЙ ПРОХОД (если шлейф нарушен, отменить состояние СВОБОДНЫЙ ПРОХОД по команде оператора нельзя).

Контроллер позволяет настроить шлейф на функцию СВОБОДНЫЙ ПРОХОД для направления прохода А, В или для двух направлений вместе (А+В).

В течение всего времени, пока направление прохода находится в режиме "**Свободный проход**", замок удерживается в открытом состоянии, контроллер регистрирует предъявление идентификаторов, ввод кодов и сохраняет по ним в журнал событие «Доступ предоставлен», независимо от состояния антипассбэка, расписания и т.д. Это используется для контроля наличия персонала в помещениях в случае экстремальной ситуации.

Для обеспечения режима свободного прохода при использовании запирающих устройств с механическим перевзводом обязательно нужно контролировать состояние точки доступа. Запирающие устройства с механическим перевзводом отпираются импульсом тока и остаются в отпертом состоянии, пока точка доступа не будет открыта, в момент закрытия точки доступа запирающее устройство переходит в закрытое состояние. Контроллер в режиме "**Свободный проход**" проверяет состояние дверного контакта и после каждого закрытия точки доступа опять подает отпирающий импульс на замок.

При работе контроллера без дверного контакта (геркона) использование типа выхода «импульсный» для отпираания замка крайне не рекомендовано. Режим "**Свободный проход**" в данном случае не будет работать корректно – отпереть двери без поднесения идентификатора невозможно.

#### Режим "**Блокировка**"

При возникновении ситуации, требующей заблокировать точки доступа для всех пользователей системы, в контроллере включается режим "**Блокировка**". Если направление прохода находится в режиме "**Блокировка**", то проход через него разрешается только владельцам идентификаторов с признаком "**Служба безопасности**". Точка доступа не может быть открыта нажатием кнопки запроса на выход.

Направление прохода переходит в режим "Блокировка" по команде оператора с компьютера или нарушением шлейфа, назначенного как БЛОКИРОВКА. Направление прохода остается в режиме "Блокировка" до тех пор, пока нарушен шлейф БЛОКИРОВКА или пока не поступит команда с компьютера.

Контроллер позволяет настроить шлейф на функцию БЛОКИРОВКА для направления прохода А, В или для двух направлений вместе (А+В).

### **Свойства идентификаторов (карточек)**

#### ***Код (электронный код карточки)***

Каждая карточка имеет свой уникальный код, который задается во время ее изготовления. Состоит из 10 шестнадцатеричных цифр.

#### ***PIN-код***

Дополнительный код, назначенный карточке. Должен состоять не более чем из шести десятичных цифр. Может использоваться совместно со считывателями, которые имеют встроенную клавиатуру.

После поднесения карточки к считывателю, на встроенной клавиатуре считывателя необходимо ввести PIN-код и нажать кнопку «#». Если введен верный PIN-код, то контроллер отпрет точку доступа и предоставит доступ. В противном случае контроллер выдаст предупреждающий сигнал, в журнале будет зарегистрировано событие «Неверный PIN-код», а точка доступа останется запертой.

#### ***Срок действия***

Дата истечения срока действия карточки.

#### ***Снятие тревоги***

При поднесении такой карточки к считывателю точки доступа, находящейся в тревожном состоянии, контроллер регистрирует событие «Завершение состояния ТРЕВОГА» и переводит точку доступа в дежурное состояние. Если же к считывателю поднести карточку, не имеющую права снятия тревоги, то точка доступа останется в том же состоянии, а в журнале регистрируется событие «Проход запрещен. Состояние ТРЕВОГА».

#### ***Служба безопасности***

Право прохода через заблокированные точки доступа.

Если точка доступа находится в состоянии «Блокировка», то поднесение обычной карточки приводит к регистрации события «Проход запрещен. Состояние БЛОКИРОВКА». При поднесении карточки с атрибутом «Служба безопасности», контроллер предоставит доступ и регистрирует событие «Проход разрешен. Состояние БЛОКИРОВКА».

#### ***AntiPassBack отключен***

Право прохода без учета режима AntiPassBack. Доступ такой карточке будет предоставлен независимо от направления предыдущего прохода, но с учетом назначенного расписания и других признаков, назначенных карточке.



## VIP

Право прохода всегда и везде, кроме случая, когда точка доступа находится в состоянии блокировки.

Карточке с этим признаком может быть назначено любое расписание, на нее не распространяется антипассбэк и ограничение срока действия. Она может иметь пинкод.

Если точка доступа находится в состоянии «Блокировка», то идентификатору с этим признаком контроллер не предоставляет доступ.

## Варианты использования и режимы работы выходов

Все выходы контроллера могут быть в произвольном порядке запрограммированы на несколько вариантов использования: **замок, сирена, тревога, программируемый выход**. Кроме того для каждого выхода программируется режим работы: **старт-стопный** (выход остается активированным пока присутствует соответствующая команда, например в течение всего времени пока контроллер находится в режиме “Тревога”), **импульсный** (выход активируется на запрограммированное время), **триггерный** (по первому событию выход активируется по следующему выключается и т.д.), **непрерывный**.

## Работа коммуникатора

Контроллер Gate-IP100 работает в автоматическом режиме. После загрузки данных с сервера выполняется отработка правил доступа для предъявляемых карточек и отправляет события об этом на сервер.

Коммуникатор контроллера работает в режиме **нотификации**, то есть при наличии события (проход, нарушение зоны) инициируется передача данных на сервер СКУД.

Контроллер Gate-IP100 может быть подключен к компьютерной сети либо с помощью проводного соединения (Ethernet), либо посредством беспроводной сети. При этом обеспечивается как работа внутри **локальной** сети предприятия (см. рис 3), так и **через сеть Интернет** (см. рис. 4), что позволяет строить распределенные системы доступа любого масштаба.

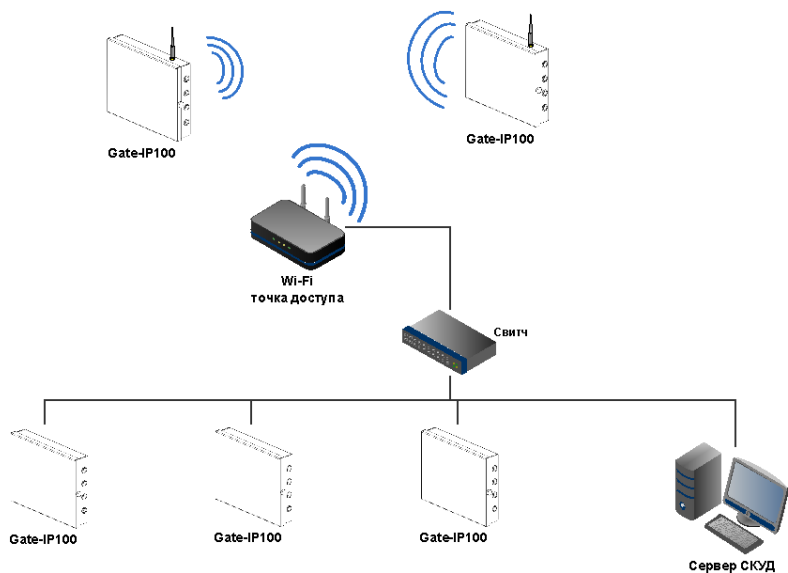


Рис 3. Пример локальной сети смешанного типа (Ethernet и Wi-Fi)

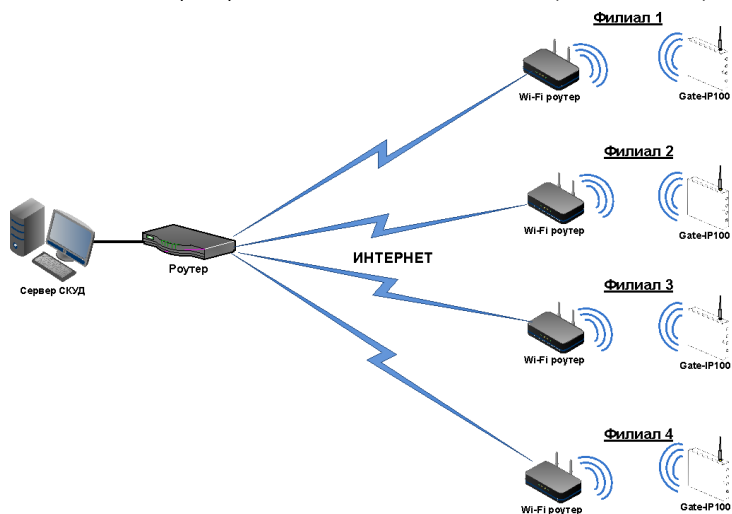


Рис 4. Пример распределенной сети

При построении общей сети центрального офиса и филиалов для дополнительной защиты рекомендуется использовать VPN технологии, а для обеспечения резервирования каналов связи - роутеры с двумя разнородными каналами доступа в Интернет.

Для резервирования беспроводного канала связи поддерживается работа с несколькими Wi-Fi точками доступа (основная и резервная) - см. рис.5.

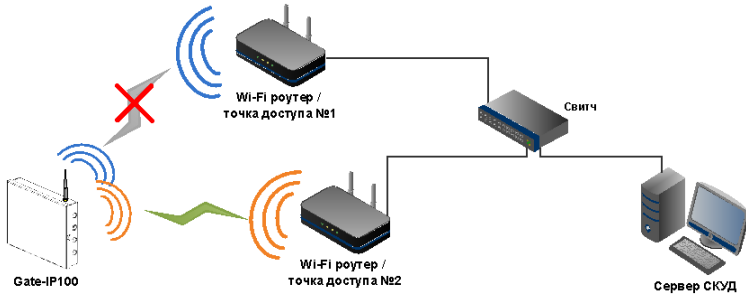


Рис 5. Работа с несколькими Wi-Fi точками доступа

#### **Алгоритм работы внутри локальной сети**

1. После включения контроллера, выполняется проверка, включен ли режим DHCP (IP адрес прибора 0.0.0.0), или прибор получил статический IP адрес;
2. Если включен режим DHCP, будет запущена процедура динамического назначения IP адреса;
3. Периодическое обновление статуса IP адреса (продление зарезервированного IP, если включен режим DHCP);
4. Определение доступности сервера СКУД и контроллера Gate-IC-Antipassback A (по IP или DNS имени);
5. Периодическая отправка тестовых сигналов;
6. Отправка событий доступа;
7. Ожидание команд;

#### **Алгоритм работы по Wi-Fi (с несколькими точками доступа)**

1. Определение доступности Wi-Fi сетей;
2. Подключение к заданному SSID №1;
3. После включения контроллера, выполняется проверка, включен ли режим DHCP (IP адрес прибора 0.0.0.0), или прибор получил статический IP адрес;
4. Если включен режим DHCP, будет запущена процедура динамического назначения IP адреса;
5. Периодическое обновление статуса IP адреса (продление зарезервированного IP, если включен режим DHCP);
6. Определение доступности сервера СКУД и контроллера Gate-IC-Antipassback A (по IP или DNS имени);
7. Периодическая отправка тестовых сигналов;
8. Отправка событий доступа;
9. Ожидание команд;
10. При сбое – переход к следующему заданному SSID.

**Алгоритм работы через сеть Интернет (локальная проводная сеть)**

1. После включения контроллера, выполняется проверка, включен ли режим DHCP (IP адрес прибора 0.0.0.0), или прибор получил статический IP адрес;
2. Если включен режим DHCP, будет запущена процедура динамического назначения IP адреса;
3. Периодическое обновление статуса IP адреса (продление зарезервированного IP, если включен режим DHCP);
4. Определение возможности выхода в Интернет (доступность IP адресов маршрутизаторов);
5. Определение доступности сервера СКУД и контроллера Gate-IC-Antipassback A (по IP или DNS имени);;
6. Периодическая отправка тестовых сигналов;
7. Отправка событий доступа;
8. Ожидание команд;
9. При сбое – переход ко второму заданному IP адресу маршрутизатора.

**Алгоритм работы через сеть Интернет (локальная сеть Wi-Fi)**

1. Определение доступности Wi-Fi сетей;
2. Подключение к заданному SSID №1;
3. После включения контроллера, выполняется проверка, включен ли режим DHCP (IP адрес прибора 0.0.0.0), или прибор получил статический IP адрес;
4. Если включен режим DHCP, будет запущена процедура динамического назначения IP адреса;
5. Периодическое обновление статуса IP адреса (продление зарезервированного IP, если включен режим DHCP);
6. Определение возможности выхода в Интернет (доступность заданных IP адресов маршрутизаторов);
7. Определение доступности сервера СКУД и контроллера Gate-IC-Antipassback A (по IP или DNS имени);
8. Периодическая отправка тестовых сигналов;
9. Отправка событий доступа;
10. Ожидание команд;
11. При сбое – переход ко второму заданному IP адресу маршрутизатора;
12. При повторном сбое – переход к следующему заданному SSID.

**Автоконфигурация контроллеров в одноранговой сети**

Использование сетевой существующей инфраструктуры, стандартных сетевых протоколов (например, DHCP) позволили реализовать принцип "подключил и работаешь". Режим автоконфигурации адреса сервера в устройствах значительно облегчает развертывание системы контроля доступа (см. рис 6).

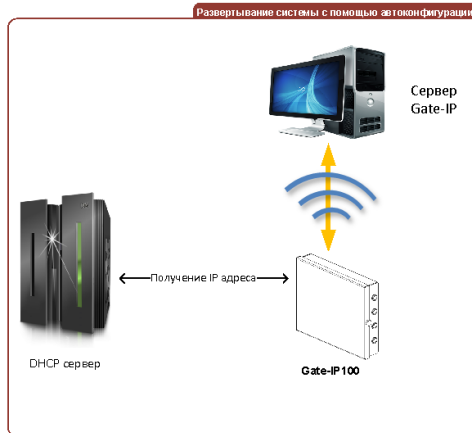


Рис.6. Автоконфигурация устройства

### Автоконфигурация адресов сервера

1. После включения контроллера, выполняется проверка, включен ли режим DHCP (IP адрес прибора 0.0.0.0), или прибор получил статический IP адрес;
2. Если включен режим DHCP, будет запущена процедура динамического назначения IP адреса;
3. Если не задан адрес сервера СКУД (IP или DNS имя), включается режим автоконфигурации контроллера:
  - a. Прибор выполняет рассылку пакетов данных, оповещающих сервер СКУД о себе как о новом устройстве в локальной сети.

Хотя данная рассылка широковещательная, но она ограничена одноранговой локальной сетью, и активным сетевым оборудованием. Поэтому для сетей со сложной топологией IP адреса сервера СКУД задаются вручную.

- b. При получении пакета данных от нового прибора оператору системы будет выдано оповещение. Далее оператор должен добавить прибор в базу данных (БД).
- c. После добавления устройства в БД прибор получает пакет с ответом от сервера СКУД. Инициализируется запись адреса сервера в настройки контроллера и прекращается широковещательная рассылка.
- d. После настройки параметров контроллера в БД оператор должен выполнить загрузку устройства. Прибор будет связан с данной СКУД, что исключит возможность перехвата управления.

Чтобы отменить привязку контроллера, его следует сбросить к заводским настройкам.

- e. В случае смены адреса сервера, устройство повторно выполнит автоконфигурацию, но обмен данными будет возможен только со СКУД, к которой был привязан прибор.

## Глобальный антипассбэк

Контроллер Gate-IP100 может работать в составе системы глобального антипассбэка. В таком случае главный контроллер серии Gate-IC-Antipassback отслеживает местоположение персоны по факту её прохода через точки доступа, получая данные от контроллеров серии Gate-IP100 и Gate-IP200.

Основной работы глобального антипассбэка является зонный антипассбэк. Помещение объекта разделено на комнаты – зоны доступа. При таком делении вход в другую зону - выход из предыдущей, и проход в зону возможен через различные точек доступа. Контроллер антипассбэка отслеживает перемещение сотрудников из зоны в зону, получая данные от контроллеров доступа. При этом отслеживается местоположение персоны, у которой может быть несколько идентификаторов (см. рис. 7)

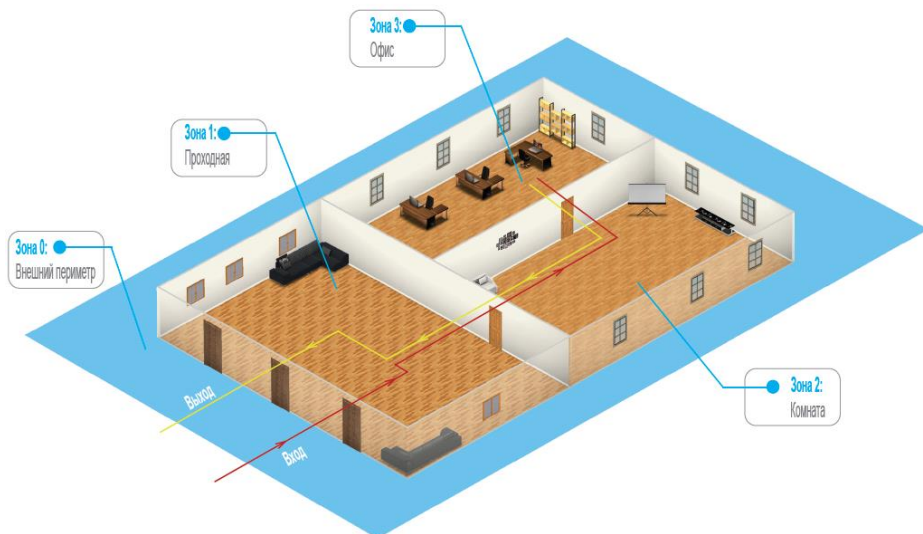


Рис 7. Распределение зон доступа

Изначально сотрудник (персона) имеет положение «Не определено» и только после первого поднесения идентификатора к считывателю его местоположение фиксируется контроллером Gate-IC-Antipassback.

Местоположение «Не определено» присваивается при регистрации нового сотрудника, либо после команды оператора системы «общий сброс местоположения».

С помощью системы глобального антипассбэка возможно пресечение повторного прохода, использования дубликатов карточек, проникновения (неожиданное появление внутри), передачи идентификатора другим лица и т.д. (см. Рис. 8):

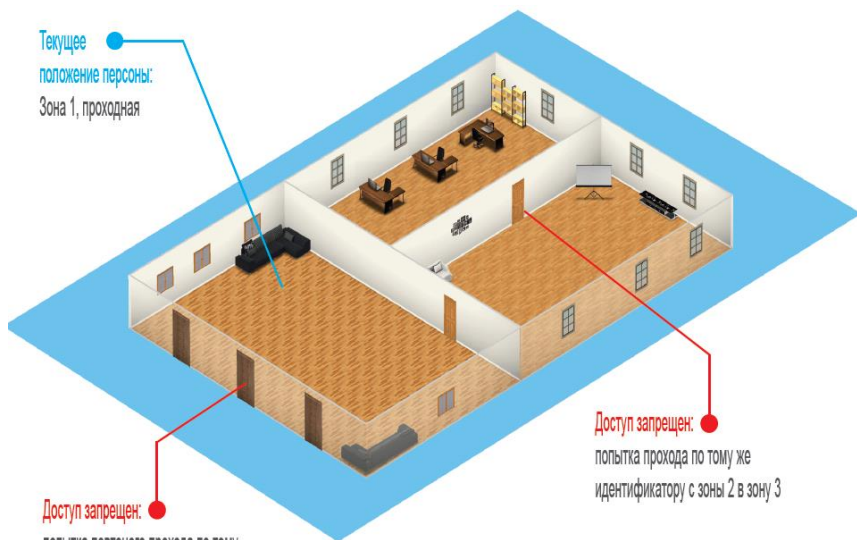


Рис 8. Отслеживание нарушений

В случае потери связи с контроллером СКУД, взлома двери, перехода точки доступа в свободный проход и т.д. контроллер антипассбэка объединяет зоны доступа в одну, считая, что персонал может находиться и там и там.

По восстановлению точки доступа или связи с контроллером – зоны разъединяются. Фактическое местоположение персонала в них определяется по последующему поднесению идентификатора к считывателю (см. Рис 9).

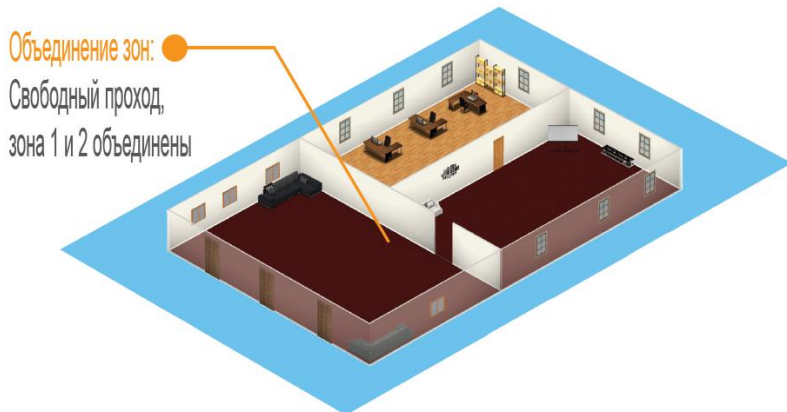


Рис 9. Объединение зон доступа

При потере связи с контроллером Gate-IC-Antipassback контроллеры доступа Gate-IP100 и Gate-IP200 могут быть настроены на два варианта поведения:

- Никого не пускать
- Пускать согласно данных о положении персоны для локального антипассбэка

**Требования к настройке контроллера Gate-IC-Antipassback**

- Контроллер должен иметь статический (фиксированный) IP адрес

**Требования к настройке контроллеров Gate-IP100 и Gate-IP200**

- В глобальном антипассбэке участвуют только контроллеры с двусторонними точками доступа (вход и выход по предъявлению идентификатора)
- Первым адресом сервера СКУД в настройках коммуникации прибора должен быть указан адрес компьютера с серверным ПО Gate-IP
- Вторым адресом сервера СКУД в настройках коммуникации прибора должен быть указан адрес контроллера Gate-IC-Antipassback
- В ПО Gate-IP для точки доступа должен быть включен режим антипассбэка "Общий"
- В ПО Gate-IP контроллеру доступа должен быть указан ведущий контроллер антипассбэка и реакция на потерю связи с ним.

Контроллеры Gate-IP100 и Gate-IP200 выполняют отправку извещений о событиях доступа по двум адресам одновременно. Первый адрес – сервер СКУД, для отображения и хранения событий в БД программы. Второй адрес – контроллер Gate-IC-Antipassback, отправляющий в ответ команду на запрет либо предоставление доступа.

После предъявления идентификатора задержка на предоставление либо отказ в доступе может составлять до 1 секунды в зависимости от топологии и пропускной способности компьютерной сети



## Порядок работы с устройством

Контроллер поставляется в металлическом корпусе без источника питания. Габаритные размеры прибора указаны на рис. 10.

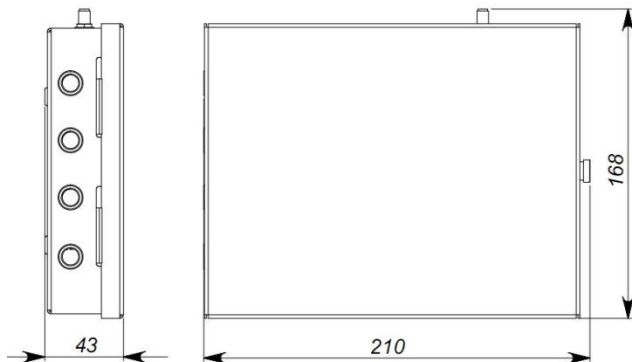


Рис 10. Габаритные размеры

### Порядок подключения

1. Перед установкой произведите начальную настройку (а именно задайте параметры сетевых настроек) контроллера с помощью утилиты "Конфигуратор" через USB порт
2. В месте установки контроллера выполните подготовку - разметьте и просверлите отверстия (см. **Рекомендации по монтажу**)
3. Выполните подводку кабеля от блока питания
4. Выполните подводку кабеля от исполнительных устройств (замка)
5. Установите выносные считыватели и выполните подводку их кабелей
6. Выполните подводку шлейфов от датчиков / кнопок
7. Выполните подводку кабеля Ethernet (по необходимости)
8. Выполните укладку монтажных кабелей в стене
9. Установите и закрепите корпус контроллера,
10. Выполните коммутацию проводов блока питания, замка, считывателя, входов контроллера со шлейфами в соответствии с разделами, приведенными ниже
11. Осуществите монтаж кабеля Ethernet в плиты разъема
12. Наденьте верхнюю крышку и зафиксируйте винтом
13. Подключите в ПО СКУД контроллер (в соответствии с инструкцией СКУД)
14. С помощью ПО СКУД выполните полную загрузку (настройки входов, выходов, расписаний, идентификаторов и т.д.) контроллера.
15. Устройство готово к работе

## Рекомендации по монтажу

Размещать контроллер следует в месте, доступном для обслуживания.

Для установки контроллера на стене (См. Рис. 7) необходимо выполнить следующие действия:

- откройте крышку корпуса, приложите корпус к предполагаемому месту крепления и выполните разметку отверстий;
- пропустите провода в отверстия в стенке корпуса;
- закрепите корпус контроллера;
- выполните подключение проводов.

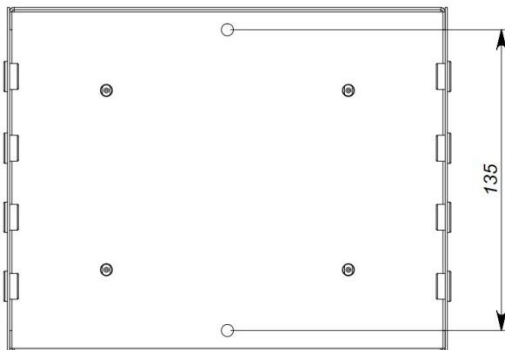


Рис 10. Разметка крепежных отверстий

## Подключение внешнего считывателя

Контроллер имеет два порта формата Wiegand для подключения считывателей. Совместно с контроллером могут работать различные считыватели. На рис. 11 показан пример подключения считывателей

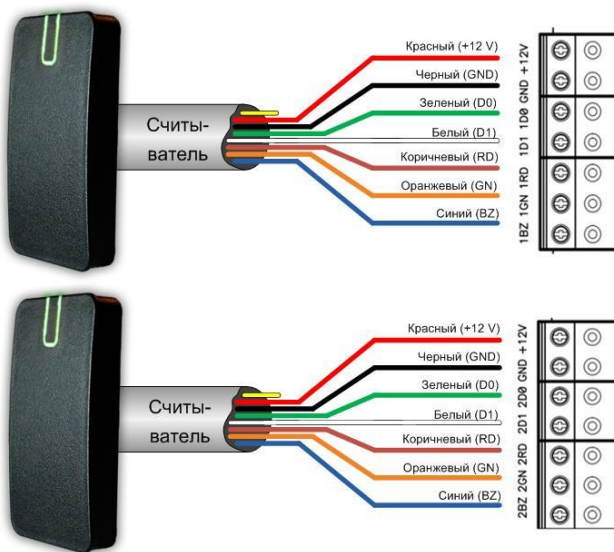


Рис.11. Подключение считывателей

Соответствие цвета проводов:

- белый - data 1
- зеленый - data 0
- синий - включение зуммера
- коричневый - включение красного индикатора
- оранжевый - включение зеленого индикатора
- черный - GND
- красный - +12 В

При использовании считывателей различных производителей цвета проводов могут отличаться. Соответствие цветов проводов смотрите в инструкции по эксплуатации на считыватель.

Ток потребления каждого внешнего считывателя подключаемого к клеммам "+12V" не должен превышать 100мА. При подключении к контроллеру считывателей большой дальности с током потребления более 100 мА, напряжение питания на них необходимо подавать от отдельного источника.

### Подключение шлейфов

Контроллер имеет восемь входов для подключения шлейфов с контролем по току. Назначение каждого из входов задается при программировании контроллера. Возможны следующие функции для входов:

- датчик прохода (дверной контакт)
- кнопка запроса на выход
- датчик прохода (дверной контакт) + кнопка запроса на выход
- свободный проход (А, В, А+В)
- блокировка (А, В, А+В)
- мониторинг состояния датчика (тревожный датчик)

Ниже описано подключение входов различных типов. После сброса контроллера к заводским установкам все шлейфы не имеют назначения и не контролируются. Все шлейфы работают как на замыкание, так и на размыкание. Использование нагрузочных резисторов обязательно.

Нормальное состояние шлейфа – от 1,4 кОм до 3кОм, К.З. шлейфа – менее 1,4 кОм, разрыв шлейфа – более 3 кОм.

### Кнопка запроса прохода

Кнопка запроса прохода применяется в случае, если проход через точку доступа контролируется только с одной стороны. Открытие точки доступа происходит при нажатии и отпуске кнопки запроса прохода.

Кроме того, кнопка запроса прохода может использоваться как кнопка дистанционного открытия точки доступа. Например, для открытия точки доступа вручную, секретарем или охранником.

На рис. 12 показан пример использования подключения нормально разомкнутых кнопок запроса на выход контактов Z1 и Z2.

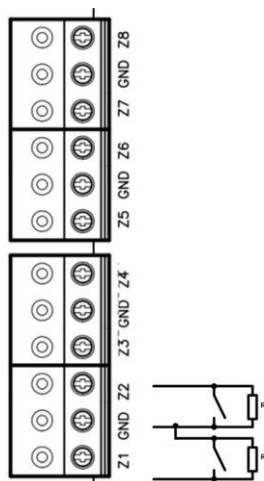


Рис.12. Подключение кнопки запроса прохода

При программировании назначено соответствие:

- Z1 - кнопка запроса прохода направления прохода А
- Z2 - кнопка запроса прохода направления прохода В

Использование для открытия точки доступа кнопки на электрозамке или кнопки пропуска на пульте турникета приводит к возникновению события ВЗЛОМ ТОЧКИ ДОСТУПА.

*Для правильной работы, при программировании необходимо назначить подключенные шлейфы как шлейфы кнопки запроса прохода.*

### Датчик прохода (Дверной контакт)

С помощью дверного контакта контроллер определяет состояние точки доступа (открыта/закрыта) или положение ротора турникета. В случае отсутствия дверного контакта контроллер не сможет обнаружить несанкционированный доступ или случай, когда точка доступа удерживается в открытом состоянии слишком долго (проход нескольких человек по одному пропуску).

На рис. 13 показан пример использования подключения дверных контактов (нормально закрытых) входов Z3 и Z3:

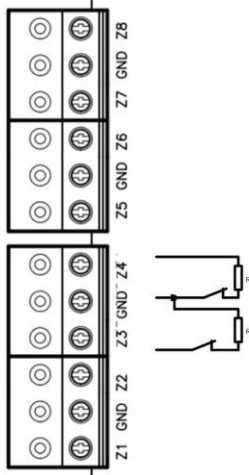


Рис.13. Подключение дверного контакта

При программировании назначено соответствие:

- Z3 - дверной контакт направления прохода А
- Z4 - дверной контакт направления прохода В

Точку доступа, управляемую системой контроля доступа, рекомендуется оборудовать доводчиком.

*Для правильной работы дверного контакта, при программировании необходимо назначить подключенные шлейфы как шлейфы дверного контакта.*

Контроллер может работать без назначения дверного контакта. В таком случае, после поднесения идентификатора и предоставления доступа, генерируется событие "Проход состоялся", контроллер подает отпирающий импульс на замок, и отсчитывается время прохода.

### Комбинированный шлейф - кнопка запроса на выход и датчик прохода (дверной контакт)

Входы контроллера можно настроить для одновременного использования для кнопки запроса на выход и для дверного контакта. При таком использовании разрыв шлейфа означает нарушение дверного контакта, а замыкание – нажатие кнопки запроса на выход.

На рис. 14 показан пример использования подключения комбинированных шлейфов к входам Z5 и Z6:

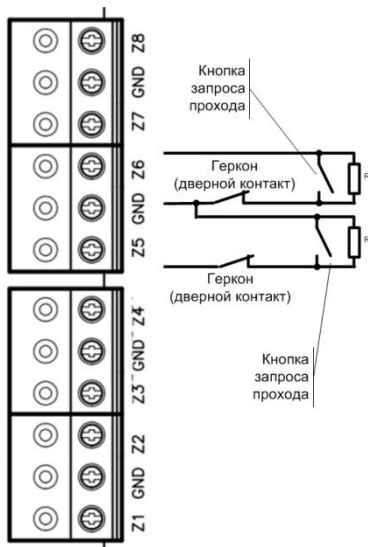


Рис.14. Подключение комбинированного шлейфа

При программировании назначено соответствие:

- Z5 - комбинированный дверной контакт и кнопка запроса прохода направления прохода А
- Z6 - комбинированный дверной контакт и кнопка запроса прохода направления прохода В

*Любой из 8 входов может быть назначен как комбинированный, для обслуживания дверного контакта и кнопки запроса на выход*

### Интеграция с охранно-пожарной сигнализацией

Благодаря наличию шлейфов, запрограммированных как СВОБОДНЫЙ ПРОХОД и БЛОКИРОВКА, контроллер полноценно интегрируется в систему охранно-пожарной сигнализации (см. Рис 15).

Для совместной работы с пожарной сигнализацией необходимо запрограммировать любой из шлейфов на тип "Свободный проход". К этому шлейфу может быть подключен непосредственно пожарный шлейф или выход пожарного ППК. При включении пожарной тревоги нарушается шлейф контроллера, назначенный как "Свободный проход", все точки доступа, управляемые контроллером, автоматически разблокируются и персонал может свободно покинуть зону пожара.

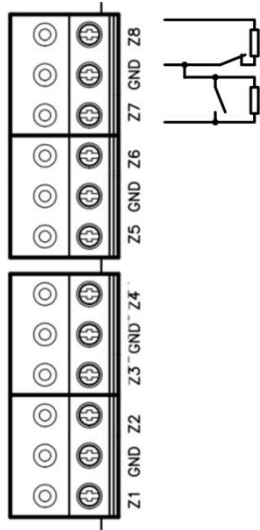


Рис.15. Подключение шлейфов блокировки и свободного прохода.

При программировании назначено соответствие:

- Z7 - "Блокировка А+В"
- Z8 - "Свободный проход А+В"

*"Блокировку" можно назначить на направления прохода А, В и А+В*

*"Свободный проход" можно назначить на направления прохода А, В и А+В*

Для совместной работы с охранной сигнализацией необходимо запрограммировать любой из шлейфов на тип "Блокировка". К этому шлейфу может быть подключен непосредственно тревожный шлейф или выход охранного ППК. При сработке охранного датчика или включении охранной тревоги нарушается шлейф контроллера, назначенный как "Блокировка", и все точки доступа, управляемые контроллером, автоматически блокируются. При этом доступ в охраняемые помещения будет предоставляться только службе безопасности.

## Исполнительные устройства

Для управления исполнительными устройствами контроллер имеет четыре реле. С помощью выходов контроллер может управлять электрозамком или защелкой, управлять работой шлагбаума, турникета, или включать другое дополнительное оборудование.

Реле 1 и 2 имеют нормально замкнутые и нормально разомкнутые контакты. Контакты реле позволяют управлять исполнительными механизмами с током потребления до 1А при напряжении 24 В.

Не допускается применение диодов при подключении исполнительных механизмов к электросети переменного тока.

Выбросы или провалы напряжения питания при одновременном включении-выключении всех исполнительных устройств не должны приводить к сбоям в работе контроллера. В противном случае необходимо подключить для питания исполнительных устройств отдельный источник питания.

### Электрозамки

Наличие нормально закрытых и нормально открытых релейных контактов, а также возможность программирования времени срабатывания замка в широких пределах (от 1 до 255 секунд) позволяет контроллеру управлять электрозамками и защелками практически любого типа.

Особым случаем является время, равное 0. В этом случае на реле подается импульс длительностью 200 ms.

На рис. 16 показан пример подключения исполнительных устройств, первое открывается подачей напряжения, второе - снятием.

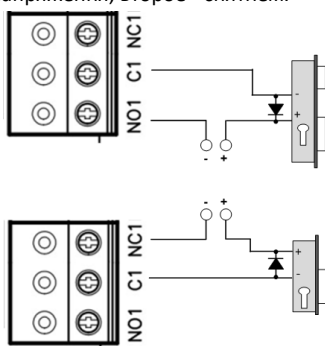


Рис.16. Подключение замков

При использовании контактов реле для включения/выключения тока через индуктивную нагрузку, например, при управлении электромагнитным замком, возникают электрические импульсы большой амплитуды. Для предотвращения выхода из строя контактов реле необходимо шунтировать индуктивную нагрузку диодом, включенным встречно напряжению питания катушки.



Следует учитывать, что недорогие электромагнитные защелки не допускают длительную подачу напряжения. Для таких защелок следует программировать время реле таким, чтобы не допустить перегрев катушки защелки.

*Для правильной работы замков, при программировании необходимо назначить подключенные релейные выходы как выходы замков.*

### Сирены и звонки

Электрозвонки (см. Рис. 17) являются для источника напряжения индуктивной нагрузкой, при подключении звонка к источнику постоянного тока необходимо использование защитного диода (смотри предупреждение об индуктивной нагрузке).

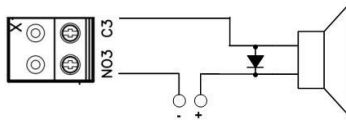


Рис.17. Подключение электровонков

При подключении сирены изучите инструкцию пользования сиреной. Ток потребления сирены не должен быть более 1 А.

При использовании нестандартных исполнительных устройств (магнитные пускатели, турникеты и т.д.) рекомендуется за консультацией по подключению обратиться к своему поставщику оборудования.

Для правильной работы сирены, при программировании необходимо назначить подключенный релейный выход как выход сирены (тревоги и т. д.).

### Коммуникация

Для связи с сервером СКУД контроллер Gate-IP100 может использовать проводную компьютерную сеть, либо беспроводную компьютерную сеть.

Настройка прибора возможна с помощью автоконфигурации или вручную с ПК с помощью ПО "Конфигуратор".

При соответствующей настройке обеспечивается:

- назначение статического или динамического (DHCP) IP адреса устройству;
- работа с IP или DNS (доменным именем компьютера) адресом сервера СКУД;
- Работа через сеть Интернет (обслуживание удаленных филиалов) с возможностью резервирования путей в Интернет через второй маршрутизатор (роутер);
- Работа с несколькими Wi-Fi точками доступа посредством резервирования (основная и резервная)

Контроллер работает в автоматическом режиме - после загрузки данных с сервера выполняет обработку правил доступа для предъявляемых карточек и отправляет события об этом на сервер.

Коммуникатор контроллера работает в режиме **нотификации**, то есть при наличии события (проход, нарушение зоны) инициируется передача данных на сервер СКУД. При работе в компьютерной сети контроллер обеспечивает защиту от несанкционированного вмешательства благодаря криптостойкости (шифрование пакета данных с использованием 256-битного ключа) и имитостойкости (контроль уникального серийного номера устройства), а также контролю канала связи посредством периодических тестовых сигналов от устройства.

### Проводная компьютерная сеть (Ethernet)

Интерфейс Ethernet используется для объединения компонентов системы (ПК и контроллеров) в сеть. Длина кабеля Ethernet без использования дополнительного оборудования может составлять до 100 метров

При коммутации используется стандартный кабель Ethernet, в котором задействованы 4 провода: TX+, TX-, RX+, RX-. Обеспечивается скорость передачи данных до 100Мбит/с. На рис. 18 показаны примеры подключения кабеля Ethernet.

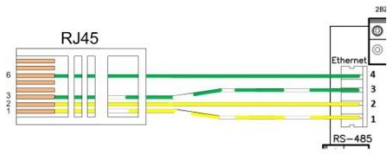
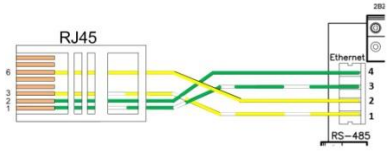
Клеммы Ethernet разъема контроллера	Цвет кабеля	Клеммы Разъема RJ-45	
<b>Прямое соединение (к свитчу или роутеру)</b>			
1	Бело-желтый	1	
2	Желтый	2	
3	Бело-зеленый	3	
4	Зеленый	6	
<b>Кроссовер(напрямую к сетевой карте компьютера).</b>			
1	Бело-желтый	3	
2	Желтый	6	
3	Бело-зеленый	1	
4	Зеленый	2	

Рис.18. Подключение кабеля Ethernet

Установка кабеля Ethernet в плиты разъема контроллера осуществляется с помощью специального инструмента - **LSA punch down tool** (например, KRONE LSA-PLUS)

При настройке Ethernet коммуникатора контроллера следует выполнить:

- Разрешение использования коммуникатора Ethernet

- Настройку сетевых параметров контроллера (при использовании DHCP – не задаются):
  - IP адрес
  - Маска подсети
  - IP адрес шлюза (роутера) интернет 1(необязательно в локальной сети)
  - IP адрес шлюза (роутера) в интернет 2 (необязательно)
  - IP адрес DNS сервера 1 (если используется передача данных на доменное имя)
  - IP адрес DNS сервера 2 (необязательно, если используется передача данных на доменное имя)
- Настройку коммуникации с сервером:
  - IP или DNS адрес сервера 1
  - IP или DNS адрес сервера 2 (адрес Gate-IC-Antipassback)
  - Порты доступа (порт чтения и порт записи)
  - Частота проверки канала связи (отправки тестового сигнала)

### Беспроводная компьютерная сеть (Wi-Fi)

Контроллер может работать в беспроводных компьютерных сетях стандартов IEEE 802.11b/g/n (частоте 2.4ГГц., шифрование WEP (Open), WPA, WPA2).

Для резервирования данного канала связи контроллер поддерживает работу с несколькими Wi-Fi точками доступа (основная и резервная).

При настройке Wi-Fi коммуникатора контроллера следует выполнить:

- Разрешение использования коммуникатора Wi-Fi
- Настройку параметров Wi-Fi (для каждой из используемых точек доступа):
  - Имя сети - SSID
  - Ключ доступа (пароль)
  - Режим шифрования
- Настройку сетевых параметров контроллера (при использовании DHCP – не задаются):
  - IP адрес
  - Маска подсети
  - IP адрес шлюза (роутера) интернет 1 (необязательно в локальной сети)
  - IP адрес шлюза (роутера) в интернет 2 (необязательно)
  - IP адрес DNS сервера 1 (если используется передача данных на доменное имя)
  - IP адрес DNS сервера 2 (необязательно, если используется передача данных на доменное имя)
- Настройку коммуникации с сервером:
  - IP или DNS адрес сервера 1
  - IP или DNS адрес сервера 2 (адрес Gate-IC-Antipassback)
  - Порты доступа (порт чтения и порт записи)
  - Частота проверки канала связи (отправки тестового сигнала)

## Порядок программирования контроллера

Программное обеспечение	Действия
	<ol style="list-style-type: none"> <li>1. Определение режима работы контроллера: автономный или в составе СКУД</li> <li>2. Определение интерфейсов связи - Wi-Fi, Ethernet</li> </ol>
<p>ПО "Конфигуратор"</p> <p>Через порт USB</p>	<ol style="list-style-type: none"> <li>3. Настройка начальных параметров, а именно сетевых настроек контроллера:               <ol style="list-style-type: none"> <li>a. Тип коммуникатора – Wi-Fi, Ethernet</li> <li>b. Wi-Fi ключ доступа к сети и тип шифрования (повторить, если несколько сетей)</li> <li>c. Настройки сервера: IP адрес или DNS имя сервера, порты доступа (порт чтения, порт записи)</li> </ol> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Пункт d при наличии DHCP (динамических адресов) в сети не нужно выполнять</p> </div> <li>d. Настройки устройства: IP адрес устройства в компьютерной сети, маска подсети, IP DNS сервера, шлюз в Интернет</li> </li></ol>
<p>ПО СКУД</p>	<ol style="list-style-type: none"> <li>4. Подключение и регистрация устройства в ПО СКУД (см. руководство по СКУД)</li> <li>5. Настройка устройства с помощью ПО СКУД               <ol style="list-style-type: none"> <li>a. Настройка точек доступа: односторонние точки доступа или двусторонняя точка доступа, режим работы антипассбэк, время ввода PIN кода (или отключен)</li> <li>b. Настройка направлений прохода: № считывателя, время прохода, признаки "Нет тревоги при взломе", "Нет тревоги, если открыто слишком долго"</li> <li>c. Настройка считывателей: тип считывателя 26 или 42 битный</li> <li>d. Настройка входов контроллера: тип реакции и направление прохода (например, датчик прохода, направление прохода А и В; свободный проход, направление прохода В).</li> <li>e. Настройка выходов контроллера: тип использования (замок, сирена и т.д.), режим работы, длительность импульса (если доступен в данном режиме), направление прохода, управляющая данным выходом.</li> </ol> </li> <li>6. Средствами СКУД создается список пользователей с набором идентификаторов и их дополнительных параметров, расписаний</li> </ol>

правил прохода через определенные направления прохода (см. руководство по СКУД)

- После формирования и загрузки конфигурации из ПО СКУД устройство готово к работе.

### Подключение контроллеров Gate-4000, Gate-8000 и Gate-P-4000 по шине RS-485

Интерфейс RS485 Gate-IP100 используется для объединения системы контроля доступа «Gate-IP» и контроллеров Gate-4000, Gate-8000 и Gate-P-4000 в сеть. Длина шины интерфейса без использования дополнительного оборудования может составлять до 1200 метров. Количество контроллеров в одном сегменте шины - до 32. При подключении устройств по шине RS485 следует на первом и последнем устройстве на шине включить оконечную нагрузку, установив переключки нагрузки.

Примеры подключения контроллеров Gate-4000, Gate-8000 и Gate-P-4000 к Gate-IP100 показаны на Рис. 19 и Рис. 20:

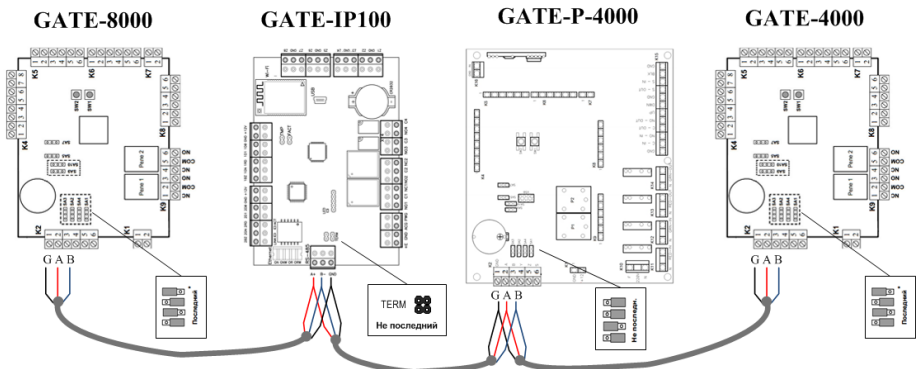


Рис.19. Контроллер Gate-IP100 центральный на шине данных

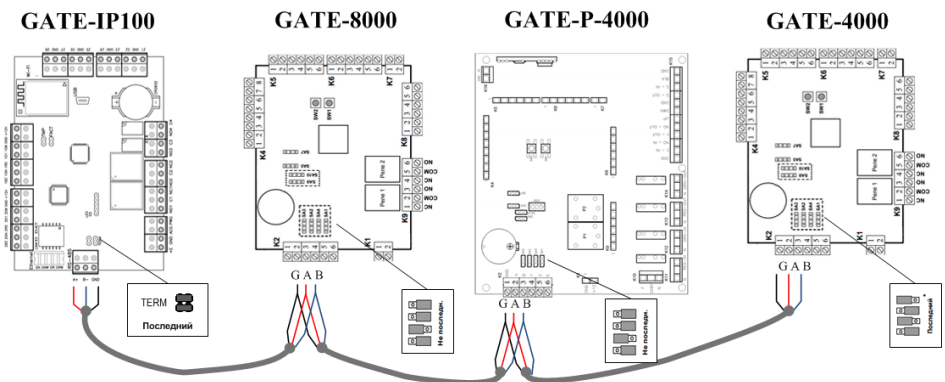


Рис.20. Контроллер Gate-IP100 последний (первый) на шине данных

### Установка ID на шине данных для контроллеров Gate-4000, Gate-8000 и Gate-P-4000

При миграции с ПО Gate-на ПО Gate-IP контроллеры Gate-4000, Gate-8000 и Gate-P-4000 могут быть подключены с теми же ID что и были ранее (если их ID от 1 до 32 включительно), в противном случае необходимо задать им новые уникальные ID (на одной шине RS485).

В заводских настройках все контроллеры Gate-4000, Gate-8000 и Gate-P-4000 имеют ID равный 0xFF (255), и изменить его можно специальной утилитой (программой Gate-Find), либо средствами контроллера Gate-IP100.

Для того чтобы упростить процедуру задания ID контроллерам Gate-4000, Gate-8000 и Gate-P-4000, находящимся в заводских настройках, в контроллере Gate-IP100 реализован специальный режим.

Процедура установки ID:

1. Монтируем контроллеры, монтируем шину данных, соединяя контроллеры последовательно, один за другим согласно инструкции.
2. Проверяем (прозваниваем) правильность подключения шины данных.
3. Обесточиваем все контроллеры Gate-4000, Gate-8000 и Gate-P-4000.
4. НЕ ОТКЛЮЧАЯ ПИТАНИЕ, устанавливаем перемычку FACT на контроллере Gate-IP100.

**Внимание!!! Если контроллер Gate-IP100 в процессе работы будет перезапущен, все его настройки будут сброшены к заводским. Не допускайте перезапуска по питанию!!!**

5. Включаем последний контроллер Gate-4000, Gate-8000 или Gate-P-4000 (с установленным режимом «последний в сети»), ждем 30 секунд – контроллер Gate-IP100 установит ему ID равный 1. *Выключать контроллер после назначения ID нет необходимости.*
6. Включаем последовательно остальные контроллеры Gate-4000, Gate-8000 и Gate-P-4000. Будут установлены ID 2, 3, 4, и т.д. *Выключать контроллеры после назначения ID нет необходимости.*
7. По окончании процедуры назначения ID НЕ ОТКЛЮЧАЯ ПИТАНИЕ, снимаем перемычку FACT на контроллере Gate-IP100.

## Сервисное обслуживание

### Сброс в заводские установки

Для возврата контроллера к заводским установкам следует выполнить следующие действия:

1. Обесточьте контроллер
2. Снимите перемычку TMP
3. Установите перемычку FACT
4. Подайте питание
5. Подождите 40-50 секунд (или, если подключены считыватели, дождитесь шести коротких сигналов, сигнализирующих об успешном сбросе контроллера)
6. Обесточьте контроллер
7. Снимите перемычку FACT, установите перемычку TMP

### Переход в режим программирования

Для перевода контроллера в режим программирования выполните следующие действия:

1. Не выключая питания, снимите перемычку TMP
2. Подключите к разъему USB кабель и выполните настройку прибора с помощью программного обеспечения "Конфигуратор"

### Замена микропрограммы устройства

1. Обесточьте контроллер
2. Снимите перемычку TMP, установите перемычку FACT
3. Подключите USB кабель сначала к компьютеру, а затем – к контроллеру
4. С помощью специального программного обеспечения выполните замену микропрограммы контроллера
5. После загрузки ПО в контроллер **ОБЯЗАТЕЛЬНО** подождите 15-20 секунд (или, если подключены считыватели, дождитесь шести коротких сигналов, сигнализирующих о корректной загрузке микропрограммы).

Внимание!!! Загрузка микропрограммы будет разрешена только в течение первых 10 секунд после запуска контроллера.

## Заводские настройки

### Коммуникатор

Режим – проводной Ethernet, DHCP включён (не установлен IP контроллера), адреса сервера СКУД не указаны

### Входы (шлейфы)

Z1 – Z8 – отключены

### Выходы

Реле 1-4 - отключены

### Считыватели

Wiegand 42bit

## Техническое обслуживание и ремонт

Гарантийное и послегарантийное обслуживание контроллеров Gate-IP100 выполняется лицами или организациями, получившими на это полномочия от производителя.

### Хранение

- Приборы должны храниться в условиях 2 ГОСТ 15150 при отсутствии в воздухе кислотных, щелочных и других активных примесей.
- Хранение приборов без тары не допускается.
- Хранение запакованных в индивидуальную или транспортную тару приборов на складах допускается при укладке в штабель без прокладок между ними. Количество рядов в штабеле — не больше шести.
- Срок хранения приборов — не более шести месяцев с момента изготовления.
- В складских помещениях должны быть обеспечены температура воздуха от 5 до 50 °С, относительная влажность до 80 %, отсутствие в воздухе кислотных и щелочных и других активных примесей.

### Транспортирование

- Упакованные приборы допускается транспортировать в условиях 5 ГОСТ 15150 в диапазоне температур от минус 50 до плюс 50 °С, при защите от прямого действия атмосферных осадков и механических повреждений.
- Упакованные в индивидуальную или транспортную тару приборы могут транспортироваться всеми видами закрытых транспортных средств в соответствии со следующими документами:
- "Правила перевозок грузов автомобильным транспортом" 2 изд., М., "Транспорт", 1983
- "Правила перевозки грузов", М., "Транспорт", 1983
- "Технические условия погрузки и крепления грузов", М., "Транспорт", 1990

### Маркировка

На приборе нанесена маркировка, содержащая:

- название, условное обозначение и вариант исполнения;
- порядковый номер;
- вид питания;
- номинальное напряжение сети электропитания;
- номинальную частоту сети электропитания;
- обозначение соединителей;
- обозначение клеммы заземления;
- "Знак соответствия" — для приборов, имеющих сертификат соответствия.



На индивидуальной таре наклеена этикетка, на которой обозначены:

- товарный знак производителя;
- название и условное обозначение прибора;
- масса прибора;
- дата изготовления.

На транспортной таре нанесена маркировка:

- товарный знак производителя;
- название и условное обозначение прибора;
- манипуляционные знаки 1, 3, 5, 11, 19 по ГОСТ 14192.

## Комплектность поставки

В комплект поставки входит:

- |  |          |
|--|----------|
| ● Контроллер   | - 1 шт.; |
| ● Резистор МЛТ-0,25 - 2кОм +/-2%<br>(или ВМХ 6 F 0,2 0,2 A20 0,6 WA 2 кОм ±2%) | - 8 шт.; |
| ● Диод 1N4001  | - 2 шт.; |
| ● Паспорт и инструкция по эксплуатации   | - 1 шт.; |
| ● Упаковка   | - 1 шт.  |

## Гарантийные обязательства

Производитель гарантирует соответствие изделия Контроллера Gate-IP100 требованиям безопасности и электромагнитной совместимости при соблюдении Покупателем правил транспортирования, хранения, монтажа и эксплуатации изделия. В течение гарантийного срока производится бесплатный ремонт изделия в мастерской Производителя или в сертифицированных сервисных центрах Производителя. Производитель оставляет за собой право отремонтировать неисправное изделие или заменить его аналогичным исправным. Срок ремонта определяется Производителем при сдаче изделия в ремонт.

Кроме гарантий, указанных выше, Производитель не предоставляет никаких других гарантий относительно совместимости данного изделия с программным обеспечением или с изделиями, произведёнными другими изготовителями, а также гарантий годности изделия для целей, не предусмотренных эксплуатационной документацией на данное изделие. Гарантией не предусматриваются претензии относительно технических параметров изделия, если они соответствуют указанным Производителем. Данное изделие относится к технически сложным товарам, поэтому Производитель не принимает обратно исправное изделие, если оно по каким-либо причинам не подошло Покупателю. Если в результате проведённой Производителем экспертизы рекламационного изделия дефекты не обнаружатся, и изделие будет признано исправным, то на Покупателя ложится обязанность оплаты расходов Производителя на экспертизу.

**Сроки гарантийных обязательств**

Гарантийный срок эксплуатации изделия составляет 12 месяцев с даты продажи, если иное не оговорено в договоре с Покупателем на поставку изделия.

**Ответственность по гарантии**

В максимальной степени, допустимой действующим законодательством, Производитель не несет ответственности ни за какие прямые или косвенные убытки Покупателя, включая убытки от потерь прибыли и информации, убытки от простоя, упущенную выгоду и другие убытки, связанные с использованием или невозможностью использования изделий и программного обеспечения, в том числе из-за возможных ошибок и сбоев в работе программного обеспечения.

**Условия предоставления гарантийных обязательств**

Гарантия действительна на территории Российской Федерации.

Гарантийные обязательства поставщика не смогут быть исполнены, если Клиент не предоставит при обращении к поставщику или уполномоченному сервисному центру неисправное оборудование, а так же гарантийный талон без каких-либо исправлений с наименованием модели оборудования, серийным номером, датой продажи и печатью изготовителя.

Гарантия не распространяется на изделия, имеющие механические повреждения корпуса, следы постороннего вмешательства или ремонта, а также имеющие повреждения и неисправности, вызванные действием непреодолимой силы (стихийных бедствий, вандализма и т.д.) или сторонних обстоятельств (скачков напряжения электропитания, электрических разрядов, попадания внутрь жидкостей, инородных предметов и т.д.).

Производитель имеет право вносить в конструкцию изделия изменения, не влияющие на основные технические характеристики и надежность изделия.

## Гарантийный талон контроллера Gate-IP100

Серийный номер: \_\_\_\_\_

Фирма-продавец: \_\_\_\_\_

Адрес фирмы-продавца: \_\_\_\_\_

Телефон, факс фирмы-продавца: \_\_\_\_\_

Дата продажи: \_\_\_\_\_

Печать: