Оглавление

Введение

Настоящий документ служит единым руководством по настройке и эксплуатации контроллера системы контроля и управления доступом (СКУД), а также по использованию программного обеспечения (ПО), предназначенного для взаимодействия с ним.
Документ ориентирован на три ключевые категории пользователей:

- Администраторы СКУД — для настройки политик доступа, управления базой данных пользователей и мониторинга событий;
- Инженеры по монтажу и пусконаладке — для корректной установки оборудования, подключения считывателей, контроллеров и других компонентов системы, а также выполнения первоначальной конфигурации;
- Конечные пользователи — для понимания основных принципов работы с системой (например, регистрация карт/брелоков, прохождение аутентификации, реагирование на индикацию и звуковые сигналы).

Структура документа построена по принципу от настроек **автономных** функций до настроек **сетевого** режима работы системы, обеспечивая последовательное освоение материала: от базовых действий до углубленных настроек. Все инструкции сопровождаются пояснениями, рекомендациями по безопасности.
В руководство включено описание терминов, используемых при описании системы,приведен перечень оборудования, поддерживаемого системой, указаны требования к ПК.

Назначение

Система контроля и управления доступом SKAT AC предназначена для управления доступом, учета и управления перемещениями физических объектов (сотрудников, посетителей, транспортных средств) через контрольные точки (двери, турникеты, шлагбаумы, ворота и др.) на охраняемой территории или в зданиях.

Система позволяет решать следующие задачи:

- Обеспечение санкционированного прохода/проезда на основе идентификации и верификации;
- Конфигурация контроллеров: присвоение имен контроллерам, объединение контроллеров в логические зоны, внутри которых, в зависимости от конфигурации объекта, допускаются другие вложенные зоны.
- Дистанционное/локальное управление точками доступа (блокировка, разблокировка, однократный проход);
- Удаленный мониторинг оборудования и событий системы;
- Гибкая настройка прав доступа по времени и зонам;
- Создание авторизованных ключей для разграничения прав доступа в различные зоны и отдельные точки прохода.

После установки контроллеров на объекте и построения логических зон в WEB-приложении, пользователь может создать расписание доступа прохода через зоны / контроллеры. Расписание предусматривает различные сценарии прохода в зависимости от дня недели и текущего времени. Время определяется локальным временем сервера, где запущено приложение, управляющее всеми контроллерами CAN-сети.

У одного контроллера может быть максимум 7 расписаний работы. Для каждого расписания доступно сохранения до 1000 ключей. Ключ не может работать в отрыве от расписания, он всегда должен быть привязан к конкретному расписанию.

Ключи выдаются сотрудникам, которым предоставляются права доступа к различным зонам / контроллерам охраняемого объекта согласно установленного расписания. В зависимости от полномочий, у одного сотрудника может быть несколько ключей, с различными правами доступа и расписаниями.

Система производит мониторинг событий, полный список событий описан ниже. Все события привязываются к какому-то контроллеру и типу событий, другие атрибуты: ключ, зона и т. д. - опциональны.

В WEB-приложении реализован учет рабочего времени в различных разрезах в виде отчетов.

Назначение контроллера СКУД

Сетевой контроллер СКУД SKAT AC 02NET PACS предназначен для организации как автономных, так и распределенных сетевых систем контроля и управления доступом. Он оснащён интерфейсом для подключения считывателей, поддерживающих протоколы Wiegand и Touch Memory, и имеет встроенный охранный шлейф, предназначенный для подключения датчиков состояния двери.

Устройство может функционировать в автономном режиме или в составе сетевой системы под управлением серверного программного обеспечения "SKAT AC". Контроллер предназначен для управления доступом в охраняемые зоны путем обработки данных, поступающих от считывателей (карт, PIN-клавиатур и др.), и принятия решений о предоставлении или запрете прохода.

Контроллер обеспечивает:

- ведение журнала событий (проходы, тревоги, сбои); (хранение ключей 1000 на один канал);
- управление исполнительными устройствами (электромагнитными и электромеханическими замками, турникетами, шлагбаумами);
- взаимодействие с ПО.

Особенностью данного контроллера является поддержка двух основных режимов работы:

Автономный режим — контроллер функционирует независимо, принимая решения на основе данных внутри памяти контроллера (например, при отсутствии связи с сервером). В этом режиме администратор может загружать список авторизованных пользователей напрямую в память контроллера.

Сетевой режим — контроллер работает в составе распределенной системы, обмениваясь данными с сервером в реальном времени. Это позволяет реализовать централизованное управление, удалённую диагностику и интеграцию с другими системами безопасности (пожарная сигнализация и др.).

Выбор режима эксплуатации определяет не только архитектуру системы, но и подход к её настройке, обслуживанию и диагностике — что учтено в соответствующих разделах настоящего документа.

Термины

СКУД (Система контроля и управления доступом) - совокупность программно-аппаратных технических средств контроля и средств управления, имеющих целью ограничение и регистрацию входа-выхода объектов (людей, транспорта) на заданной территории через «точки прохода»: двери, ворота, КПП.
WEB-приложение - клиент-серверное приложение, в котором пользователь взаимодействует с серверной частью при помощи браузера. Логика **WEB-приложения** распределена между сервером и клиентом, хранение данных осуществляется, преимущественно, на сервере, обмен информацией происходит по сети.
CAN-сеть - промышленный сетевой стандарт, позволяющий по витой паре осуществить объединение в единую сеть различных узлов, механизмов, датчиков и т. п.
Контроллер - исполнительное устройство, принимающее решение о предоставлении / отказе в доступе пользователя по ключу с регистрацией данного события в системе.
Точка прохода - физическое препятствие (дверь, турникет, шлагбаум, ворота), оснащенное контроллером доступа и считывателем на вход (или двумя считывателя на “вход / выход”), которые осуществляют или запрещают доступ в охраняемую зону после проведения процедуры идентификации.
Зона (группа контроллеров) - объединение контроллеров в логическое понятие для простого и удобного программирования ключей.
Ключ – любой носитель авторизованного цифрового кода для доступа к защищенной зоне через точку прохода. В системе SKAT AC ключи функционально делятся на следующие типы:

- **Ключ доступа** - данный тип ключей обеспечивает проход через соответствующие зоны/контроллеры в разрешенное для него по расписанию время, при условии снятия с охраны всей системы.
- **Ключ безопасности** - ключ обеспечивает **постановку** на охрану контроллер/зону, во время, разрешенное ему по расписанию.
- **Универсальный ключ (ключ доступа и безопасности)** – универсальный ключ обеспечивает проход через соответствующие зоны/контроллеры и **снятие** с охраны всей СКУД, во время, разрешенное ему по расписанию.

Аккаунт – запись в БД WEB-приложения, в которой хранится информация о каждом новом пользователе. При регистрации каждый новый аккаунт наделяется правами **Администратора** или **Пользователя**.
Администратор – авторизованный технический специалист, обеспечивающий настройку приложения и создание аккаунтов новых Пользователей и Администраторов. Администратор уполномочен активировать общую охранную и пожарную тревогу.
Пользователь – авторизованный оператор WEB-приложения, следящий и реагирующий на события, происходящие на охраняемом объекте.
Сотрудник – работник, имеющий ключ, который обеспечивает доступ на определенные участки объекта в установленное время. Все перемещения сотрудника фиксируются в журнале событий WEB-приложения и могут быть проанализированы в соответствующих отчетах.
БД – база данных WEB-приложения

Поддерживаемое оборудование

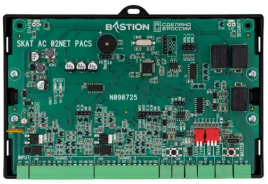
Для функционирования системы контроля и управления доступом SKAT AC в сетевом режиме необходимо наличие преобразователя CAN-USB. Преобразователь подключается напрямую к USB-порту ПК, на котором установлено ПО SKAT AC.

1. Считыватели

Наименование	Описание	Внешний вид
SPRUT RFID Reader-17BL	Считыватель используется для ввода номеров карт EM-marin. Подключается автоматически через USB, не требует дополнительной настройки. Подходит для быстрого переноса ключей в систему, достаточно просто поднести проксимити-карту и считыватель сразу введет ее в точку ввода текста указанную на компьютере.	
SPRUT RFID Reader-16BL	Считыватель предназначен для получения информации с идентификаторов - карт формата EM-Marin, в системе контроля и управления доступом, с дальнейшей передачей полученной информации контроллеру	
SPRUT RFID Reader-16WH	Считыватель предназначен для получения информации с идентификаторов - карт формата EM-Marin, в системе контроля и управления доступом, с дальнейшей передачей полученной информации контроллеру	
SPRUT RFID Reader-15GR-K	Считыватель предназначен для получения информации с идентификаторов - карт формата EM-Marin, в системе контроля и управления доступом. В конструкцию считывателя SPRUT RFID Reader-15GR-K входит цифровая клавиатура, что позволяет организовать доступ по ПИН коду.	

SPRUT RFID Reader-14BL	Считыватель предназначен для получения информации с идентификаторов - карт формата EM-Marin, в системе контроля и управления доступом, с дальнейшей передачей полученной информации контроллеру	
SKAT AC 13BL Reader	Накладной считыватель для идентификаторов формата EM-Marine со световой и звуковой индикацией.	
SPRUT RFID Reader-12WH	Накладной считыватель для идентификаторов формата EM-Marine со световой и звуковой индикацией.	
SPRUT RFID Reader-12GR	Накладной считыватель для идентификаторов формата EM-Marine со световой и звуковой индикацией.	
SPRUT RFID Reader-11BL	Накладной считыватель для идентификаторов формата EM-Marine со световой и звуковой индикацией.	
SPRUT RFID Reader-11WH	Накладной считыватель для идентификаторов формата EM-Marine со световой и звуковой индикацией.	

2. Контроллеры доступа

Наименование	Описание	Внешний вид
SKAT AC 02NET PACS	предназначен для организации как автономных, так и распределенных сетевых систем контроля и управления доступом. Дополнительно контроллер доступа оснащён охранным шлейфом, который используется для подключения датчика состояния двери (геркона). К контроллеру возможно подключение электромагнитных, электромеханических и соленоидных ригельных замков. Также контроллер может управлять турникетами и шлагбаумами разных производителей.	
SPRUT PACS-02NET	поддерживает до 1 000 пользовательских ключей и обеспечивает надежную идентификацию на основе электронных брелков и карт форматов TM DS, EM-Marine и Mifare. Контроллер позволяет управлять различными элементами доступа: кнопками разблокировки дверей, электромагнитными и электромеханическими замками, считывателями электронных ключей, включая кодовый набор от 4 до 8 символов, а также турникетами производства SKAT.	

3. Замки

Наименование	Описание	Внешний вид
SPRUT Lock-03ER	электромеханический замок в уличном исполнении	

SPRUT Lock	Электромагнитные замки SPRUT-Lock устанавливаются на любых дверях и обеспечивают надежное запирание.	
SKAT AC Lock	Электромагнитные замки SKAT AC устанавливаются на двери любого типа и обеспечивают надёжное запирание.	

- электромеханические замки сторонних производителей
- электромагнитные замки сторонних производителей

4. Турникеты

Наименование	Описание	Внешний вид
SPRUT TRIPOD-1001	Предназначен для контроля доступа в местах скопления людей, обеспечивая разделение их потока «по одному».	
SPRUT Tripod-1001-EC	Предназначена для контроля доступа и управления потоками людей, обеспечивая разделение их потока «по одному». Имеет функцию работы по радиоканалу, поставляется в комплекте с радиобрелками.	

- Турникеты сторонних производителей

5. Шлагбаумы

- шлагбаумы сторонних производителей

Установка контроллера

При установке и эксплуатации изделия необходимо руководствоваться действующими нормативными документами, регламентирующими требования по охране труда и правила безопасности при эксплуатации электроустановок. Далее нужно выбрать место для установки.
Корпус контроллера рассчитан на монтаж на стене или на DIN-рейке. Установка производится в вертикальной плоскости. Особое внимание следует уделить прокладке кабельной проводки, чтобы обеспечить её надежность и исключить несанкционированный доступ.
Кабельную проводку следует разместить так, чтобы исключить свободный доступ к ней.
Подключение питания

- Используется стабилизированный блок питания требуемого напряжения (12В DC); **(уточнить Амперы по питанию или мощность) - смотреть какие у юзера замки**

Следуя схеме, приведённой в руководстве, к контроллеру подключаются:

- Считыватели (по интерфейсам Wiegand, Touch Memory);
- Исполнительные устройства (электрозамки, турникеты и шлагбаумы — через сухие контакты);
- Датчики состояния двери (герконы, концевые выключатели — для контроля «открыто/закрыто»);
- Кнопки выхода;

Обязательно обратите внимание, что если датчик состояния двери не подключается, то контакты SENS и GND нужно замкнуть перемычкой. Для сетевой работы контроллер подключается к CAN-шине с помощью отмеченных на контроллере контактов - CAN_HIGH и CAN_LOW. Важно помнить, что первое и последнее устройства в CAN-цепочке должны быть оконцованы терминирующими резисторами, которые входят в комплект поставки.
Обязательно при отсутствии подключения пожарного шлейфа, замкнуть контакты К1 + - между собой.
В случае, если при включении контроллера без подключения охранного шлейфа индицируется ошибка «Security Loop», подключите к контактам «Охранный шлейф» (+) (-) резистор 2 кОм.
Проверка и первоначальная настройка

- Визуальный и электрический контроль — отсутствие КЗ, правильная полярность, заземление.
- Включение питания — контроль индикации на контроллере (питание, связь, ошибки).
- Тест подключения периферии — например, считывание тестовой карты, срабатывание замка по команде.

После установки на лицевой панели контроллера проверьте 2 пользовательских светодиода:

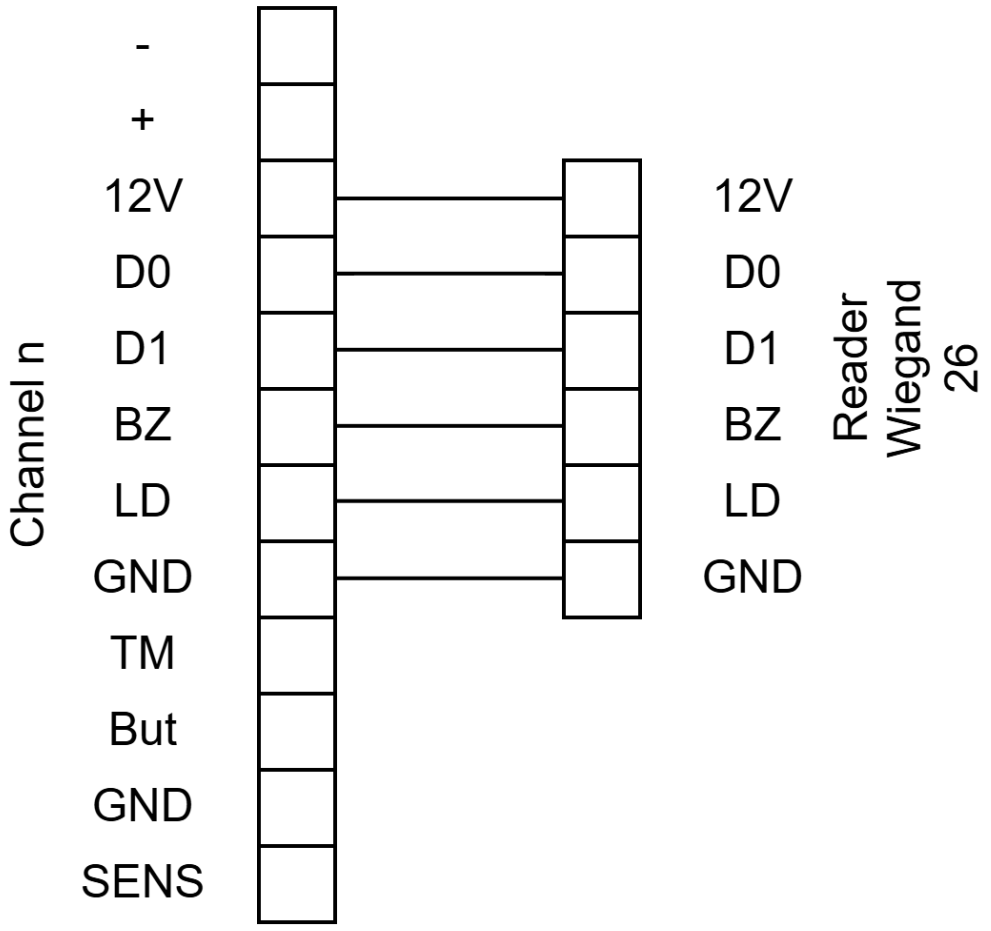
Светодиод	Поведение	Результат
Зеленый индикатор «Статус»	светодиод светится постоянно	Контроллер доступа в режиме «Нормальный»
	мигает 1 раз в секунду	Контроллер доступа в режиме записи пользовательских ключей любого статуса
Красный индикатор «Охрана»	светодиод светится постоянно	Охранная сигнализация включена
	светодиод отключён	Охранная сигнализация выключена
	мигает 2 раза в секунду	Обрыв охранного шлейфа

На плате устройства, доступной после снятия крышки, находятся дополнительные индикаторы. Красный светодиод питания должен светиться постоянно, что подтверждает наличие питания. Зелёный индикатор соединения с CAN-шиной будет светиться постоянно при установленной связи с сетью и мигать во время обмена данными. Если сеть CAN не подключена, этот индикатор не светится, и контроллер может сигнализировать об ошибке CAN ERROR, что не

мешает ему работать автономно. Красный индикатор ошибок обмена данными по CAN-шине светится постоянно в случае возникновения проблем с сетью.

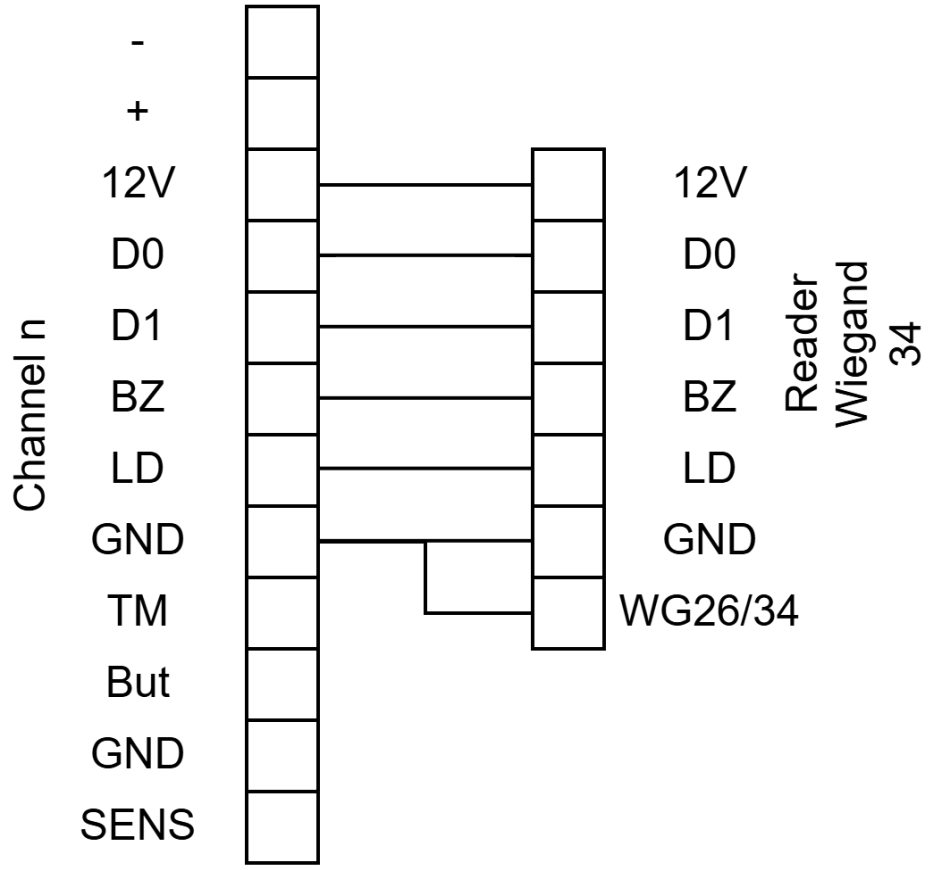
Подключение Wiegand 26 считки

Подключение осуществляется следующим образом:
На левой стороне схемы представлен разъем контроллера, где обозначены его выводы для любого из каналов. На правой стороне — соответствующие выводы самого считывателя.
Питание: Вывод 12V на контроллере соединяется с контактом 12V на считывателе. Это обеспечивает подачу необходимого напряжения питания на устройство.
Заземление: Вывод GND на контроллере подключается к контакту GND на считывателе. Это создает общую электрическую землю для стабильной работы цепи.
Передача данных (Wiegand): Данные о считанном ключе передаются по двум линиям:
Линия D0 контроллера соединяется с контактом D0 считывателя.
Линия D1 контроллера соединяется с контактом D1 считывателя.
Эти линии используются для передачи битовой информации в соответствии с протоколом Wiegand 26.
Сигналы управления и состояния:
Вывод BZ контроллера подключается к контакту BZ считывателя. Этот контакт используется для управления встроенным звуковым сигналом (buzzer) на считывателе.
Вывод LD контроллера подключается к контакту LD считывателя. Этот контакт управляет светодиодом (LED) на считывателе, который сигнализирует о результате считывания (например, зелёный — доступ разрешен, красный — доступ запрещен).
Таким образом, данная схема показывает прямое и последовательное соединение соответствующих контактов контроллера и считывателя, обеспечивающее как питание устройства, так и двунаправленную передачу данных и управляющих сигналов.



Подключение Wiegand 34 считки

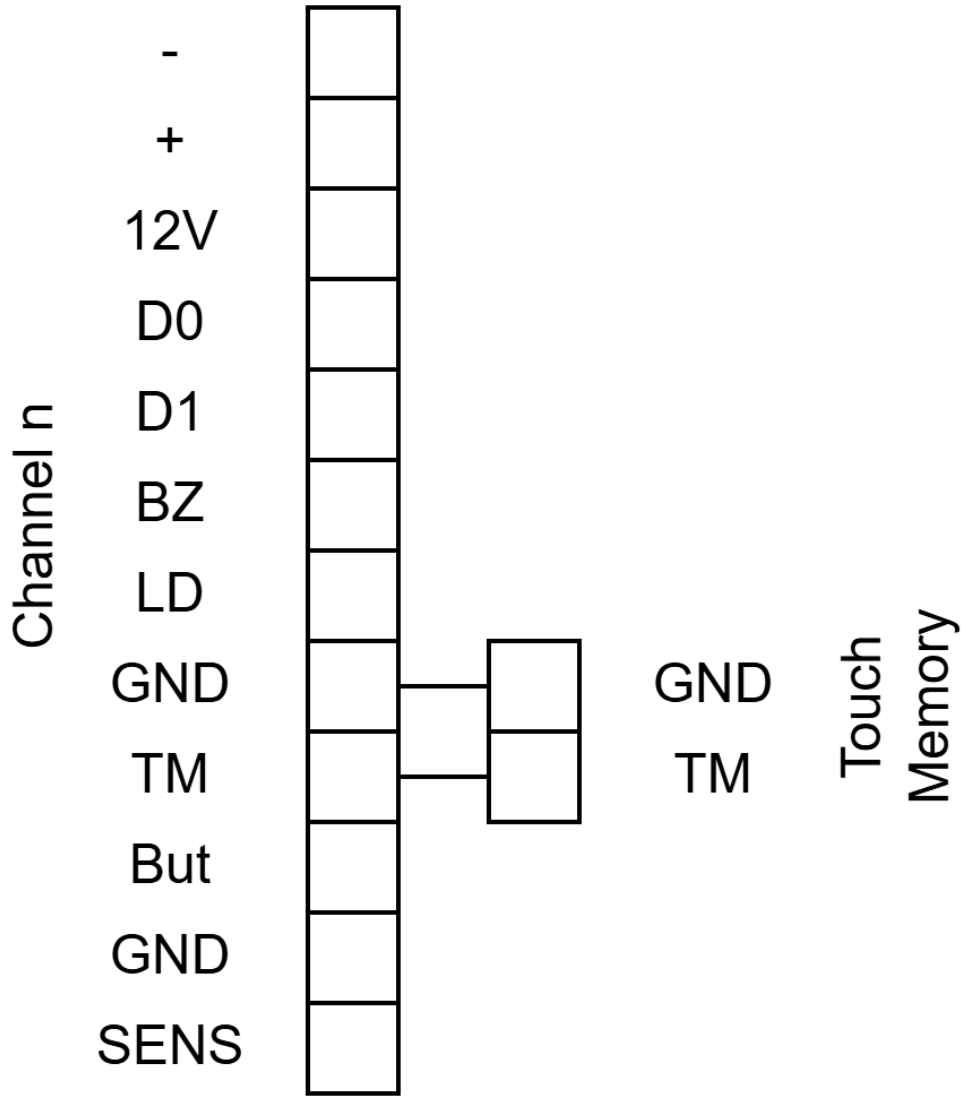
Подключение осуществляется следующим образом:
На левой стороне схемы представлен разъем контроллера, где обозначены его выводы для канала n. На правой стороне — соответствующие выводы самого считывателя.
Питание: Вывод 12V на контроллере соединяется с контактом 12V на считывателе. Это обеспечивает подачу необходимого напряжения питания на устройство.
Заземление: Вывод GND на контроллере подключается к контакту GND на считывателе. Это создает общую электрическую землю для стабильной работы цепи.
Передача данных (Wiegand): Данные о считанном ключе передаются по двум линиям:
Линия D0 контроллера соединяется с контактом D0 считывателя.
Линия D1 контроллера соединяется с контактом D1 считывателя.
Эти линии используются для передачи битовой информации в соответствии с протоколом Wiegand 34.
Сигналы управления и состояния:
Вывод BZ контроллера подключается к контакту BZ считывателя. Этот контакт используется для управления встроенным звуковым сигналом (buzzer) на считывателе.
Вывод LD контроллера подключается к контакту LD считывателя. Этот контакт управляет светодиодом (LED) на считывателе, который сигнализирует о результате считывания (например, зелёный — доступ разрешен, красный — доступ запрещен).
Протокол: Контакт WG26/34 на считывателе является общим для выбора протокола. В данном случае он указывает на использование протокола Wiegand 34 и подключен к контакту GND.



Подключение Touch Memory считки

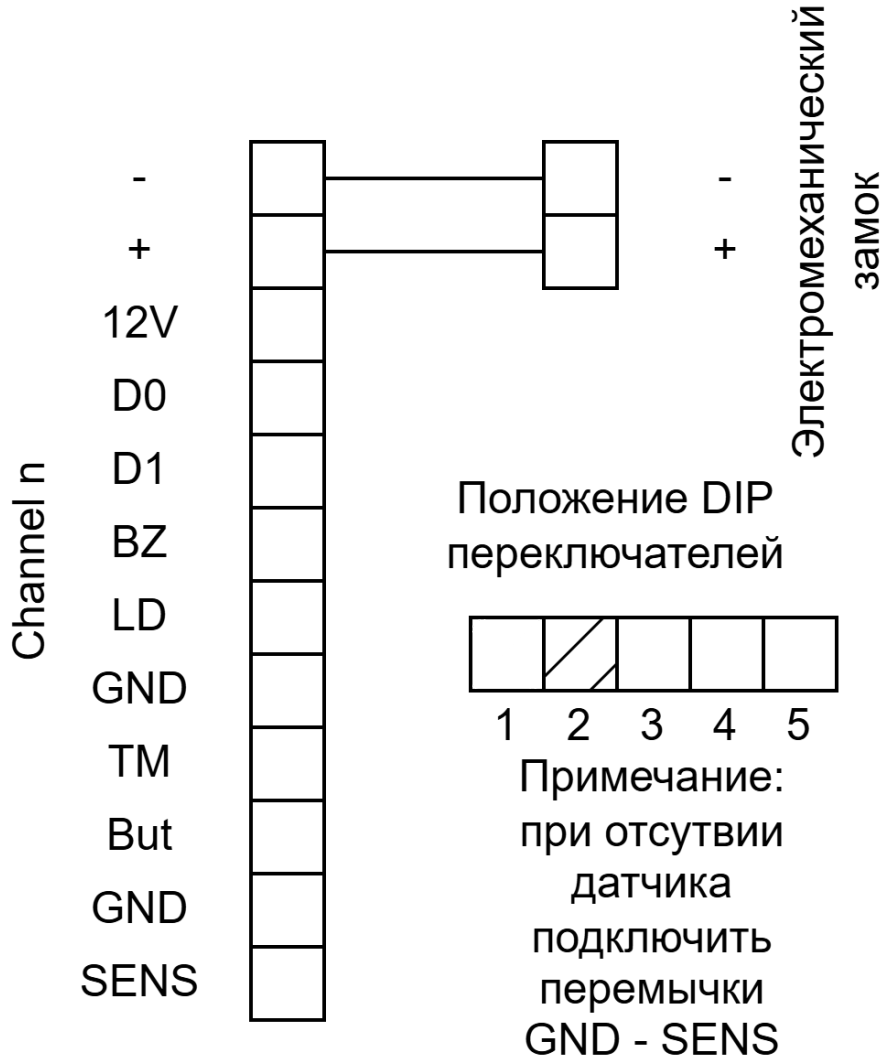
Подключение осуществляется следующим образом:
На левой стороне схемы представлен разъем контроллера, где обозначены его выводы для канала n. На правой стороне — соответствующие выводы самого считывателя Touch Memory.
Заземление: Вывод GND на контроллере соединяется с контактом GND на считывателе. Это создает общую электрическую землю для стабильной работы цепи.
Передача данных (Touch Memory): Данные о считанном ключе передаются по одной линии:

Линия TM контроллера соединяется с контактом TM считывателя. Этот контакт является линией связи для протокола Touch Memory, по которой происходит обмен данными между считывателем и контроллером.



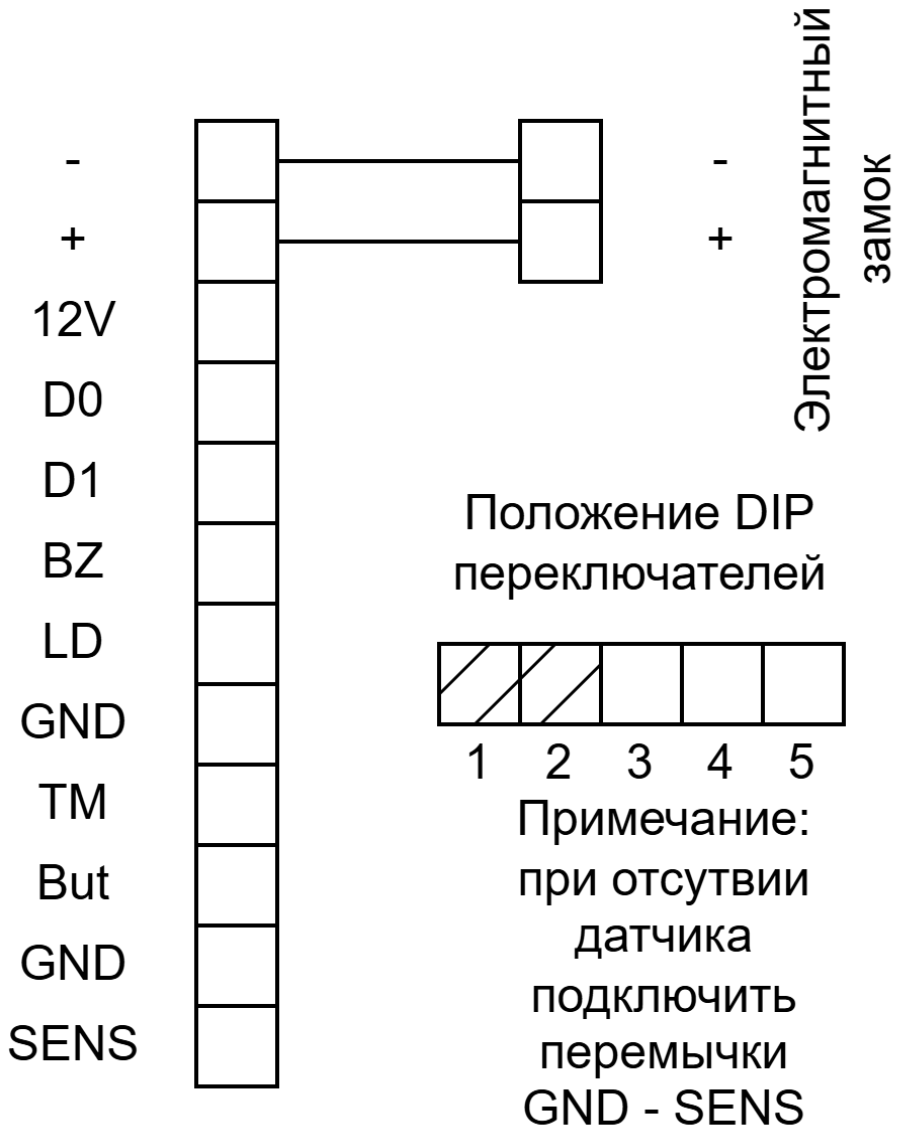
Подключение электромеханического замка

Подключение осуществляется следующим образом:
На левой стороне схемы представлен разъем контроллера, где обозначены его выводы для канала n. На правой стороне — контакты самого электромеханического замка.
Питание: Вывод + на контроллере соединяется с положительным контактом (+) электромеханического замка. Вывод - на контроллере соединяется с отрицательным контактом (-) замка. Таким образом, замок подключается параллельно источнику питания контроллера. При срабатывании контроллера он замыкает цепь, подавая напряжение на замок и приводя его в действие (открывая дверь).
Важно отметить, что для корректной работы системы при использовании электромеханического замка необходимо правильно установить DIP-переключатели на плате контроллера. Как указано в руководстве, для этого нужно включить DIP-переключатель 2 в блоке LOCK TYPE.
Также в схеме присутствует примечание, которое указывает на необходимость дополнительных действий: если не используется датчик состояния двери (геркон), то следует подключить перемычки между контактами GND и SENS на соответствующем канале контроллера.



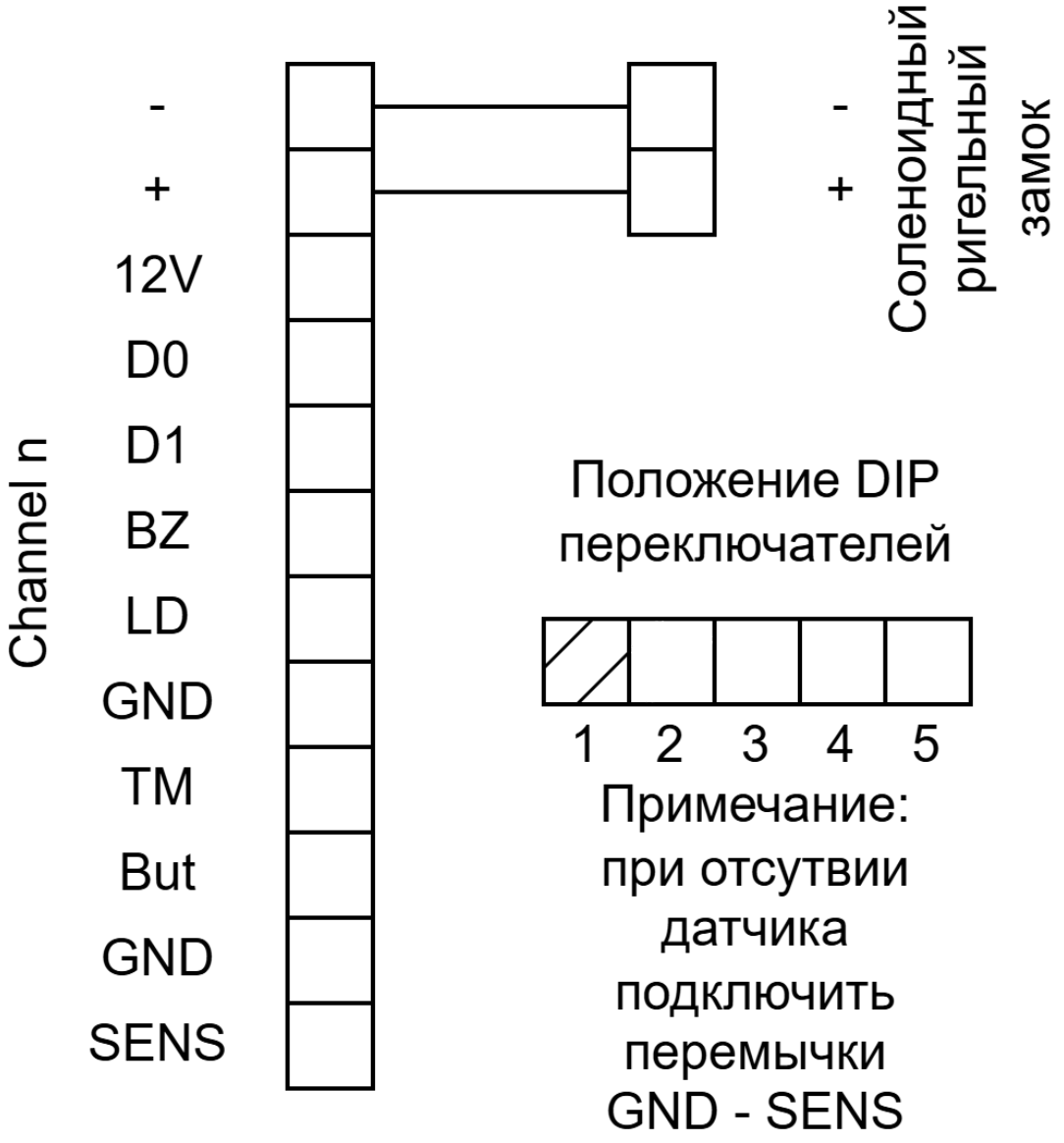
Подключение электромагнитного замка

Подключение осуществляется следующим образом:
На левой стороне схемы представлен разъем контроллера, где обозначены его выводы для канала n. На правой стороне — контакты самого электромагнитного замка.
Питание: Вывод + на контроллере соединяется с положительным контактом (+) электромагнитного замка. Вывод - на контроллере соединяется с отрицательным контактом (-) замка. Таким образом, замок подключается параллельно источнику питания контроллера. При срабатывании контроллера он замыкает цепь, подавая напряжение на замок и приводя его в действие (открывая дверь).
Важно отметить, что для корректной работы системы при использовании электромагнитного замка необходимо правильно установить DIP-переключатели на плате контроллера. Как указано в руководстве, для этого нужно оставить оба переключателя 1 и 2 в блоке LOCK TYPE выключенными.
Также в схеме присутствует примечание, которое указывает на необходимость дополнительных действий: если не используется датчик состояния двери (геркон), то следует подключить перемычки между контактами GND и SENS на соответствующем канале контроллера.



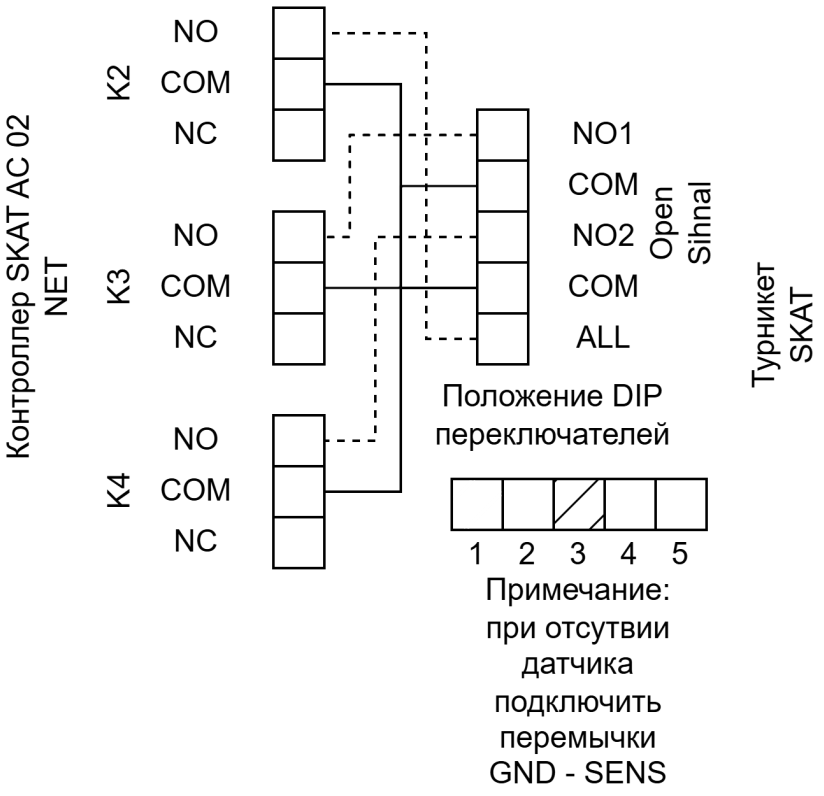
Подключение соленоидного замка

Подключение осуществляется следующим образом:
На левой стороне схемы представлен разъем контроллера, где обозначены его выводы для канала n. На правой стороне — контакты самого соленоидного ригельного замка.
Питание: Вывод + на контроллере соединяется с положительным контактом (+) соленоидного ригельного замка. Вывод - на контроллере соединяется с отрицательным контактом (-) замка. Таким образом, замок подключается параллельно источнику питания контроллера. При срабатывании контроллера он замыкает цепь, подавая напряжение на замок и приводя его в действие (открывая дверь).
Важно отметить, что для корректной работы системы при использовании соленоидного ригельного замка необходимо правильно установить DIP-переключатели на плате контроллера. Как указано в руководстве, для этого нужно включить DIP-переключатель 1 в блоке LOCK TYPE. Также в схеме присутствует примечание, которое указывает на необходимость дополнительных действий: если не используется датчик состояния двери (геркон), то следует подключить перемычки между контактами GND и SENS на соответствующем канале контроллера.



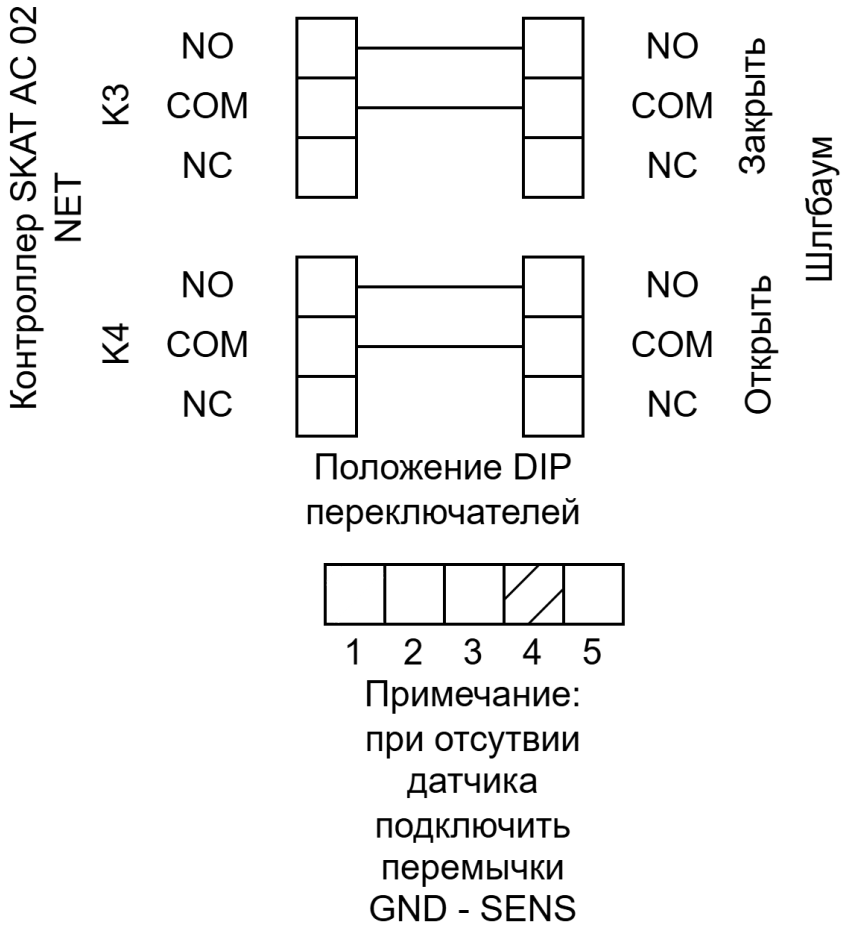
Подключение турникета

Подключение производится следующим образом:
На левой стороне схемы представлены три релейных выхода контроллера: K2, K3 и K4. Каждый из них имеет три контакта: NO (нормально-открытый), COM (общий) и NC (нормально-замкнутый). На правой стороне — входы турникета: NO1, COM, NO2, а также специальные сигналы "Open" и "Signal".
Сигнал открытия (Open): Для управления открытием турникета используется контакт NO1 турникета. Он соединяется с нормально-открытым контактом NO реле K2 на контроллере. Общий контакт COM реле K2 подключается к общему контакту COM турникета. При срабатывании реле K2 цепь между COM и NO замыкается, что передает сигнал «открыть» на турникет.
Сигнал закрытия (Close): Для управления закрытием или возвратом турникета в исходное положение используется контакт NO2 турникета. Он соединяется с нормально-открытым контактом NO реле K3 на контроллере. Общий контакт COM реле K3 подключается к общему контакту COM турникета. При срабатывании реле K3 цепь между COM и NO замыкается, что передает сигнал «закрыть» или «возврат».
Общий сигнал (All): Контакт ALL турникета подключается к нормально-открытому контакту NO реле K4 на контроллере. Общий контакт COM реле K4 также подключается к общему контакту COM турникета. Этот сигнал может использоваться для универсального управления или сигнализации состояния.
Важно отметить, что для корректной работы системы при использовании турникета необходимо правильно установить DIP-переключатели на плате контроллера. Как указано в руководстве, для этого нужно включить DIP-переключатель 1 в блоке MODE.
Также в схеме присутствует примечание, которое указывает на необходимость дополнительных действий: если не используется датчик состояния двери (геркон), то следует подключить перемычки между контактами GND и SENS на соответствующем канале контроллера.



Подключение шлагбаума

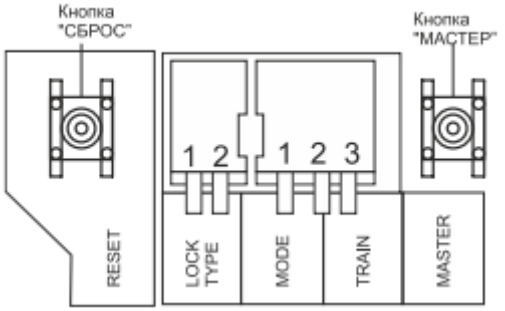
Подключение производится следующим образом:
На левой стороне схемы представлены два релейных выхода контроллера: K3 и K4. Каждый из них имеет три контакта: NO (нормально-открытый), COM (общий) и NC (нормально-замкнутый). На правой стороне — входы шлагбаума: NO, COM, NC для двух функций — "Закрыть" и "Открыть".
Сигнал закрытия (Закрыть): Для управления закрытием шлагбаума используется контакт NO на входе "Закрыть". Он соединяется с нормально-открытым контактом NO реле K3 на контроллере. Общий контакт COM реле K3 подключается к общему контакту COM на входе "Закрыть" шлагбаума. При срабатывании реле K3 цепь между COM и NO замыкается, что передает сигнал «закрыть» на шлагбаум.
Сигнал открытия (Открыть): Для управления открытием шлагбаума используется контакт NO на входе "Открыть". Он соединяется с нормально-открытым контактом NO реле K4 на контроллере. Общий контакт COM реле K4 подключается к общему контакту COM на входе "Открыть" шлагбаума. При срабатывании реле K4 цепь между COM и NO замыкается, что передает сигнал «открыть».
Важно отметить, что для корректной работы системы при использовании шлагбаума необходимо правильно установить DIP-переключатели на плате контроллера. Как указано в руководстве, для этого нужно включить DIP-переключатель 2 в блоке MODE.
Также в схеме присутствует примечание, которое указывает на необходимость дополнительных действий: если не используется датчик состояния двери (геркон), то следует подключить перемычки между контактами GND и SENS на соответствующем канале контроллера.



Настройки контроллера

Сетевой контроллер СКУД SKAT AC 02NET PACS (далее по тексту – контроллер, изделие) предназначен для организации как автономных, так и распределенных сетевых систем контроля и управления доступом (СКУД) с использованием CAN-шины, обеспечивающей максимальную удаленность между первым и крайним в линии контроллером доступа до 300 м. Прежде чем начать эксплуатацию изделия убедитесь в правильной настройке блока DIP переключателей:

Блок	Положение переключателей	Режим работы
Блок LOCK TYPE	DIP переключатели «1» и «2» выключены	Электромагнитный замок
	DIP переключатель «1» включен	Соленоидный ригельный замок
	DIP переключатель «2» включен	Электромеханический замок
Блок MODE	DIP переключатели «1» и «2» выключены	Режим работы на две двери (замка)
	DIP переключатель «1» включен	Режим электронной проходной (турникета)
	DIP переключатель «2» включён	Режим работы со шлагбаумом
	DIP переключатели «1» и «2» включены	Режим одной двери (замка) на два считывателя
Блок TRAIN	DIP переключатели «3» включен	Режим безусловного прохода. Каждый ключ доступа записывается в память контроллера и разрешает доступ



Настройка для работы в автономном режиме

При первом запуске контроллер находится в дежурном режиме.

- Для записи пользовательских карт можно воспользоваться кнопкой «МАСТЕР» на плате контроллера, либо запрограммировать мастер ключи в режиме «Мастер ключи»
- Для входа в режим программирования мастер ключей необходимо ЗАЖАТЬ кнопку «СБРОС» на контроллере при отключенном питании, после чего подать питание на контроллер.
- Отпустить кнопку «СБРОС» после включения контроллера.
- Контроллер перейдёт в режим «Мастер ключи» (при этом светодиод «Статус» будет мигать зелёным 1 раз в секунду) в котором можно сохранить не более двух мастер ключей.
- После сохранения мастер ключей контроллер автоматически перейдёт в следующий режим - «Ключи доступа» (дважды прозвучит короткий звуковой сигнал).
- В режиме «Ключи доступа» любая поднесённая пользовательская карта будет добавлена как «карта доступа» в память контроллера.
- При поднесении мастер ключа к считывателю в режиме работы контроллера «Ключи доступа», либо нажатии на кнопку «МАСТЕР», контроллер перейдёт в режим «Охранные ключи» (трижды прозвучит короткий звуковой сигнал).
- В режиме «Охранные ключи» любые пользовательские ключи станут картами включения/отключения охранного режима контроллера.
- Последующее однократное использование мастер ключа или кнопки «МАСТЕР» переведёт контроллер в режим «Универсальные ключи» (четыре раза прозвучит короткий звуковой сигнал). В этом режиме пользовательские карты автоматически снимают режим охраны, а также являются пользовательскими ключами доступа.
- Последующее однократное использование мастер ключа или кнопки «МАСТЕР» возобновит работу в режиме «Базовый».

Рис.1

Описание режимов работы и пользовательских ключей.

Режим «Мастер ключи»

В режиме «Мастер ключи» контроллер доступа находится после перезапуска питания при зажатой кнопке «СБРОС» на плате управления. Все записанные ранее ключи доступа будут удалены при активации режима. Зелёный индикатор «Статус» мигает 1 раз в секунду в ожидании записи двух мастер ключей. Для добавления мастер ключей в данном режиме необходимо поднести пользовательский ключ к считывателю. Успешное добавление мастер ключа сопровождается коротким звуковым сигналом. Выход из режима происходит

автоматически при сохранении в памяти контроллера доступа двух мастер ключей (допустимо использовать один мастер ключ, для этого его нужно дважды приложить к считывателю контроллера доступа)

Режим «Базовый»

В базовом режиме контроллер доступа находится «по умолчанию» при первом включении и является основным режимом контроллера доступа.

Контроллер анализирует статус пользовательского ключа, поднесённого к считывателю, и запускает соответствующий сценарий работы:

- «Карта доступа» статус пользовательской карты, который переводит контроллер доступа в режиме «Базовый» активирует исполнительное устройство (электромагнитный, электромеханический, соленоидный (ригельный) замки, а также турникет или шлагбаум);
- «Ключ охраны» статус пользовательской карты, который переводит контроллер доступа из режима «Базовый» в режим «Охрана»;
- «Универсальный ключ» статус пользовательской карты, который переводит контроллер доступа из режима «Охрана» в режим «Базовый», а далее работает как пользовательская карта со статусом «Карта доступа».

Режим «Охрана»

В режиме «Охрана» контроллер доступа находится при наличии охранного шлейфа и поднесении к считывателю контроллера доступа в режиме «Базовый» пользовательского ключа в статусе «Ключ охраны». Пользовательские ключи со статусом «Карта доступа»; «Мастер ключ» - не активны. Выход из режима возможен только с помощью пользовательского ключа со статусом «Универсальный ключ».

Режимы «Ключи доступа», «Охранные ключи», «Универсальные ключи»

Режимы переключаются последовательно в порядке «Ключи доступа» -> «Охранные ключи» -> «Универсальные ключи». Переход в эти режимы возможен только из режимов работы контроллера «Мастер ключи» либо «Базовый». Для этого необходимо однократно нажать кнопку «МАСТЕР», либо приложить мастер ключ к считывателю устройства. Аналогичным образом режимы последовательно переключаются между собой. В этих режимах можно присвоить статусы пользовательским картам «Карта доступа», «Ключ охраны» либо «Универсальный ключ» соответственно.

Приложение СКУД SPRUT «Менеджер управления ключами»

Приложение "Менеджер ключей" предназначено для локального управления базой ключей контроллера СКУД в условиях, когда он функционирует в автономном режиме, то есть без постоянного подключения к центральному серверу. Основной задачей приложения является упрощение процесса добавления, удаления и настройки статусов ключей непосредственно на устройстве через USB-соединение.
С его помощью администратор может создавать новые записи ключей, присваивать им определённый уровень доступа, а также удалять существующие записи. Приложение позволяет экспортировать текущую базу ключей из контроллера в файл на компьютере, что удобно для резервного копирования. Обратно, сформированную или изменённую базу можно импортировать из файла на компьютере непосредственно в память контроллера. Важно учитывать, что операция импорта приводит к полной замене содержимого памяти контроллера на данные из файла, поэтому перед её выполнением рекомендуется сделать резервную копию текущих настроек.

Технические требования

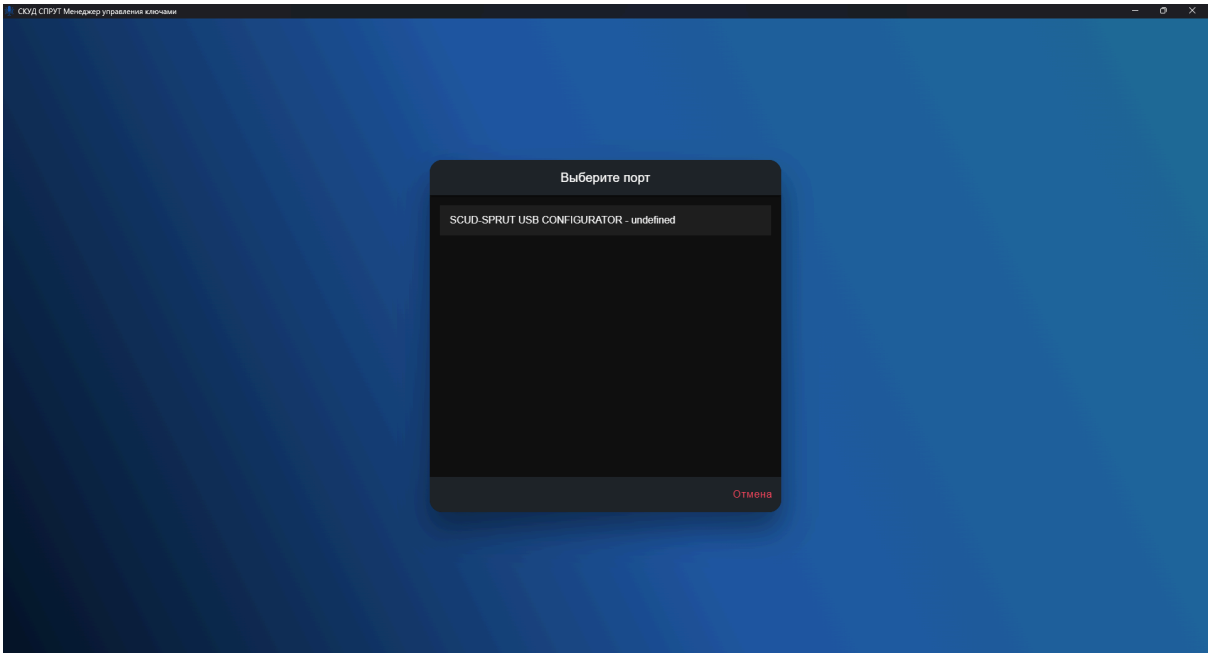
Приложение СКУД SPRUT «Менеджер управления ключами» устанавливается на компьютеры пользователя под управлением операционных систем Windows. После установки интерфейс программного обеспечения открывается в отдельном окне и запускается через соответствующий ярлык. Поддерживаемые версии Windows: Windows 10 или Windows 11. Корректная работа приложения на более ранних версиях операционной системы или на базе других операционных систем не гарантируется.

Установка приложения

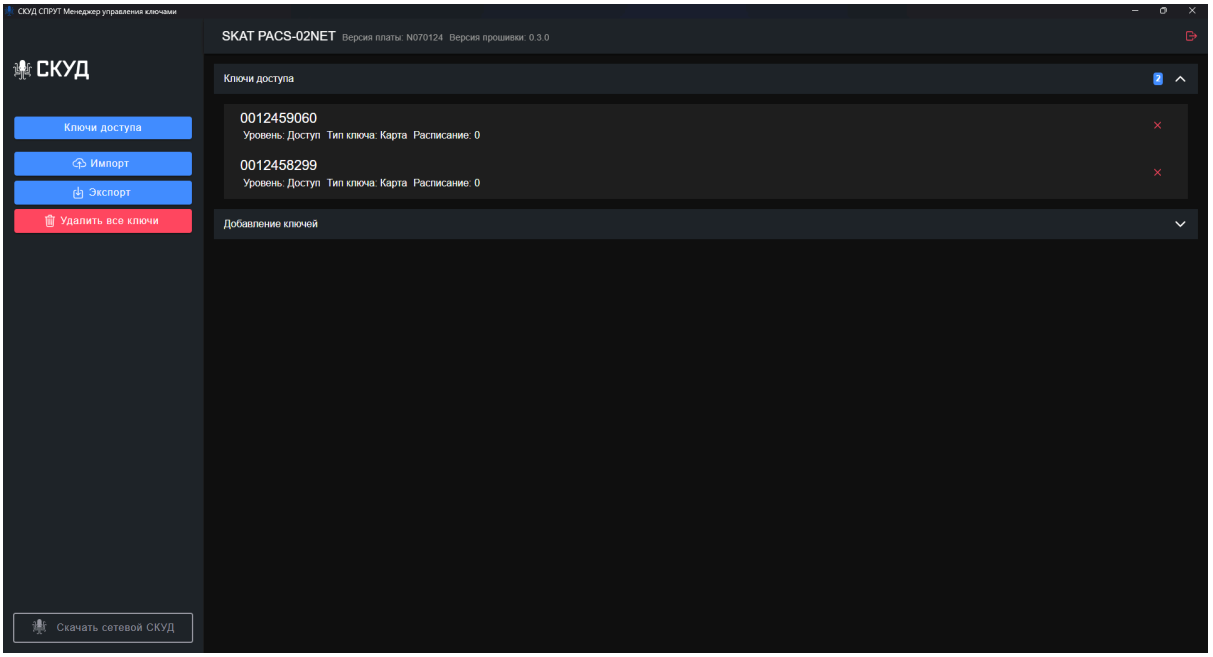
Установка приложения должна осуществляться в Windows-системах при помощи инсталляционного файла. Ярлык приложения создастся автоматически. Далее после запуска приложение будет открываться в отдельном окне.

Подключение контроллера

Для подключения контроллера к ПК необходимо воспользоваться кабелем USB Type-C- USB Type-A или кабелем USB Type-C-USB Type-C. Далее необходимо выбрать соответствующий контроллер в интерфейсе ПО (изделие должно быть включено)

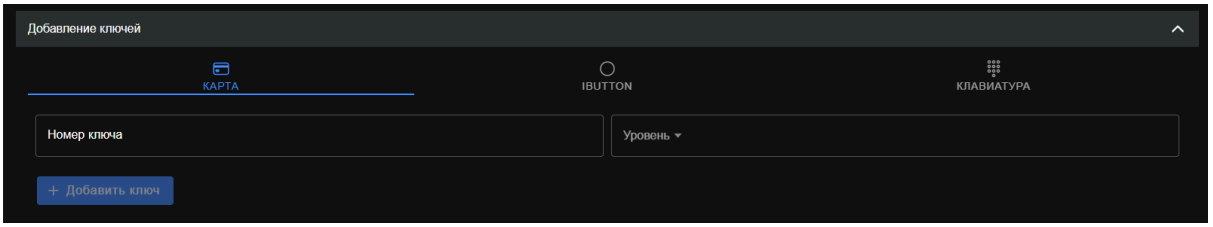


Далее автоматически будет произведен экспорт доступных ключей, их данные будут отражены в интерфейсе приложения.



Меню и функционал приложения

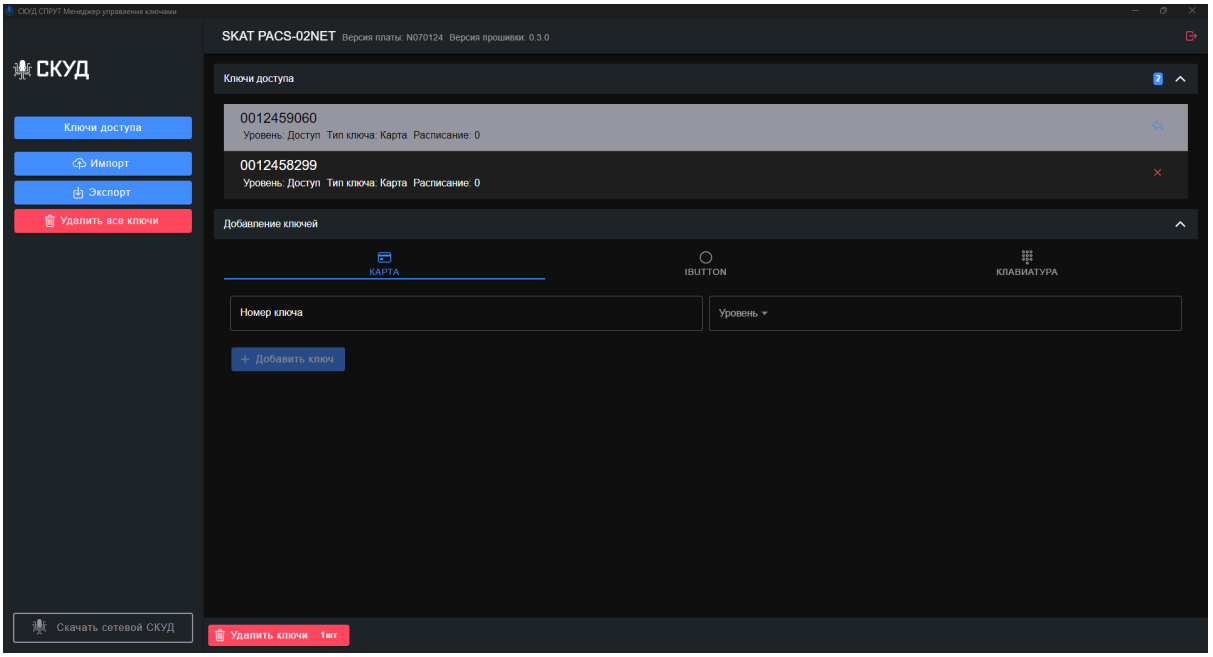
В меню «Ключи доступа» необходимо выбрать раздел «Добавление ключей», далее выбрать тип ключа:
Карта – карты формата EM-Marine;
Контактная память – магнитные ключи формата IButton;
Клавиатура – код доступа для считывателя с клавиатурой.



Введите номер ключа и выберите его уровень (см. Рис. 3). Уровни ключей:
Мастер-ключ. Ключ для переключения сервисных автономных режимов контроллера
Доступ и безопасность. Ключ для одновременного прохода и снятия/постановки охраны
Безопасность – ключ для снятия и постановки на охрану;
Доступ – ключ для прохода.
Далее нажать на кнопку «Добавить ключ» и он отобразится в списке ключей, доступных для сохранения в память контроллера.

Пример удаления ключей

Для удаления ключа в разделе «Ключи доступа» выберите необходимый ключ и нажмите на пиктограмму удаления. После удаления всех нужных ключей нажмите на кнопку удаления, чтобы удалить выбранные ключи из памяти контроллера. При необходимости возврата удаленного ключа нажмите на соответствующую пиктограмму



Импорт базы ключей на устройство

ПО «СКУД Менеджер ключей» не поддерживает импорт пользовательской базы ключей. Для корректного импорта подойдут только файлы, созданные посредством экспорта через ПО.
Для импорта базы ключей необходимо нажать на кнопку «Импорт» бокового меню. Далее выбрать файл формата .csv, в котором данные соответствуют формату: Номер ключа, тип доступа (где тип доступа определяется числом:
1 - Доступ, 2 - Безопасность, 3 - Доступ и безопасность, 4 - Мастер-ключ).
При этом все ключи из файла импортируются напрямую в устройство. Новые ключи появятся в разделе «Ключи доступа».

Экспорт базы ключей

Для экспорта базы ключей на ПК в виде файла формата .csv необходимо нажать на соответствующую кнопку в боковом меню. Далее при необходимости изменить имя файла и выбрать местоположения для сохранения

Сохранение ключей на устройство

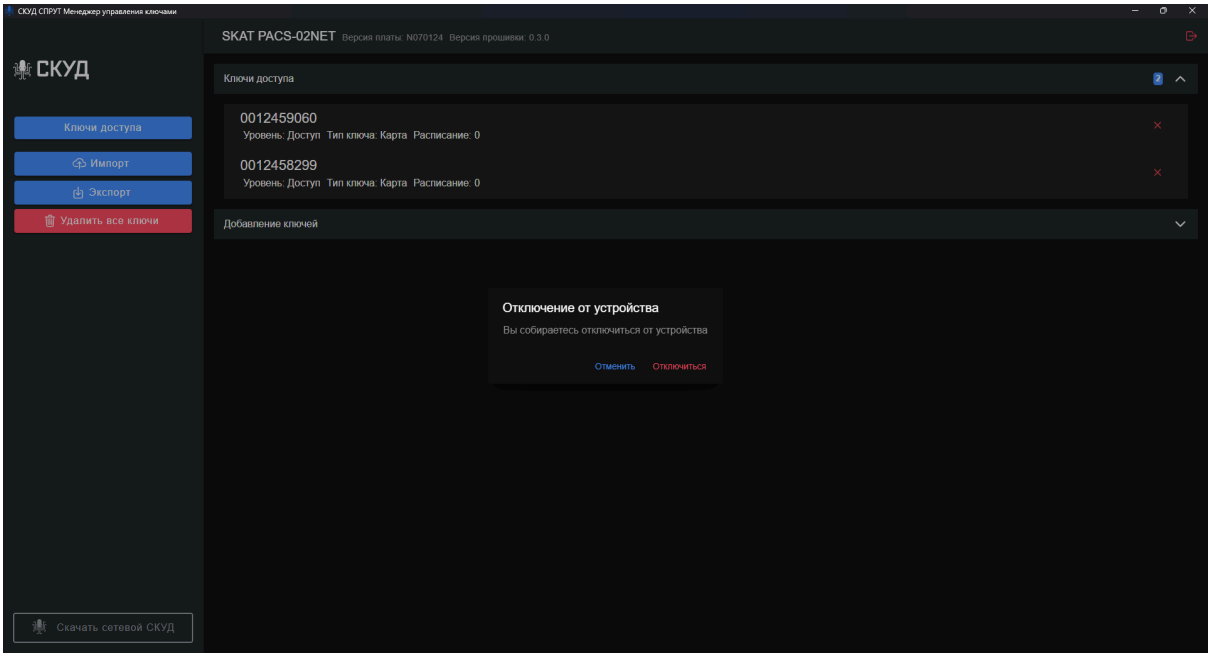
Для того, чтобы загрузить все добавленные ключи в память контроллера необходимо нажать на кнопку «Сохранить ключи», она появится при наличии новых добавленных ключей. После этого ключи добавится в раздел «Ключи доступа» и на устройство.

Сброс устройства

Для удаления всех ключей с устройства необходимо нажать на соответствующую кнопку бокового меню. При этом все ключи будут удалены из памяти устройства.

Отключение от устройства

Для отключения от устройства нажмите на соответствующую пиктограмму выхода в верхнем правом углу экрана. После подтверждения отключения вы будете перенаправлены на экран подключения к устройству.

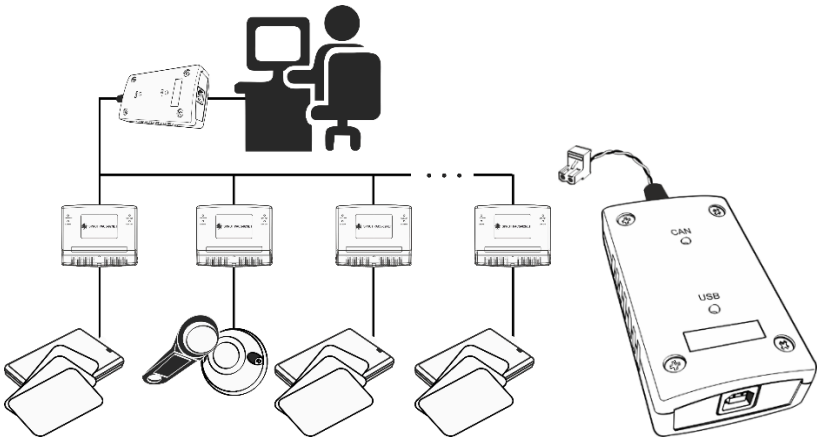


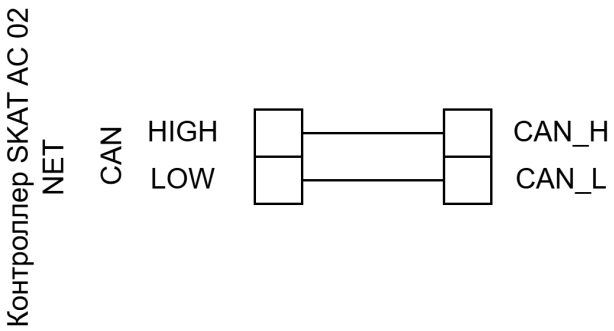
Настройка для работы в сетевом режиме, состав и принципы работы системы

В сетевом режиме использования контроллер подключается к серверному программному обеспечению СКУД посредством CAN-шины. Для перевода контроллера в сетевую тактику использования необходимо установить ПО «СКУД SKAT» на персональный компьютер и подключить контроллер доступа в общую CAN-линию всех устройств СКУД, или напрямую к персональному компьютеру через CAN-USB преобразователь (производитель – «БАСТИОН», в комплект поставки не входит). Для подключения к CAN-шине на контроллере есть специальный разъём «CAN». Переключение в сетевой режим работы и интеграция в ПО произойдут автоматически.

Все контроллеры собраны в последовательную двухпроводную CAN-сеть по витой паре и подключаются к серверу, где установлено десктопное WEB-приложение. WEB-приложение связывается с CAN сетью посредством USB-CAN преобразователя (адаптера). На компьютере работа с адаптером осуществляется как со стандартным HID-устройством.

При взаимодействие контроллера в сетевом режиме и получении новых ключей (например перетаскивание контроллера в новую зону) прошлые ключ, хранимые на устройстве, будут удалены. При необходимости предварительно создайте базу ключей с помощью ПО «СКУД Менеджер ключей».





Технические требования

Кроссплатформенное WEB-приложение СКУД SPRUT устанавливается на компьютеры пользователя под управлением операционных систем Windows или Unix (Ubuntu, Debian). Для работы системы на ПК должна быть установлена 64-битная лицензионная версия ОС семейства Microsoft Windows или ОС семейства Linux. Рекомендованы к использованию:

- Windows 10 (Pro, Home, Corporate Edition), но не ниже; (???)
- Ubuntu 22.04

После установки интерфейс программного обеспечения можно запустить на следующих браузерах:

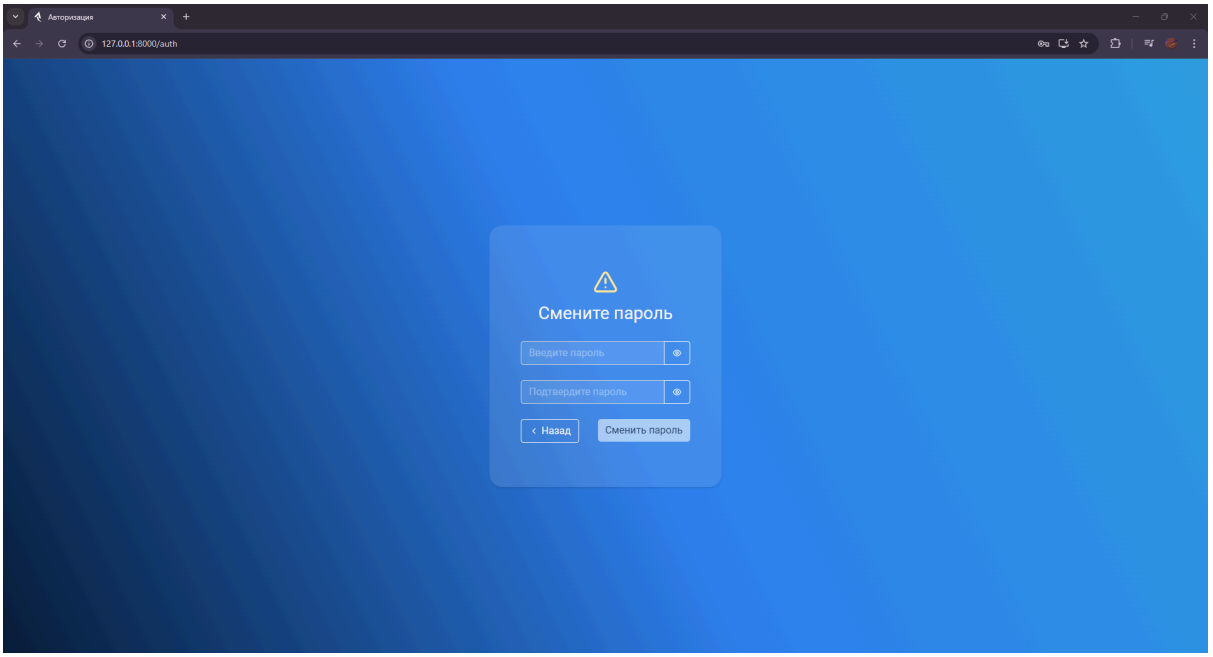
- Firefox (от 85.0.0 и выше)
- Google Chrome (от 90.0.0 и выше)
- Opera (от 75.0.0. и выше)
- Safari (от 14.1.2 и выше)
- Microsoft Edge (от 90 и выше)
- Яндекс браузер (от 21.11.2.773 и выше)

Версии браузеров должны быть датированы не ранее чем 1 января 2021 года. Корректная работа сайта на более ранних версиях указанных браузеров или на других браузерах не гарантируется. ПО работает в фоновом режиме для постоянного мониторинга сети, мониторинга событий и выполнения системных действий. В качестве базы данных используется SQLite. Работа приложения осуществляться на любых свободных, не занятых портах компьютера, на котором оно запущено. Например, порт по умолчанию для:

- клиентского web - интерфейса - 8080
- сервера web - приложения - 8081

Первая установка и запуск

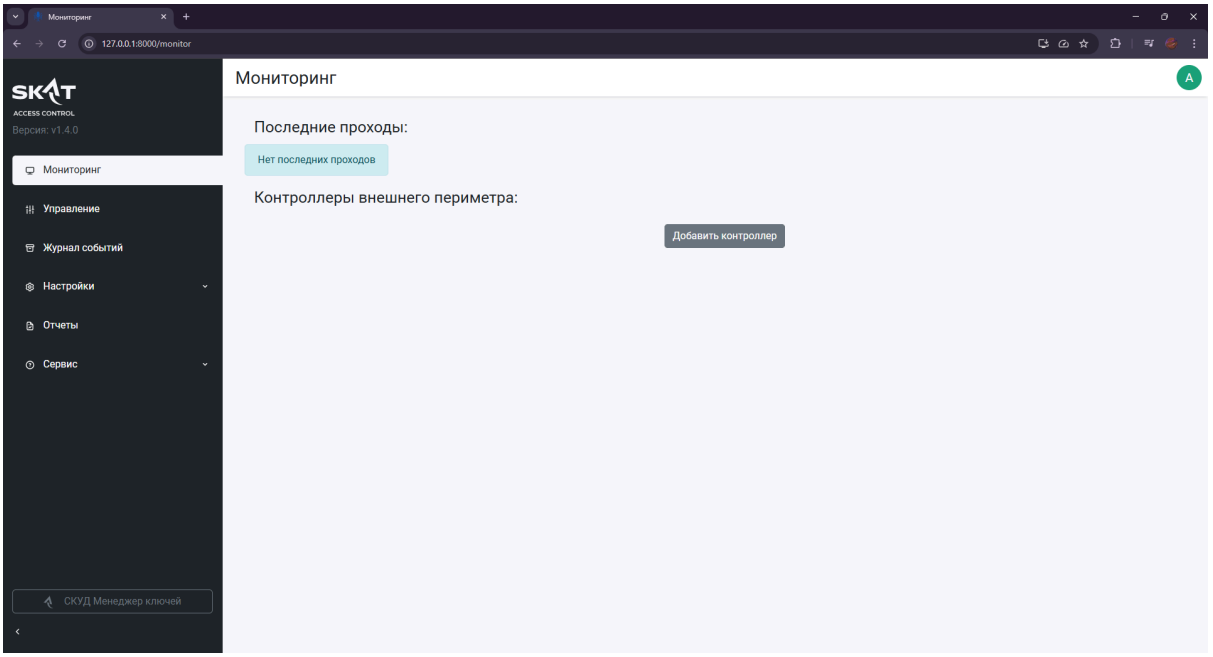
Установка приложения должна осуществляться в Windows системах при помощи инсталляционного файла, с включением автозапуска после старта системы. В графической оболочке рабочего стола необходимо создать ярлык для быстрого запуска интерфейса WEB-приложения, который откроет страницу браузера на нужном порте локального адреса, на котором запущено приложение.
Если клиент запускает систему в первый раз, то в качестве стартовой страницы приложения появится страница авторизации, иначе - страница Журнала событий (мониторинга). При физическом отсутствии БД (при первом запуске или удалении её вручную) создается пустая БД.
Для авторизации необходимо использовать доступ по логину и паролю. После инсталляции приложения в разделе меню Настройки необходимо создать аккаунт пользователя с правами “Администратор” со следующими данными для входа:
login: admin password: admin
После появиться окно с просьбой заменить пароль на более защищенный. Пароль обязательно должен быть более 8 символов. Содержать верхние и нижние регистры символов и хотя бы один спецсимвол и цифру. (На тестах поняли, что надо восемь символов, содержать буквы и цифры)
Разрешается вводить спецсимволы:) , (, & , !, @ , #



ВНИМАНИЕ! В дальнейшем, для обеспечения безопасности работы, стандартный пароль пользователя admin требуется изменить на пароль размером не менее 8 символов, включающий в себя буквы, цифры и символы в различных регистрах.
При последующих подключениях будет открываться вкладка мониторинга.

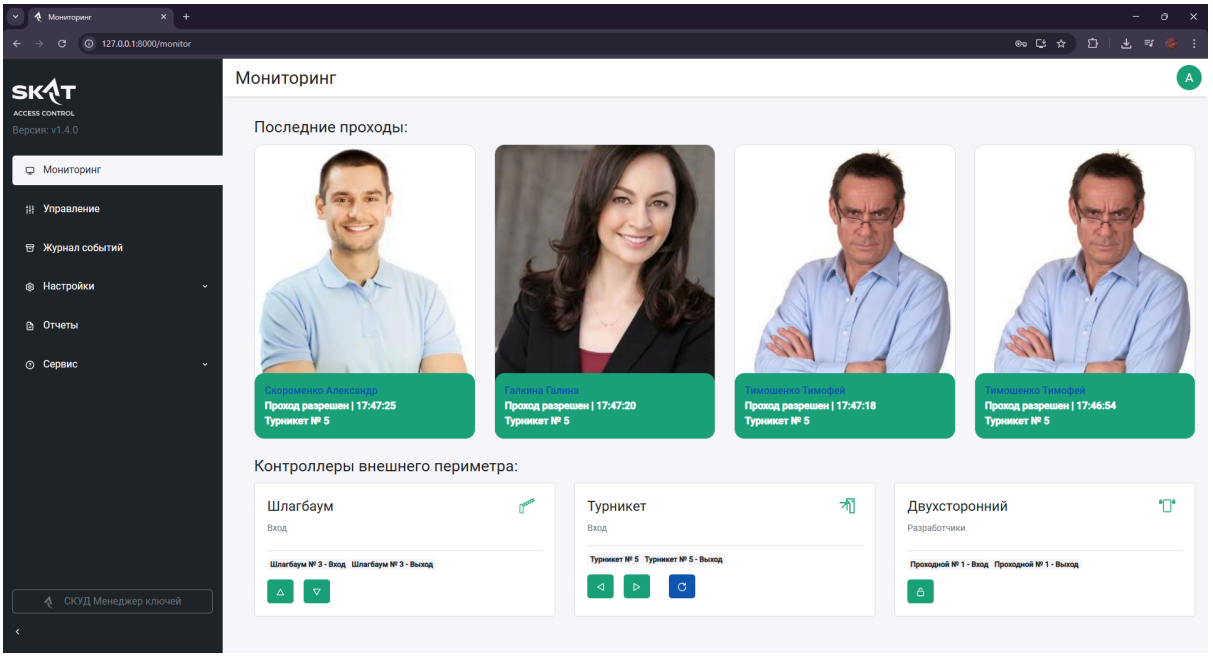
Главное окно и боковое меню

Интерфейс выполнен в темной цветовой гамме с использованием контрастных светлых элементов для обеспечения читаемости. Слева расположена вертикальная панель навигации, содержащая логотип системы и информацию о текущей версии. Ниже представлены пункты меню: «Мониторинг», «Управление», «Журнал событий», «Настройки», «Отчеты» и «Сервис». Пункт «Мониторинг» выделен белым фоном, что означает его активность. Пункты «Настройки» и «Сервис» имеют индикатор раскрывающегося списка. В нижней части бокового меню размещена кнопка «СКУД Менеджер ключей» с соответствующей иконкой.
В правом верхнем углу интерфейса расположен круглый зеленый значок с буквой «А», обозначающий авторизованного пользователя, в данном случае администратора. Общий вид интерфейса соответствует стандартам современных административных панелей, обеспечивая функциональность и наглядность для оператора, осуществляющего мониторинг и управление системой безопасности.



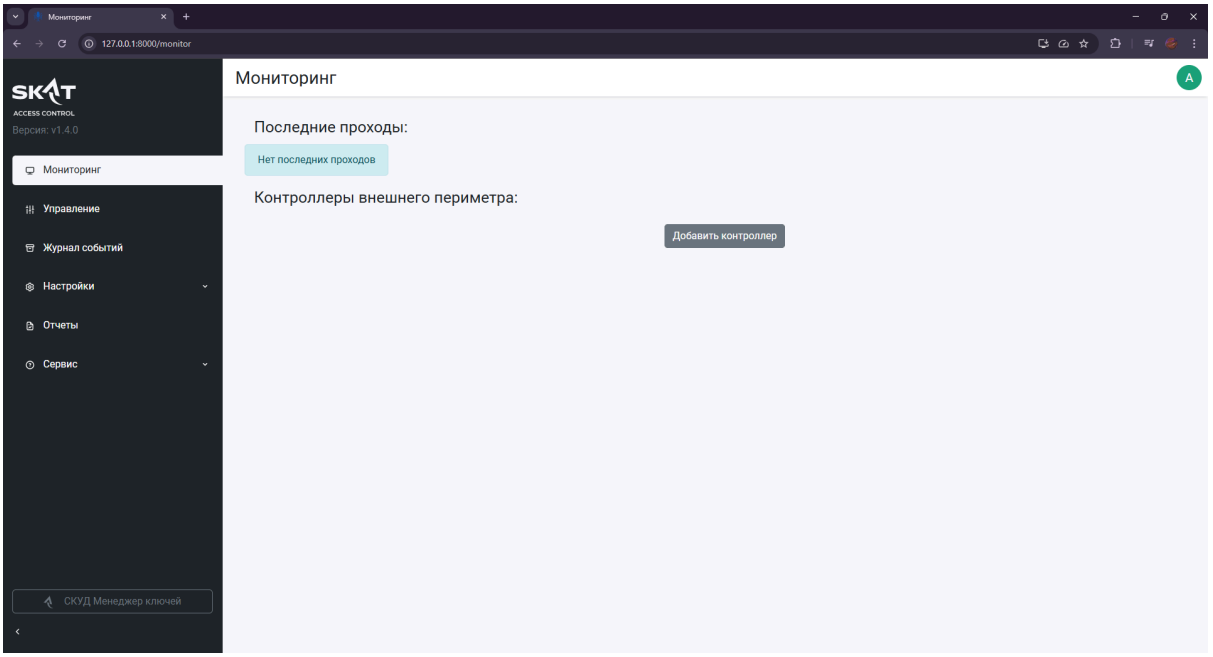
Вкладка Мониторинг

Заголовок раздела — «Мониторинг». Под ним расположен блок «Последние проходы», который на данном этапе заполнен информацией о четырех последних событиях. Каждое событие представлено в виде карточки, содержащей фотографию лица прошедшего, его полное имя и фамилию, отметку времени прохода и название зоны или устройства, через которое было осуществлено перемещение. Все четыре события зафиксированы через «Турникет № 5» и имеют статус «Проход разрешен». Отображенные персоны — Скороменко Александр, Галкина Галина и Тимошенко Тимофей — демонстрируют разнообразие типов пользователей, регистрируемых системой.



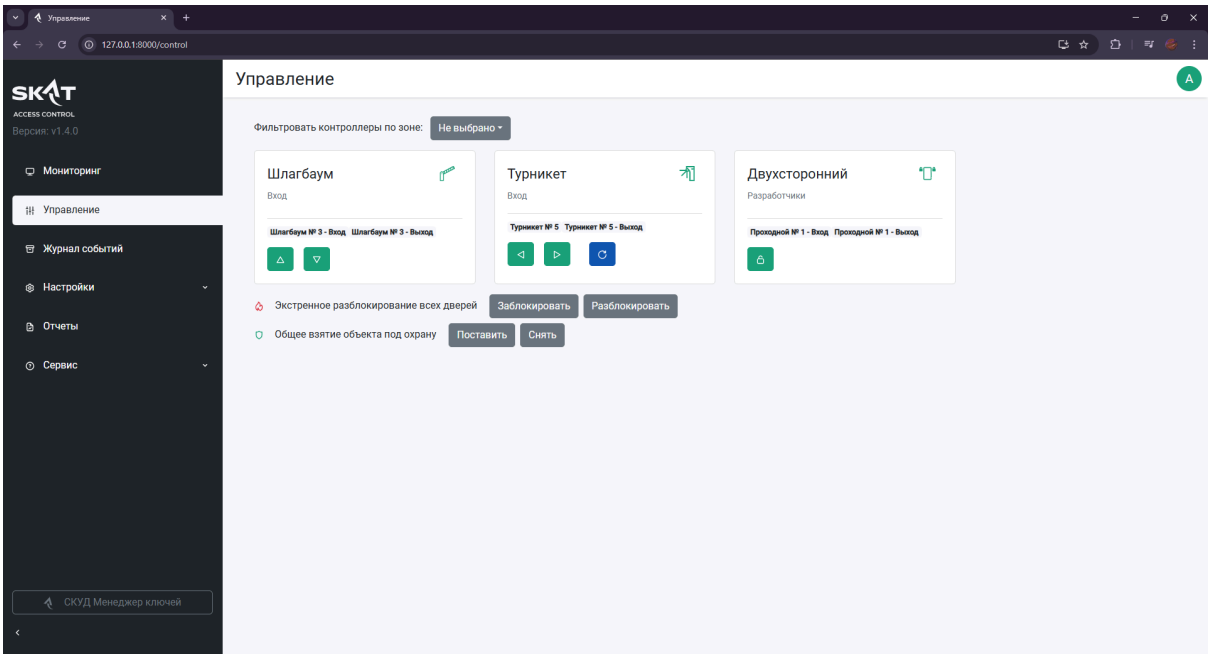
Ниже расположен раздел «Контроллеры внешнего периметра», представляющий собой панель управления устройствами. Здесь отображаются три карточки контроллеров: «Шлагбаум», «Турникет» и «Двухсторонний». Каждая карточка содержит название устройства, его зону (например, «Вход» или «Разработчики»), а также список связанных точек доступа. Для каждого контроллера предусмотрены интуитивно понятные кнопки управления: для «Шлагбаума» — стрелки вверх и вниз; для «Турникета» — стрелки влево и вправо, а также синяя кнопка с символом обновления; для «Двухстороннего» — зеленая кнопка с замком для блокировки или разблокировки. Иконки рядом с названиями устройств визуально кодируют их тип: шлагбаум, турникет и двухсторонний проходной пункт соответственно.

При первом запуске окно не будет содержать в себе никакой информации о проходах. Далее следует раздел «Контроллеры внешнего периметра», рядом с которым находится серая кнопка с надписью «Добавить контроллер», предназначенная для инициации процесса добавления отображения проходов с отмеченного контроллера .


Мониторинг
127.0.0.1:8000/monitor
SKAT
ACCESS CONTROL
Версия: v1.4.0
Мониторинг
Управление
Журнал событий
Настройки
Отчеты
Сервис
СКУД Менеджер ключей
Мониторинг
A
Последние проходы:
Нет последних проходов
Контроллеры внешнего периметра:
Добавить контроллер

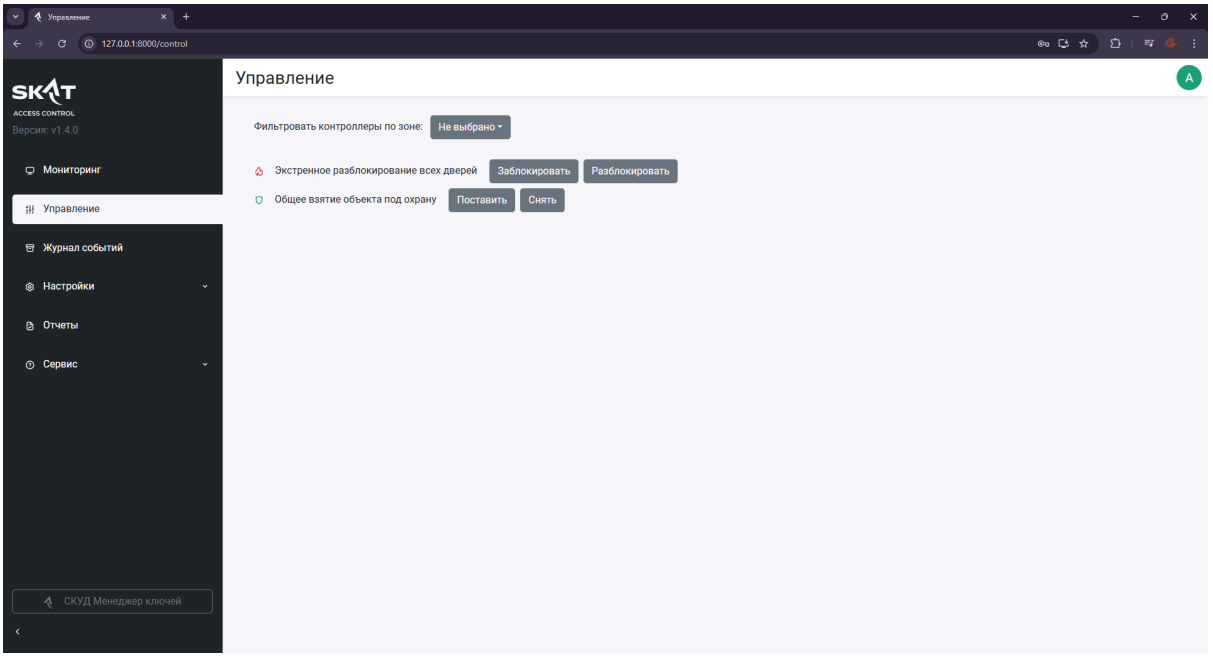
Вкладка Управление

В верхней части страницы, под заголовком «Управление», расположен элемент фильтрации — выпадающий список с надписью «Фильтровать контроллеры по зоне: Не выбрано», позволяющий администратору осуществлять выборочное отображение устройств в зависимости от их принадлежности к определенной охраняемой зоне.
Основное содержимое страницы структурировано в виде карточек, каждая из которых представляет тип устройства: «Двухсторонний», «Шлагбаум», «Двунаправленный» и «Турникет». Под названием каждого типа указана зона, в которой расположены контроллеры: «Нераспределенные контроллеры», что указывает на то, что данные устройства пока не привязаны к конкретным зонам или группам доступа. Внутри каждой карточки перечислены конкретные точки прохода и их названия (можно поменять в настройках контроллера): для «Шлагбаум № 3 - Вход» и «Шлагбаум № 3 - Выход»; «Турникет № 5 - Вход» и «Турникет № 5 - Выход»; «Проходной № 1 - Вход» и «Проходной № 1 - Выход». Такая структура отражает двунаправленный характер работы данных устройств. Для точек, которые не были сконфигурированы в настройках контроллера будет указано состояние «Без контроля направления». Подробнее о настройке можно прочитать пункт **Вкладка Настройки. Контроллеры и зоны.**
Под каждым списком точек доступа размещены кнопки управления, соответствующие типу устройства: для «Двухстороннего» — зеленая кнопка с символом замка для блокировки прохода; для «Шлагбаума» — две зеленые кнопки со стрелками вверх и вниз, предназначенные для ручного управления подъемом и опусканием шлагбаума; для «Турникета» — три кнопки: зеленая со стрелкой влево, зеленая со стрелкой вправо и синяя с символом обновления для функции прохода группы лиц **(опускание соленоида, антипаника)**.
Ниже основных карточек расположены две глобальные функциональные группы. Первая — «Экстренное разблокирование всех дверей» — сопровождается красной иконкой и двумя серыми кнопками «Заблокировать» и «Разблокировать», предназначенными для активации аварийного режима безопасности. Вторая — «Общее взятие объекта под охрану» — с зеленой иконкой щита и кнопками «Поставить» и «Снять», обеспечивающими управление общим режимом охраны объекта. При повреждении охранного шлейфа и нажатии на кнопку «Поставить» в журнале событий будет показано событие с ошибкой - «Ошибка постановки на охрану».



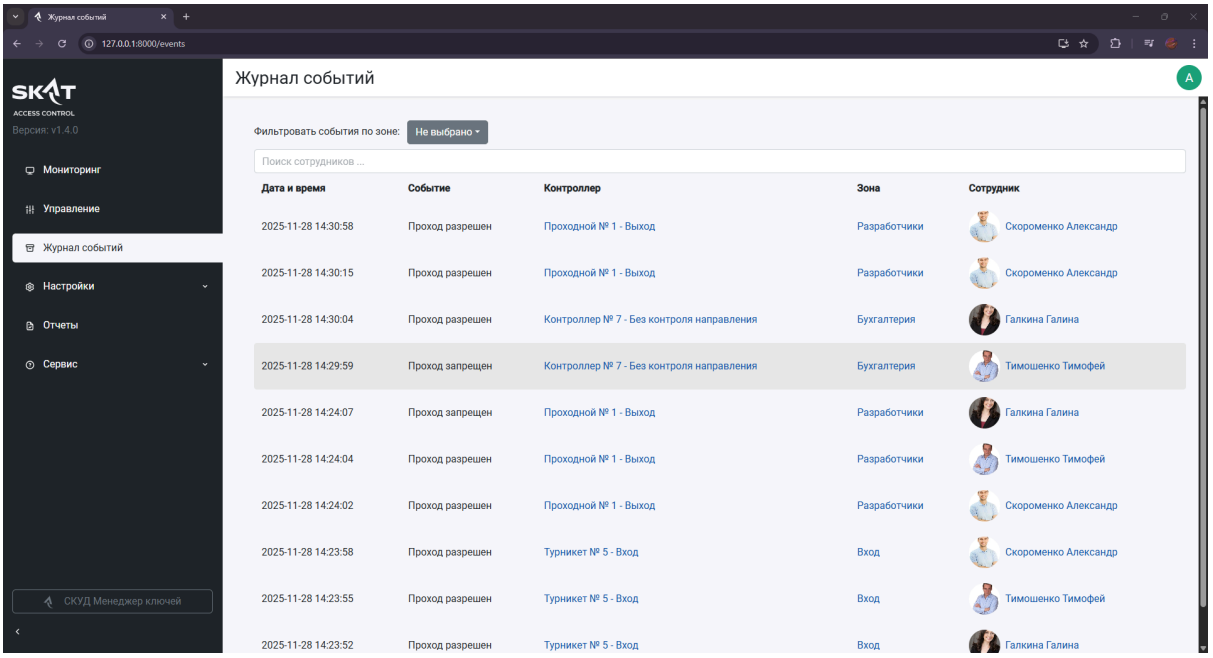
При первом запуске при условии, что контроллеры не подключены в систему или происходит

настройка контролеры не будут отображаться в системе. Обеспечивать удаленный контроль способны контроллеры SKAT AC 02NET PACS.



Вкладка Журнал событий

В верхней части страницы, под заголовком «Журнал событий», расположен функциональный блок фильтрации. Он включает выпадающий список «Фильтровать события по зоне: Не выбрано», позволяющий администратору осуществлять выборочное отображение записей в зависимости от принадлежности к определенной охраняемой зоне. Непосредственно под ним размещена строка поиска с подсказкой «Поиск сотрудников...», предназначенная для быстрого поиска конкретных пользователей по имени или фамилии в исторических данных.
Основное содержимое страницы представляет собой таблицу с хронологически упорядоченными записями событий. Таблица структурирована по следующим столбцам: «Дата и время», «Событие», «Контроллер», «Зона» и «Сотрудник». Каждая строка таблицы соответствует одному зафиксированному событию и содержит полную информацию о нем. В столбце «Дата и время» указаны точные отметки времени в формате YYYY-MM-DD HH:MM:SS. В столбце «Событие» отражается тип действия — «Проход разрешен» или «Проход запрещен». Столбец «Контроллер» указывает на конкретное устройство, через которое было совершено действие, например, «Проходной № 1 - Выход» или «Турникет № 5 - Вход». Столбец «Зона» обозначает зону, к которому относится контроллер — такие как «Разработчики», «Бухгалтерия» или «Вход». В последнем столбце «Сотрудник» приводится полное имя и фамилия пользователя, а также его аватар, что обеспечивает визуальную идентификацию лица, совершившего проход.

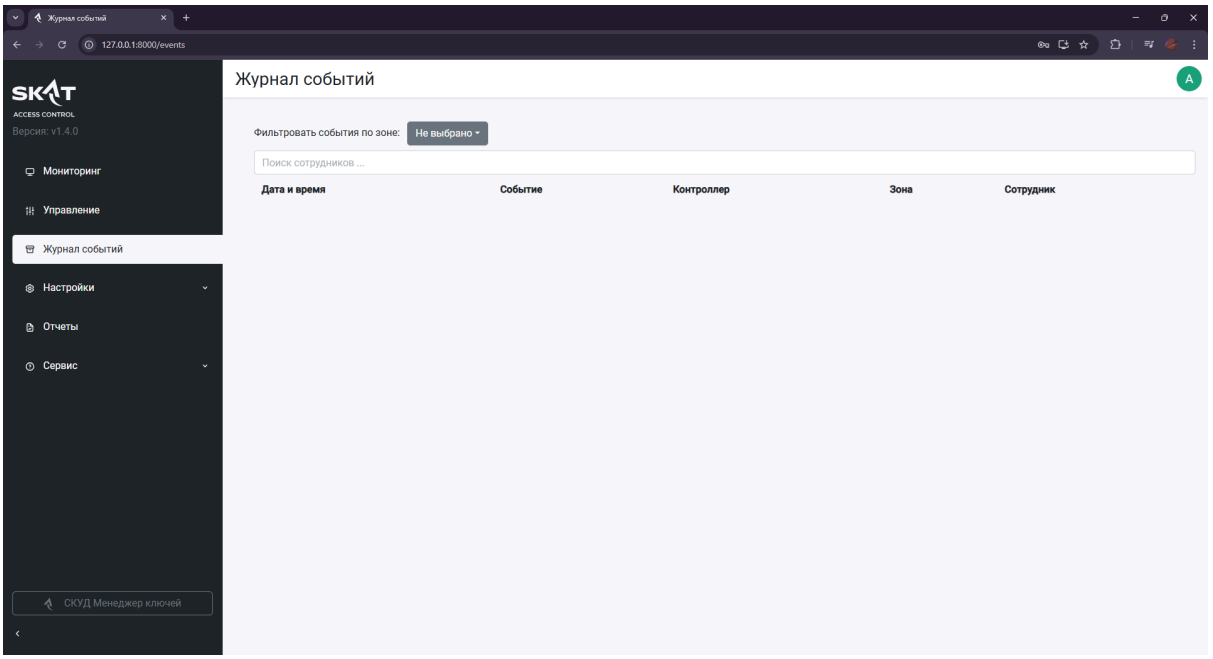


Типы возможных событий:

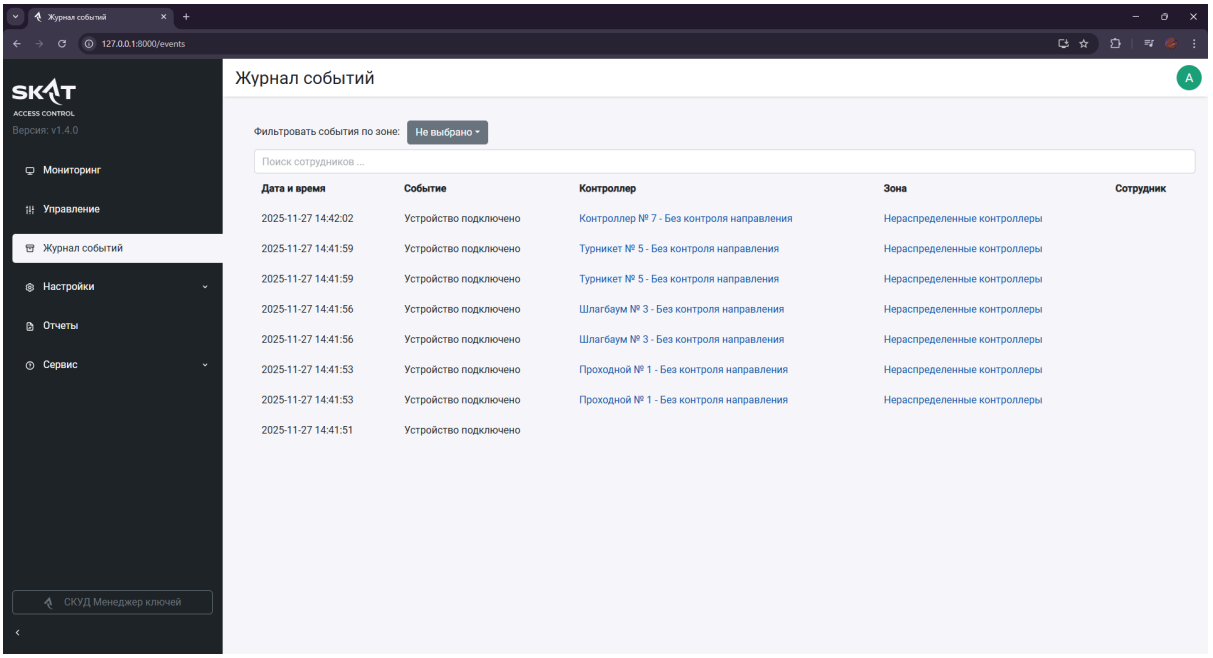
1. Проход запрещён
2. Проход разрешён
3. Локальное (с использованием МАСТЕР-ключа) добавление нового ключа
4. Локальное (с использованием МАСТЕР-ключа) удаление сохранённого ключа
5. Локальное (по ключу) снятие с охраны
6. Локальная (по ключу) постановка на охрану
7. Ошибка постановки на охрану (шлейф нарушен)
8. Нарушение периметра (сработавший шлейф охраны, только для устройств, поставленных на охрану)
9. Удаленное (по команде) снятие с охраны
10. Удалённая (по команде) постановка на охрану
11. Режим “ПОЖАРНАЯ ТРЕВОГА” установлен
12. Режим “ПОЖАРНАЯ ТРЕВОГА” снят

13. Выход по кнопке запрещён
14. Выход по кнопке разрешён

При первом запуске Журнал событий будет пустым и не будет отображать события.

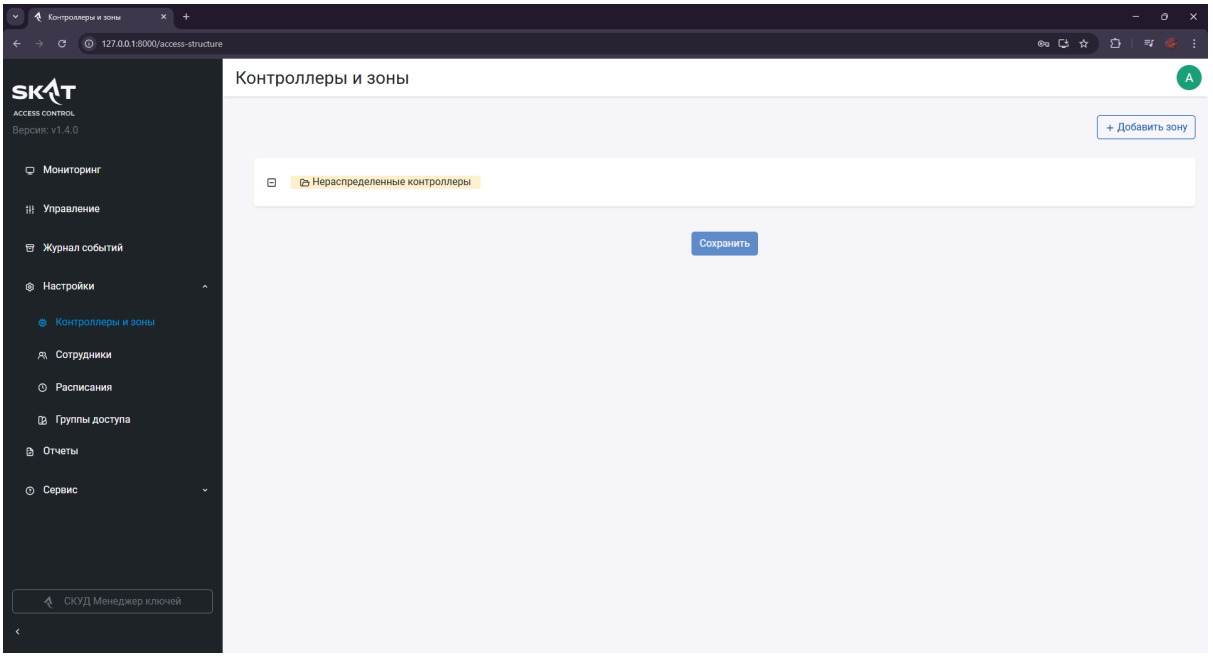


По мере подключения контроллеров и нахождения их в сети будут появляться уведомления о подключении.

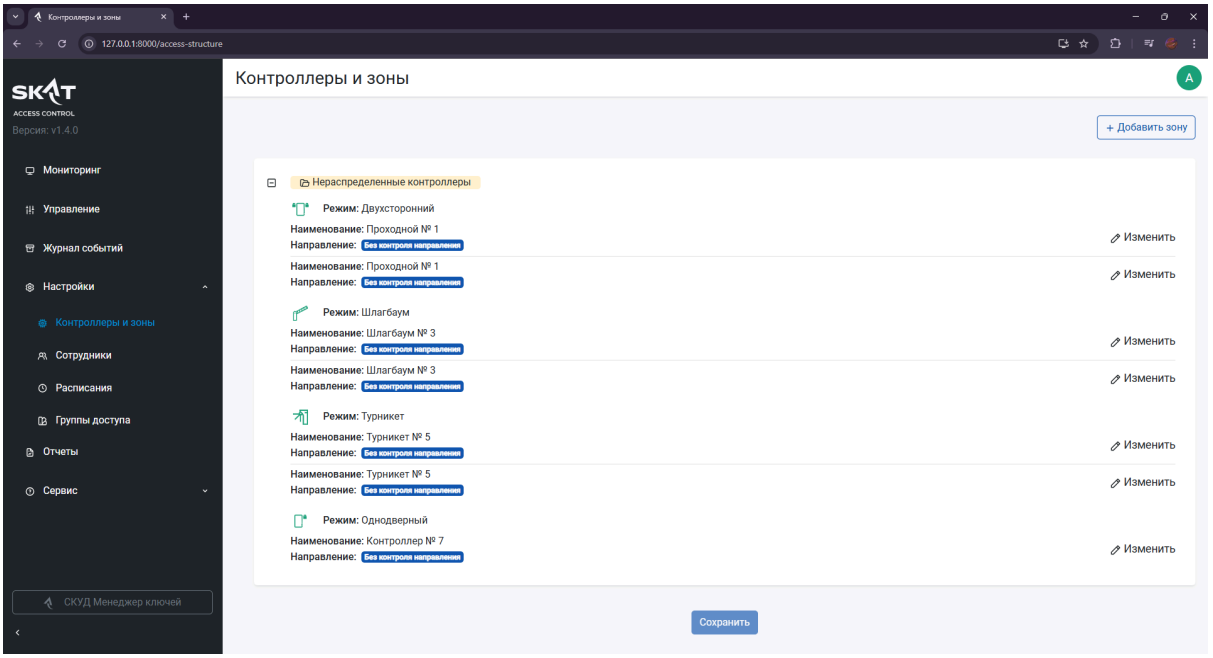


Вкладка Настройки. Контроллеры и зоны

При первом запуске в системе не будет не отображать ни одного контроллера.

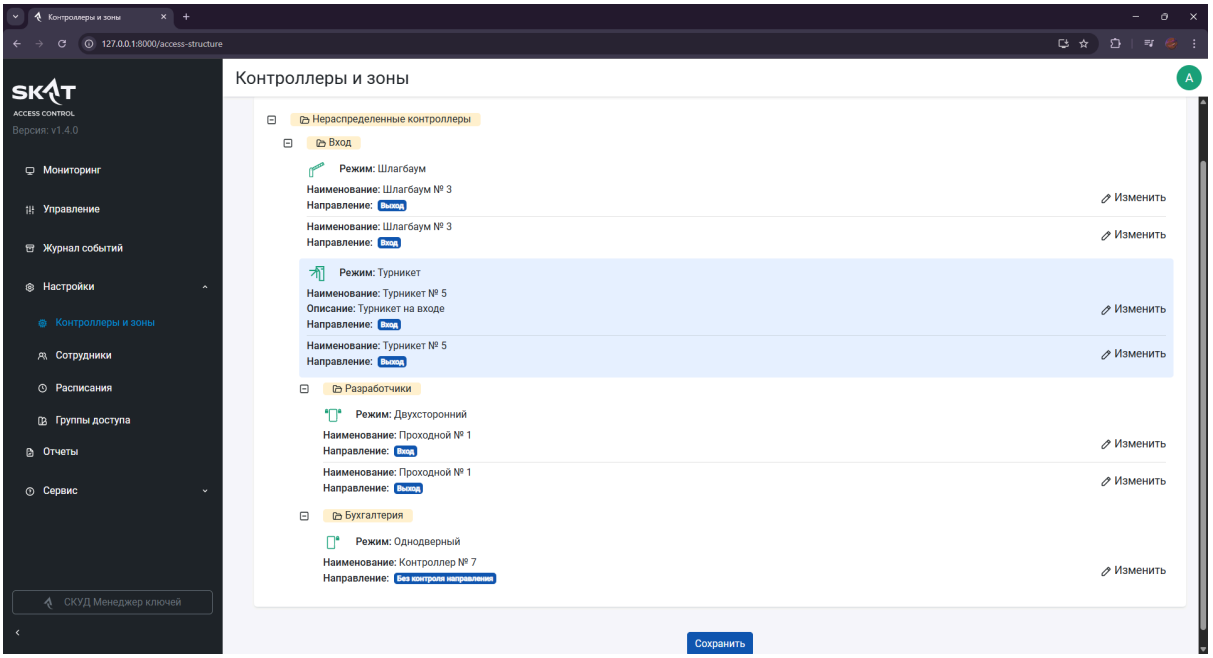


Все найденные в системе контроллеры будут находиться в зоне нераспределенных при первом подключении. Необходимо перенести контроллеры в новую зону. Ее можно создать при помощи кнопки добавить в зону. Контроллеры, находящиеся в зоне нераспределенных не будут обновляться и получать ключи доступа сотрудников.



В верхней части страницы, под заголовком «Контроллеры и зоны», расположен блок с заголовком «Нераспределенные контроллеры», выделенный светло-желтым фоном, что указывает на наличие устройств, не назначенных ни одной из существующих зон. Ниже следует структурированный список, организованный по принципу иерархической группировки: каждая зона представлена в виде раскрывающегося элемента с соответствующим названием — «Вход», «Разработчики», «Бухгалтерия» — и содержит перечень контроллеров, привязанных к данной зоне.

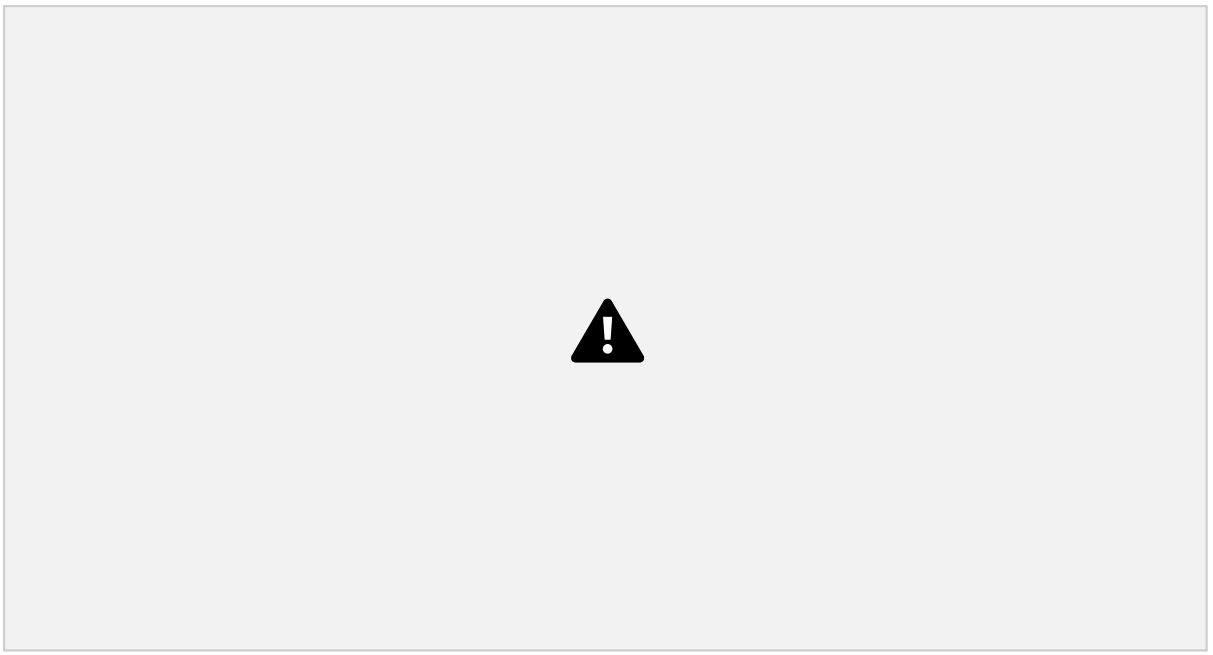
Внутри каждой зоны размещены карточки контроллеров, каждая из которых содержит иконку, визуально кодирующую тип устройства — шлагбаум, турникет или проходной пункт. Зеленый цвет иконки указывает на то, что контроллер находиться в сети и функционирует. Серым будут отмечаться контроллеры выключенные из сети или по каким-то причинам потерявшим связь с ПО. Для каждого контроллера указан режим работы — «Шлагбаум», «Турникет» или «Однодверный» — а также его уникальное наименование, например, «Шлагбаум № 3», «Турникет № 5» или «Проходной № 1». В случае турникета дополнительно присутствует поле «Описание», содержащее уточняющую информацию — «Турникет на входе». Каждая запись также содержит указание направления функционирования устройства — «Вход», «Выход» или «Без контроля направления» — что определяет его роль в системе управления перемещениями.
Справа от каждой записи контроллера расположена ссылка «Изменить» с иконкой карандаша, предназначенная для редактирования его параметров. Кнопка изменить находиться напротив каждой из точек прохода для контроллеров имеющих подключения двух считывателей. Первый по счету относится к считывателю, подключенному к клеммам Channel 1, второй соответственно к Channel 2. В нижней части страницы размещена кнопка «Сохранить», выполненная в синем цвете, предназначенная для фиксации всех внесенных изменений в структуре зон и конфигурации контроллеров.



Пример архивации контроллера

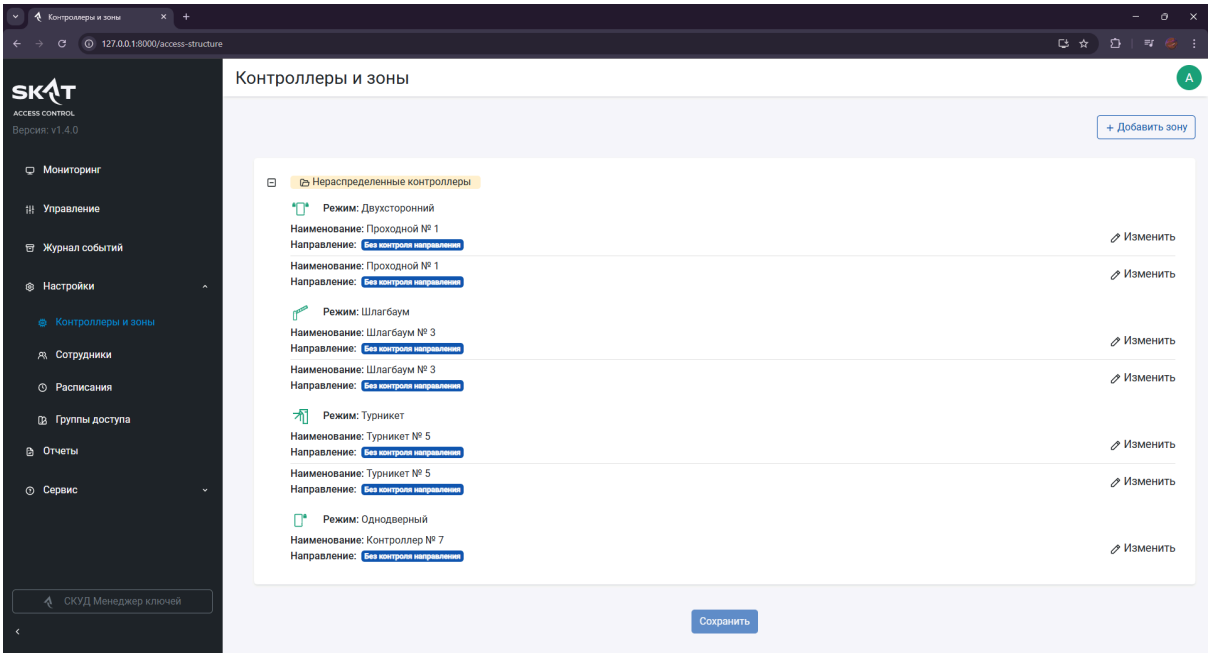
При необходимости, контроллеры, которые вышли из строя можно добавить в скрытые. Помните, что контроллер, не имеющий связи с сетью имеет серую иконку. Можно скрыть только неактивный контроллер. Курсор мыши наведите на первую запись в секции «Нераспределенные контроллеры», которая относится к устройству типа «Двухдверный» с наименованием «Двухдверный № 8» и направлением «Без контроля направления».
Рекомендуется все неактивные контроллеры перемещать в зону нераспределенных контроллеров.
Нажмите на ссылку «Изменить», расположенную в правой части строки записи.
После нажатия ссылки система, открывает модальное окно редактирования, что является стандартной процедурой для изменения параметров устройства. Это действие позволяет администратору скорректировать такие атрибуты, как наименование, описание, режим работы или направление прохода, а также привязать устройство к конкретной зоне безопасности.
Одним из важных элементов управления, доступных в процессе редактирования, является

переключатель типа toggle с меткой «Скрыть везде». Активация данного переключателя приводит к тому, что устройство исключается из основного представления списка контроллеров и перемещается в специальную плашку, расположенную в верхней части экрана, которая служит временным хранилищем для скрытых устройств. Это позволяет оператору управлять видимостью оборудования без его физического удаления или переноса в другую зону, что особенно полезно при проведении технического обслуживания или тестирования.
Для восстановления видимости скрытого контроллера достаточно кликнуть по указанной плашке, после чего список скрытых устройств будет развернут, и контроллер «Двухдверный № 8» снова станет доступным для просмотра и взаимодействия. При необходимости возврата устройства в исходное состояние — то есть в категорию «Нераспределенные контроллеры» — пользователю следует воспользоваться кнопкой закрытия, обозначенной символом крестика, расположенной рядом с записью о скрытом устройстве. Нажатие этой кнопки инициирует процесс возвращения контроллера в секцию где когда-то располагался контроллер, тем самым восстанавливая его первоначальное положение в системе и делая его доступным для последующего назначения в любую зону или для дальнейшей настройки.

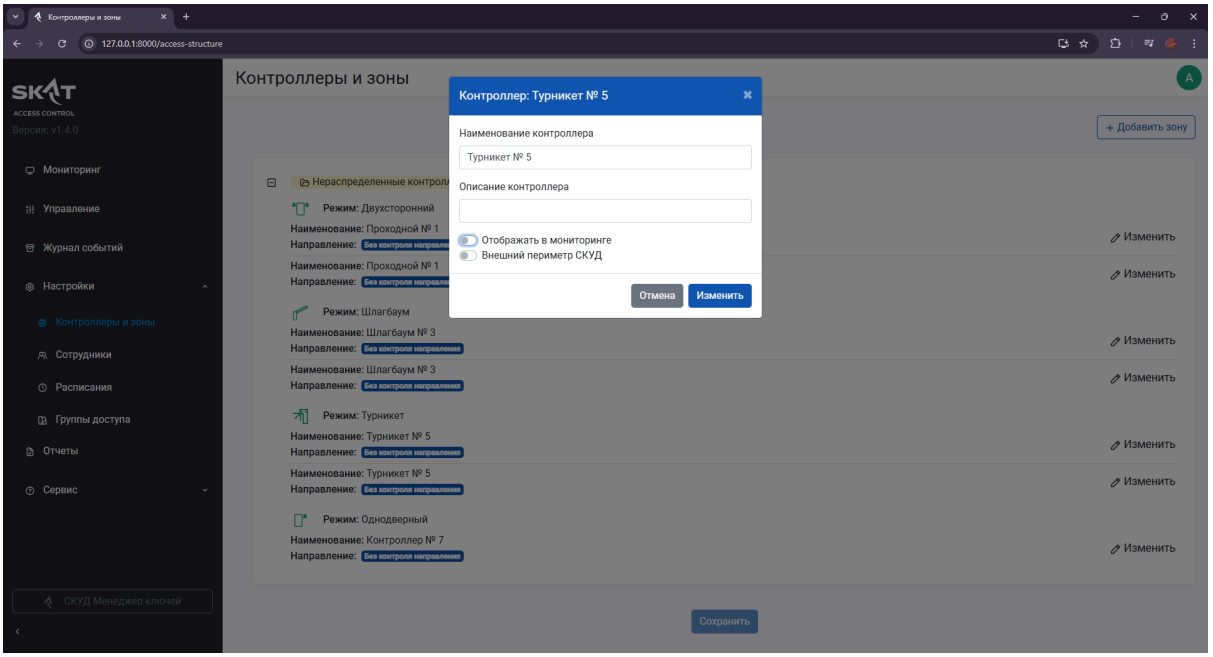


Пример пошаговой настройки контроллеров

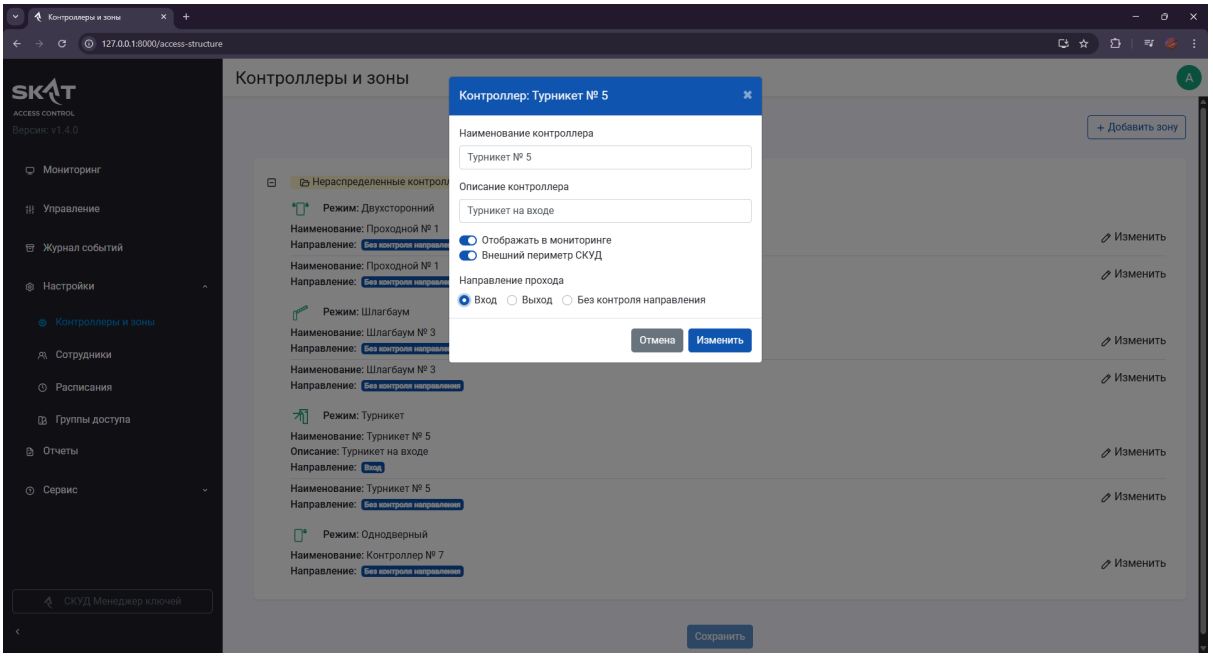
При первом подключении и пока контролеры не будут перераспределены находятся в зоне Нераспределенные контроллеры.



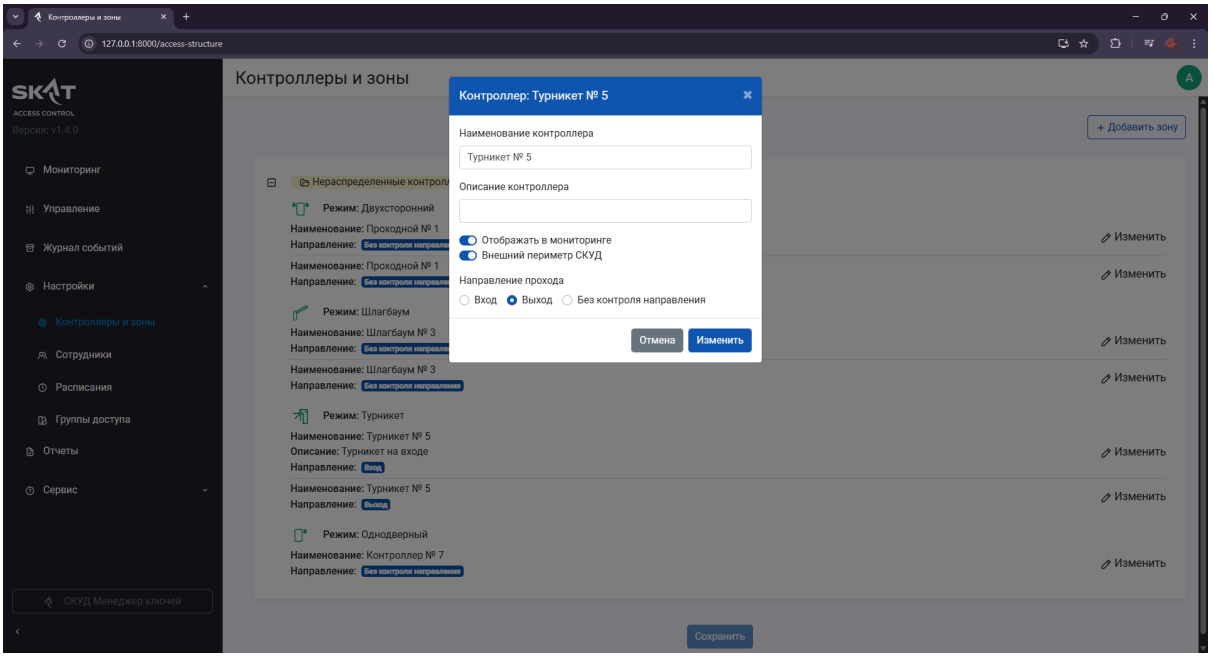
Нажмите на кнопку изменить, напротив направления, чтобы сконфигурировать и настроить контроллер. Напоминаем, что кнопка изменить находиться напротив каждой из точек прохода для контроллеров имеющих подключения двух считывателей. Первый по счету относится к считывателю, подключенному к клеммам Channel 1, второй соответственно к Channel 2
Обратите внимание, что Первое поле — «Наименование контроллера» — содержит текущее название устройства, которое может быть изменено пользователем. Второе поле — «Описание контроллера» — представляет собой пустое текстовое поле, предназначенное для внесения дополнительной информации, поясняющей назначение или особенности данного контроллера.
(Примечание) Для корректного формирования отчета необходимо отметить контроллер, который контролирует проход через внешний периметр. На вкладке Настройки. Контроллеры и зоны выберите необходимый контроллер, отметь его как проход внешнего периметра. Если это один контроллер, то настройте его каналы на вход и выход. Если два разных контроллера, отметьте каждый из них как главный проход и по необходимости отметь один как вход, а другой как выход. Остальным контроллерам нет необходимости настраивать каналы и конфигурировать их как выходы и входы. Могут остаться без контроля направления.
Ниже этих полей размещены два переключателя типа toggle. Первый — «Отображать в мониторинге» — позволяет определить, будет ли данный контроллер отображаться в режиме реального времени на главной странице мониторинга событий. Второй — «Внешний периметр СКУД» — служит для маркировки устройства как элемента внешнего охранного периметра, что влияет на его алгоритмы обработки событий. При переключении будет доступен блок выбора направления прохода, содержащий три радиокнопки: «Вход», «Выход» и «Без контроля направления».



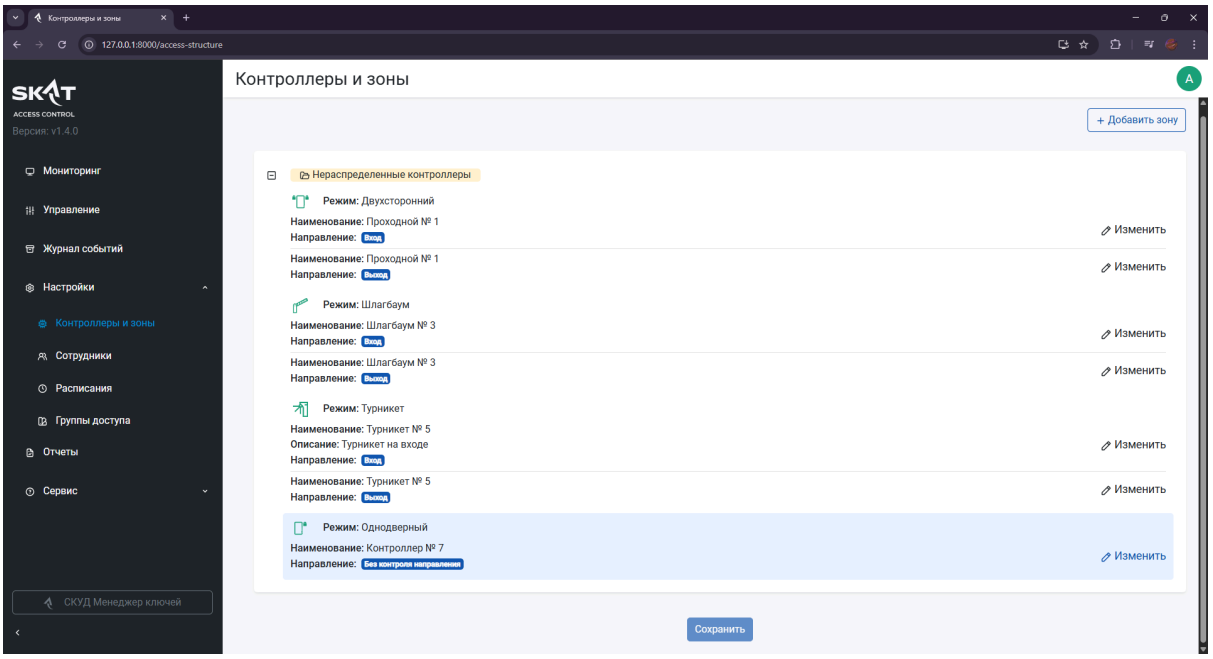
После полной настройки окно будет выглядеть следующим образом. Заполнены поля Описание, что указывает на расположение турникета. Проходы через этот контроллер будут отображаться в мониторинге, а выбранный канал сконфигурирован как вход.



Проделываем подобную операцию для второго направления. В этот раз выбираем после включения переключателя Внешний периметр СКУД радиокнопку выход, конфигурируя эту точку прохода как выход.

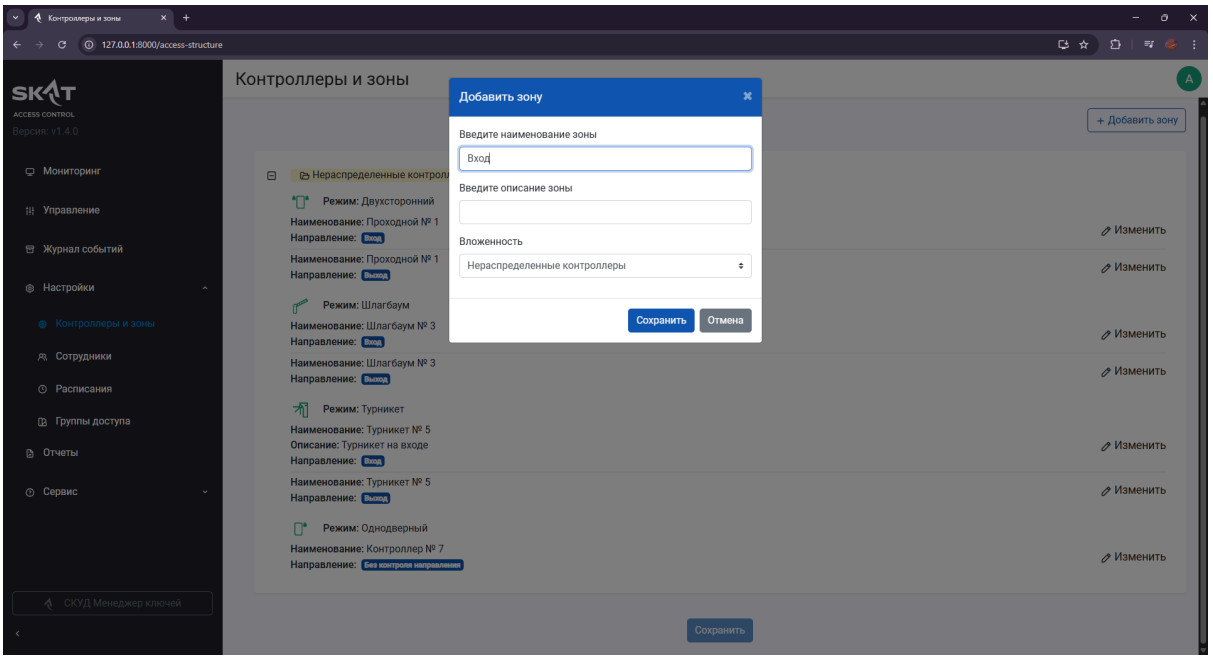


Аналогично конфигурируем и остальные контроллеры, оставшиеся в зоне нераспределенных контроллеров. Итого получается система, состоящая из 4 контроллеров со своими настройками входа и выхода, отображением необходимых в мониторинге, описаниями и названиями. Теперь необходимо распределить их по логическим зонам.

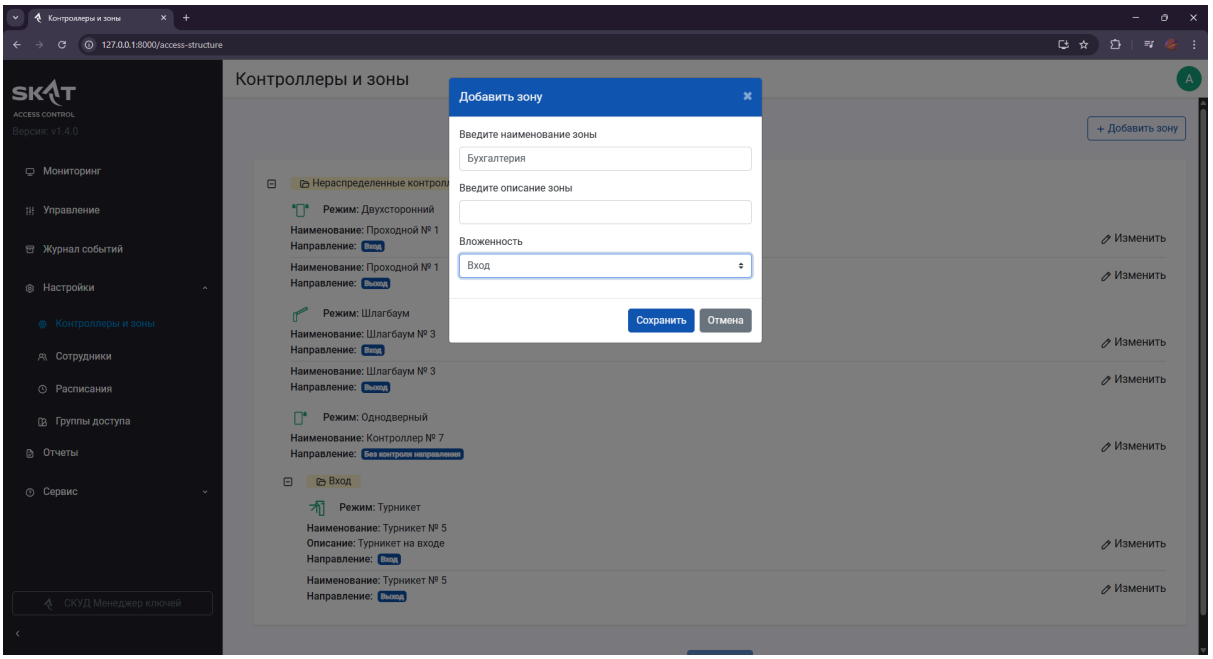


Далее необходимо создать зону для перемещения в нее контроллеров. Для этого нажмите на кнопку добавить зону в верхнем углу экрана. Заголовок окна четко обозначает выполняемую операцию — добавление новой структурной единицы. Ниже расположен блок полей для ввода информации о создаваемой зоне. Первое поле — «Введите наименование зоны» — содержит текст «Вход», что указывает на назначение или функциональную роль данной зоны в системе. Второе поле — «Введите описание зоны» — является пустым и предназначено для внесения дополнительных пояснений, характеризующих зону более подробно.
Ниже этих полей находится элемент управления — выпадающий список с меткой «Вложенность». В текущий момент выбрано значение «Нераспределенные контроллеры», что означает, что новая зона будет создана на верхнем уровне иерархии, без привязки к

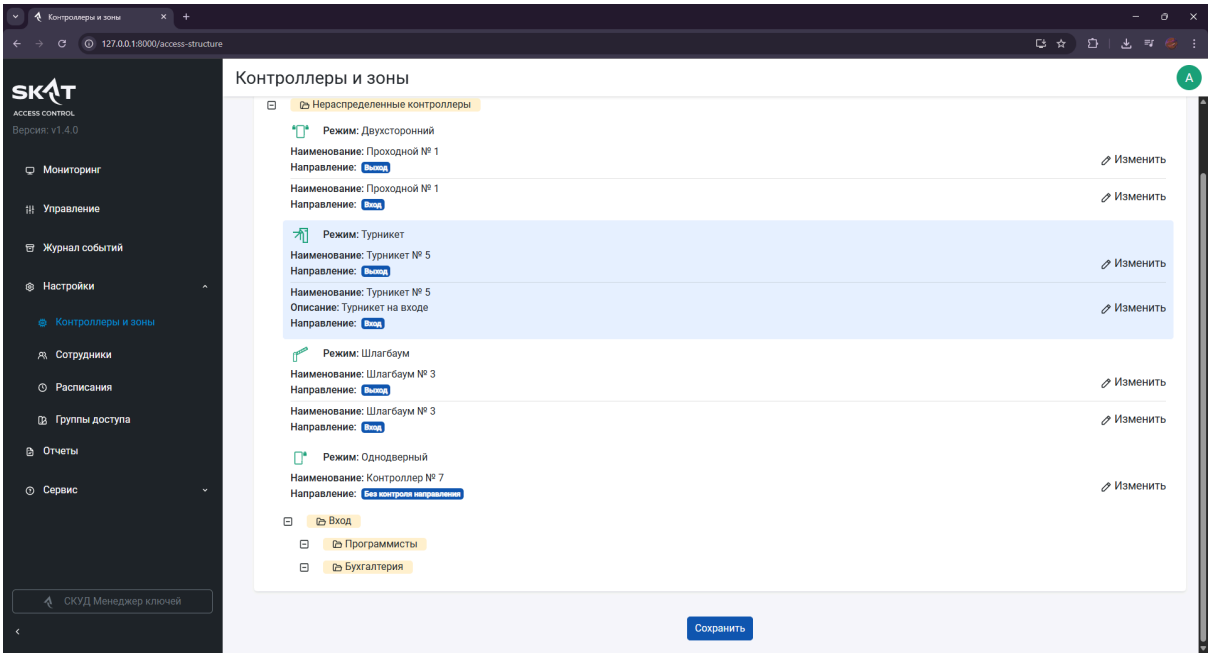
существующим родительским зонам. Этот параметр позволяет гибко строить многоуровневую структуру зон, соответствующую физической или организационной архитектуре объекта.
В нижней части модального окна размещены две кнопки управления: «Сохранить», выполненная в синем цвете, которая фиксирует введенные данные и создает новую зону в системе, и «Отмена», выполненная в сером цвете, предназначенная для закрытия окна без сохранения изменений и возврата к предыдущему состоянию интерфейса. Нажимаем кнопку «Сохранить».



Аналогичным образом создадим новую зону, только теперь становиться доступным выбор созданной ранее зоны - Вход. Нажмем кнопку сохранить.

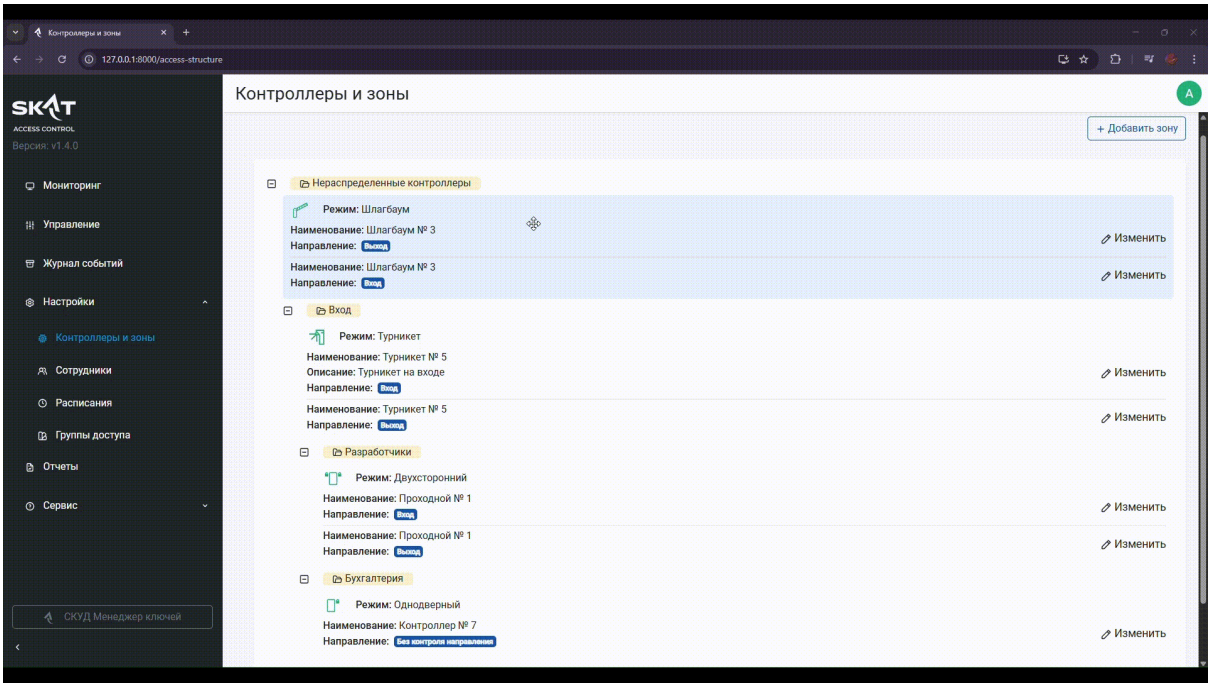


Тогда контроллеры будут выглядеть следующим образом.



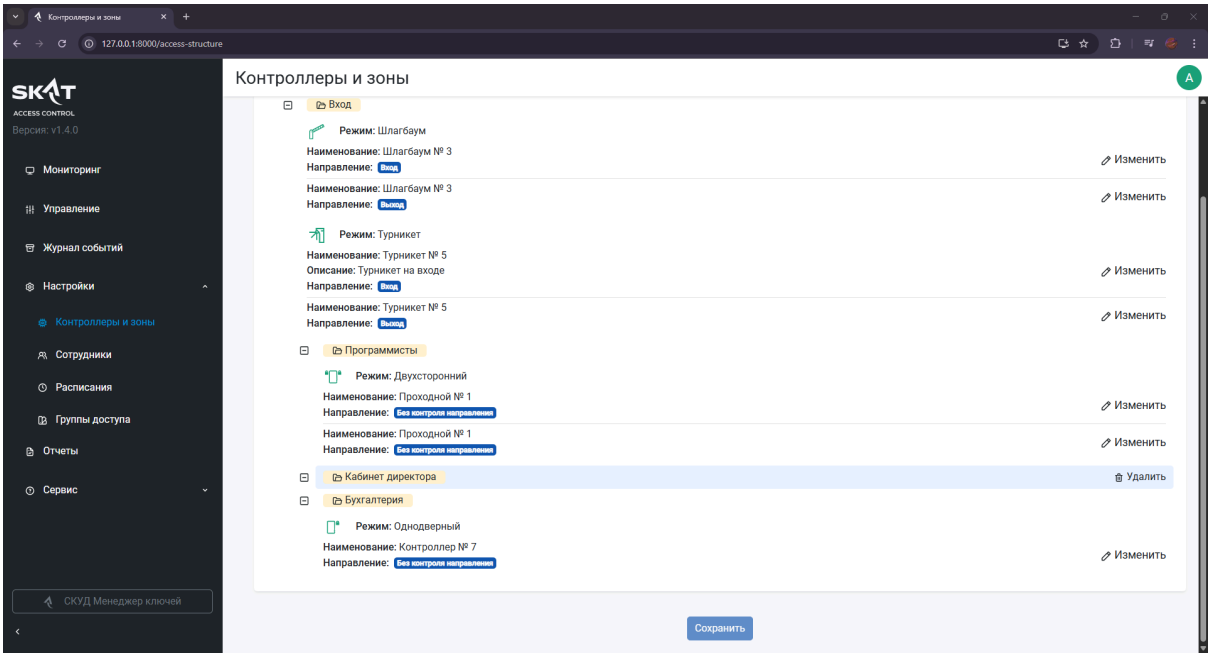
Следующим шагом распределим контроллеры по логическим зонам. В начальный момент времени на экране отображается список устройств, сгруппированных по зонам: «Вход», «Разработчики» и «Бухгалтерия». В верхней части списка выделена секция «Нераспределенные контроллеры», содержащая устройство типа «Шлагбаум № 3» — одно с направлением «Вход», другое — «Выход». Пользователь инициирует действие по перетаскиванию первого устройства — «Шлагбаум № 3» с направлением «Вход» — из этой секции в группу «Вход».

В ходе выполнения операции курсор мыши перемещает карточку устройства к целевой зоне. Для этого зажмите левую кнопку мыши. При достижении границы группы «Вход» происходит визуальное подтверждение действия — контур зоны слегка подсвечивается, указывая на возможность размещения элемента. Отпустите левую кнопку мыши. После того как устройство помещено в новую группу, оно исчезает из секции «Нераспределенные контроллеры» и появляется в составе зоны «Вход», занимая соответствующее место в иерархическом списке. Данная операция является стандартной процедурой конфигурирования системы контроля доступа, позволяющей администратору структурировать физические точки доступа по логическим зонам безопасности. Это обеспечивает точное соответствие между архитектурой объекта и функциональными возможностями системы, что является необходимым условием для корректного управления доступом и формирования отчетности.



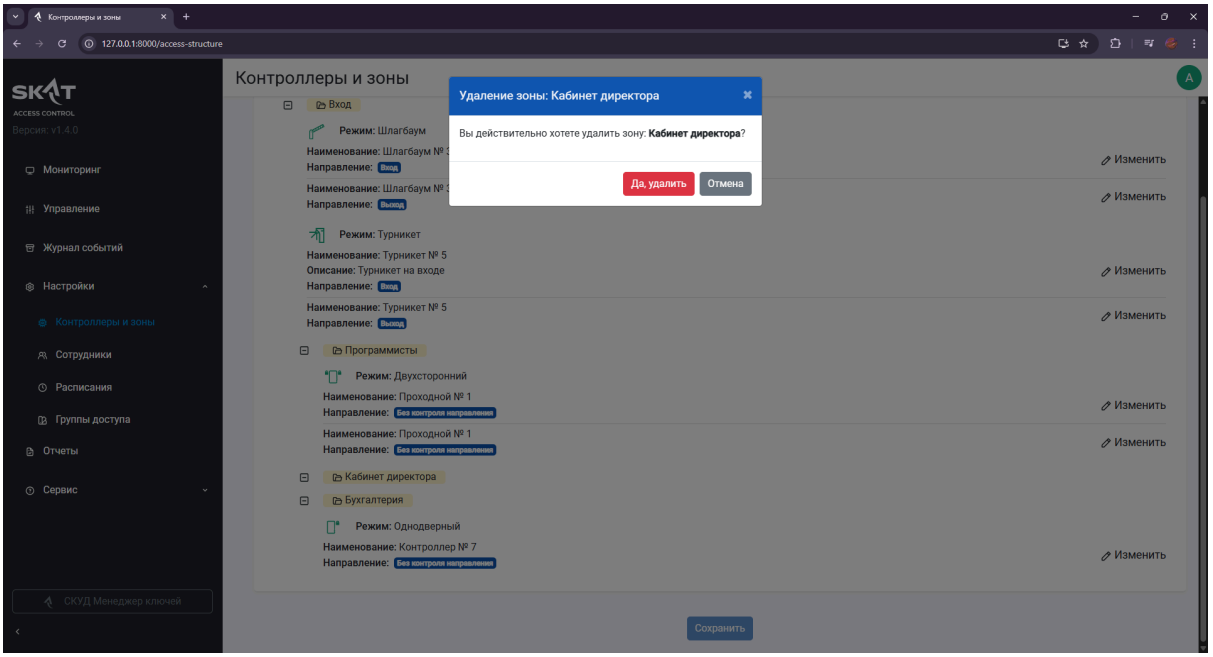
Пример удаления зоны

Основное содержимое страницы представляет собой иерархический список, организованный по принципу группировки устройств по зонам. В верхней части списка находится секция «Нераспределенные контроллеры», выделенная светло-желтым фоном, что указывает на наличие устройств, не назначенных ни одной из существующих зон. Ниже следует структурированный список зон: «Вход», «Программисты», «Кабинет директора» и «Бухгалтерия». Каждая зона содержит перечень контроллеров, привязанных к данной зоне. Для удаления зоны обязательно перенести из нее все контроллеры, зона должна остаться пустой. При наведении на зону будет расположена ссылка «Удалить».

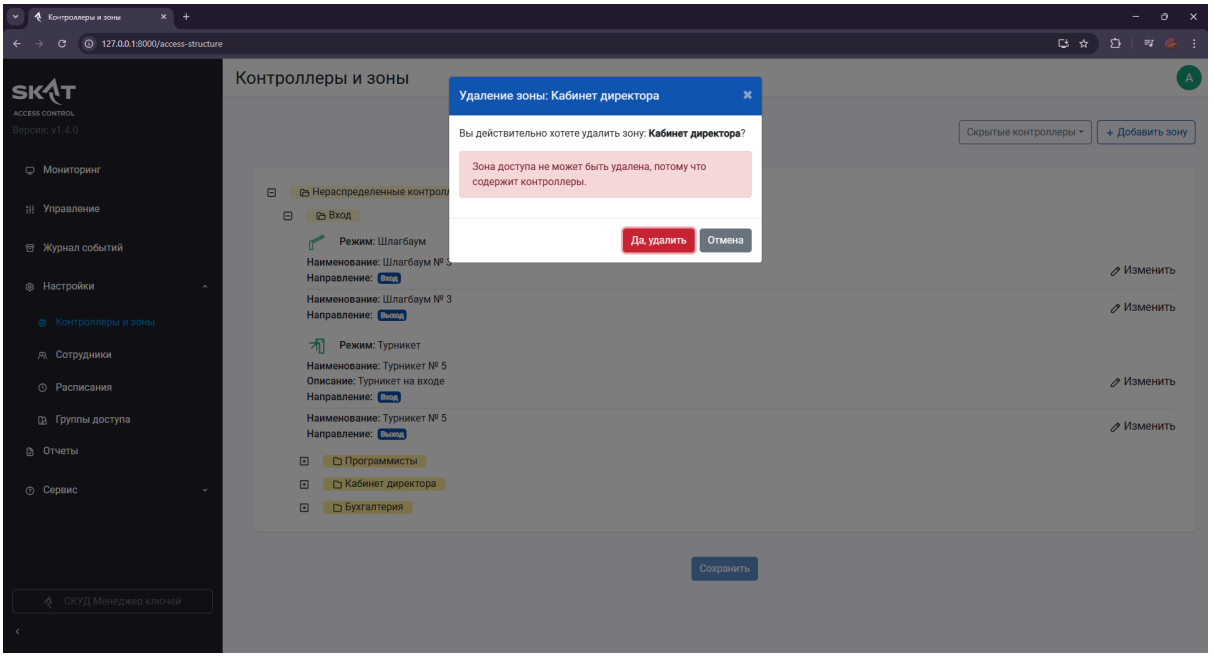


Центральным элементом экрана является модальное окно с заголовком «Удаление зоны: Кабинет директора», которое активировано после инициации операции по удалению логической зоны безопасности.

Заголовок модального окна четко определяет выполняемую операцию — удаление зоны с наименованием «Кабинет директора». Внутри окна размещено текстовое сообщение, состоящее из одного вопроса: «Вы действительно хотите удалить зону: Кабинет директора?» — что служит для подтверждения намерения оператора и предотвращения случайных действий. Это сообщение подчеркивает важность процедуры, поскольку удаление зоны может повлечь за собой потерю всех связанных с ней контроллеров и настроек доступа.
В нижней части модального окна расположены две кнопки управления: «Отмена», выполненная в сером цвете, предназначенная для закрытия окна без выполнения удаления, и «Да, удалить», выделенная красным цветом, которая инициирует процесс удаления выбранной зоны из системы. Красный цвет этой кнопки служит визуальным сигналом о серьезности и необратимости действия, что способствует повышению внимательности оператора при его выполнении.

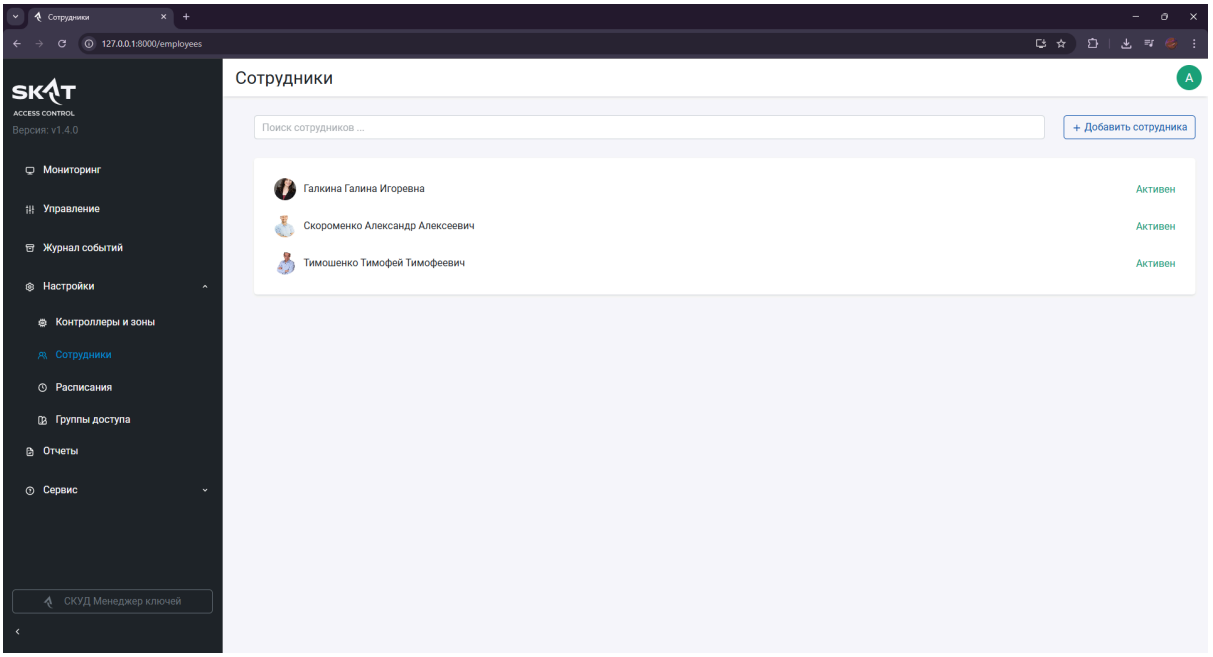


Если при попытке удаления зоны можно столкнуться с важным системным уведомлением, выделенное на светло-розовом фоне: «Зона доступа не может быть удалена, потому что содержит контроллеры.» — что указывает на наличие ограничения целостности данных. Это сообщение информирует администратора о том, что операция удаления невозможна в текущем состоянии, поскольку зона содержит привязанные к ней физические устройства, и для ее удаления необходимо сначала перенести или удалить все связанные контроллеры.
Если визуально в зоне не находится никаких контроллеров, то попробуйте вернуть скрытые контроллеры. Они могут содержаться в этой зоне, но не отображаться визуально.


Контроллеры и зоны
127.0.0.1:8000/access-structure
SKAT
ACCESS CONTROL
Версия: v1.4.0
Мониторинг
Управление
Журнал событий
Настройки
Контроллеры и зоны
Сотрудники
Расписания
Группы доступа
Отчеты
Сервис
СКУД Менеджер ключей
Контроллеры и зоны
Скрытые контроллеры
+ Добавить зону
Удаление зоны: Кабинет директора
Вы действительно хотете удалить зону: Кабинет директора?
Зона доступа не может быть удалена, потому что содержит контроллеры.
Да, удалить
Отмена
Вход
Режим: Шлагбаум
Наименование: Шлагбаум № 3
Направление: Вход
Изменить
Наименование: Шлагбаум № 3
Направление: Выход
Изменить
Режим: Турникет
Наименование: Турникет № 5
Описание: Турникет на входе
Направление: Вход
Изменить
Наименование: Турникет № 5
Направление: Выход
Изменить
Программисты
Кабинет директора
Бухгалтерия
Сохранить

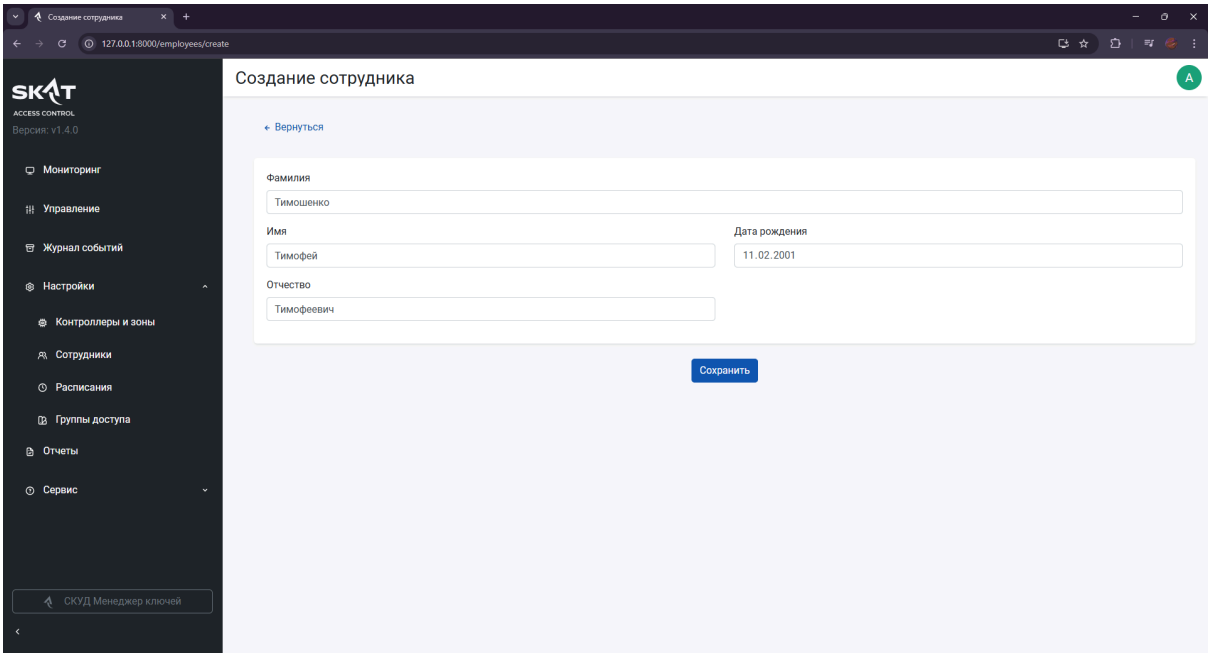
Вкладка Настройки. Сотрудники

В верхней части страницы, под заголовком «Сотрудники», расположен функциональный блок, включающий строку поиска с подсказкой «Поиск сотрудников...» и кнопку «+ Добавить сотрудника». Строка поиска позволяет оператору быстро находить конкретных пользователей по имени или фамилии, что существенно ускоряет навигацию в списках с большим количеством записей. Кнопка добавления служит для инициации процесса регистрации нового сотрудника в системе, что является основным действием при расширении перечня авторизованных лиц. Основное содержимое страницы представляет собой список зарегистрированных пользователей, каждый из которых отображен в виде строки с аватаром и полным именем. Справа от каждого имени расположена метка статуса — «Активен», выполненная зеленым цветом, что указывает на то, что учетная запись данного сотрудника активна и он имеет право на проход через контроллеры системы.



Пример пошагового добавления сотрудника

Нажмем на кнопку Добавить сотрудника в верхнем правом углу экрана. В верхней части страницы, под заголовком «Создание сотрудника», расположен элемент навигации — ссылка «← Вернуться», позволяющая оператору отменить текущую операцию и вернуться к предыдущему экрану без сохранения введенных данных. Ниже размещена форма ввода персональной информации, состоящая из четырех полей: «Фамилия», «Имя», «Отчество» и «Дата рождения». В каждом поле уже введены данные: фамилия, например, «Тимошенко», имя, например, «Тимофей», отчество, например, «Тимофеевич», дата рождения, например, «11.02.2001». Такая структура формы обеспечивает сбор необходимых идентификационных данных, требуемых для формирования уникального профиля пользователя в системе.
В нижней части формы расположена кнопка «Сохранить», выполненная в синем цвете, которая предназначена для фиксации всех введенных данных и создания новой учетной записи сотрудника. После нажатия этой кнопки система должна провести валидацию данных и, при их корректности, добавить нового пользователя в базу данных, после чего возможно будет приступить к назначению ему групп доступа или привязке к конкретным контроллерам.

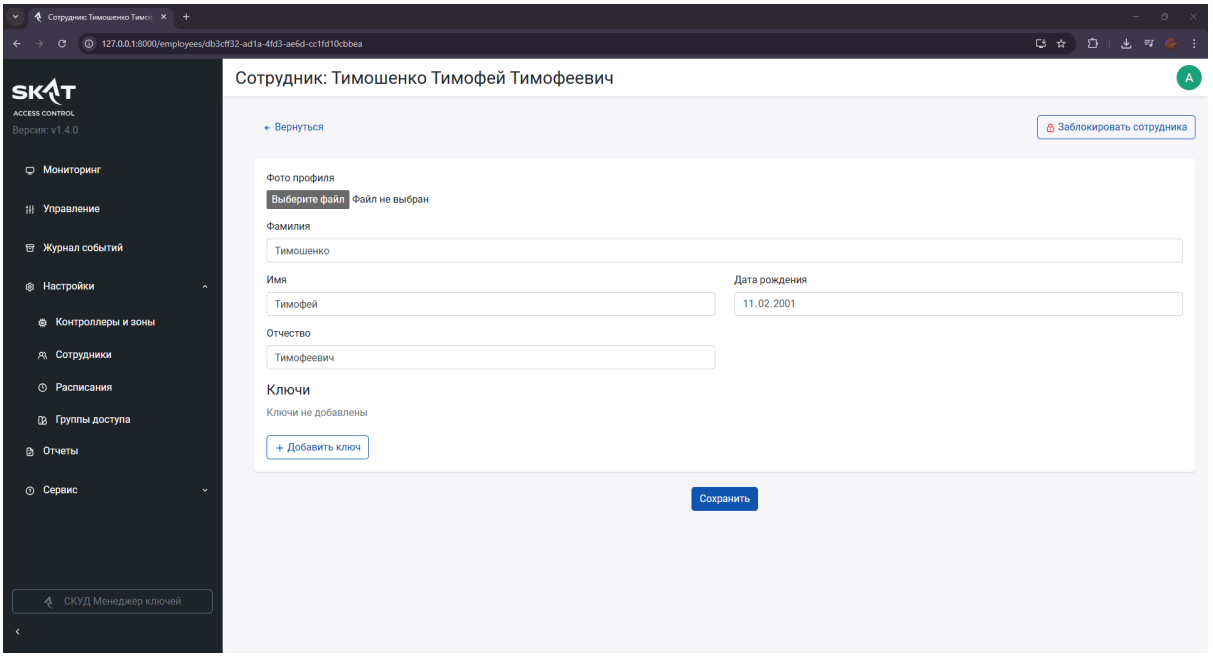


В верхней части страницы расположен элемент навигации — ссылка «← Вернуться», позволяющая оператору покинуть текущий экран без сохранения изменений и вернуться к списку сотрудников. Справа от заголовка размещена кнопка «Заблокировать сотрудника», выполненная с иконкой замка, предназначенная для временного или постоянного отключения доступа данного пользователя к системе контроля доступа. Это является важным инструментом управления безопасностью, позволяющим оперативно реагировать на изменения в статусе персонала.

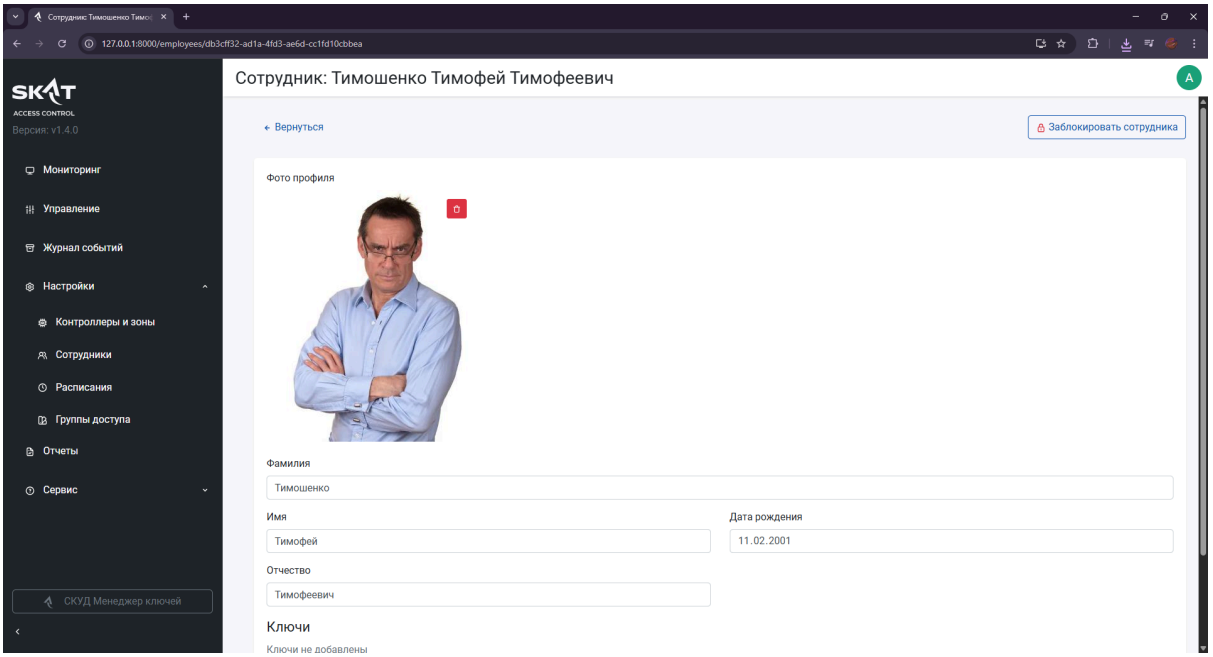
Основное содержимое страницы представляет собой форму редактирования персональных данных. В начале формы расположено поле «Фото профиля» с кнопкой «Выберите файл» и текстовым указанием «Файл не выбран», что свидетельствует о возможности добавления фотографии для визуальной идентификации сотрудника в системе. Ниже следуют поля для ввода фамилии, имени и отчества, а также дата рождения, все из которых заполнены соответствующими данными: «Тимошенко», «Тимофей», «Тимофеевич» и «11.02.2001».

Ниже блока персональных данных находится секция «Ключи», содержащая сообщение «Ключи не добавлены» и кнопку «+ Добавить ключ». Данная секция предназначена для привязки к учетной записи физических ключей доступа, таких как Wiegand или TM, что является необходимым условием для предоставления сотруднику физического доступа через контроллеры системы.

В нижней части формы расположена кнопка «Сохранить», выполненная в синем цвете, которая служит для фиксации всех внесенных изменений в профиле сотрудника.

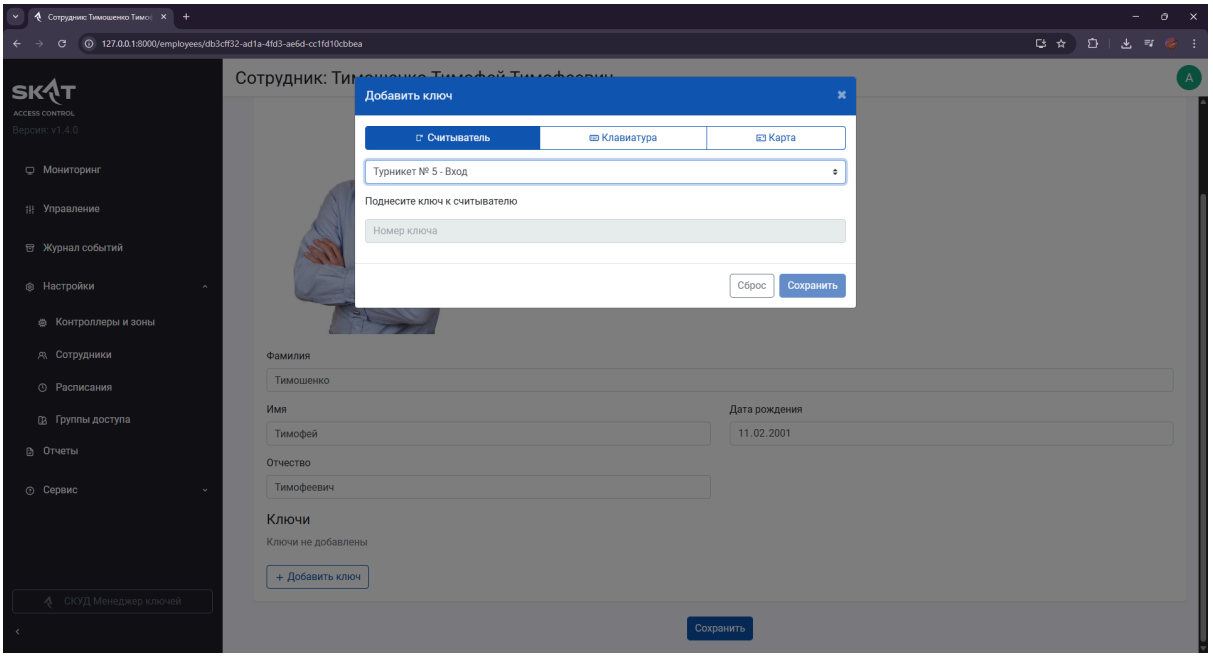


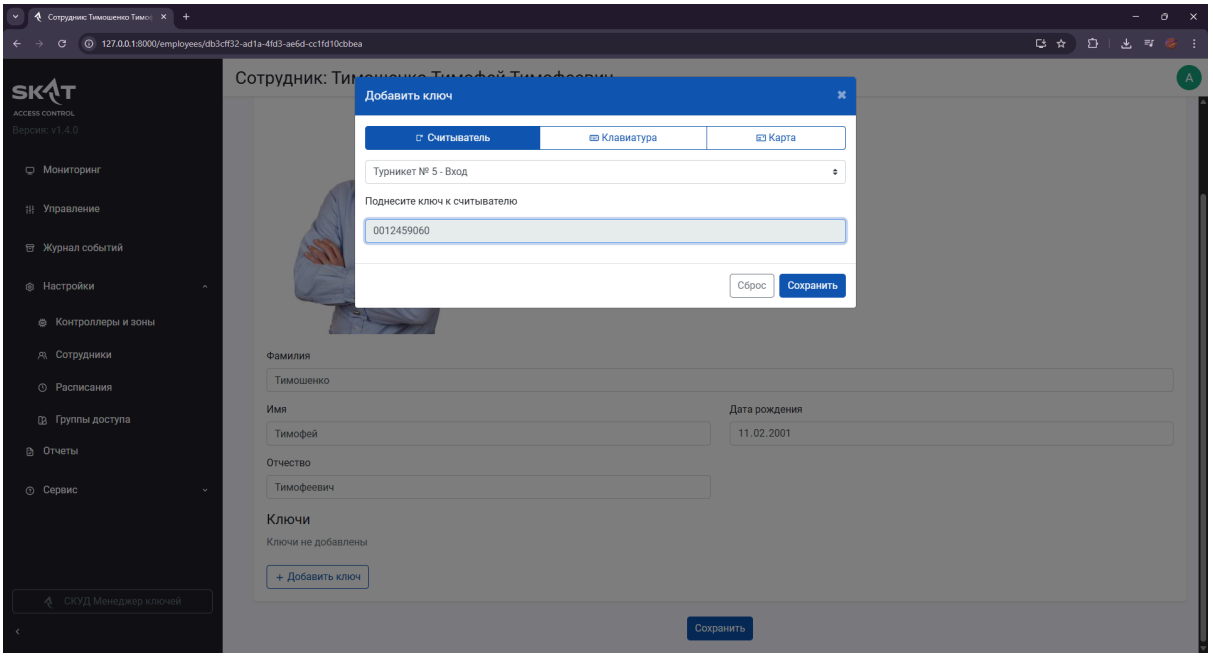
Для осуществления процедуры загрузки фотографии в профиль сотрудника необходимо выполнить следующее действие: нажать на серую кнопку, обозначенную текстом «Выберите файл». Данная операция инициирует открытие стандартного диалогового окна системы управления файлами, в котором пользователю предоставляется возможность произвести выбор необходимого изображения из локального хранилища. После идентификации и выделения требуемого файла следует подтвердить его выбор, что приведет к его загрузке в систему и последующей привязке к профилю указанного сотрудника. Сохранитесь после добавления новой фотографии.



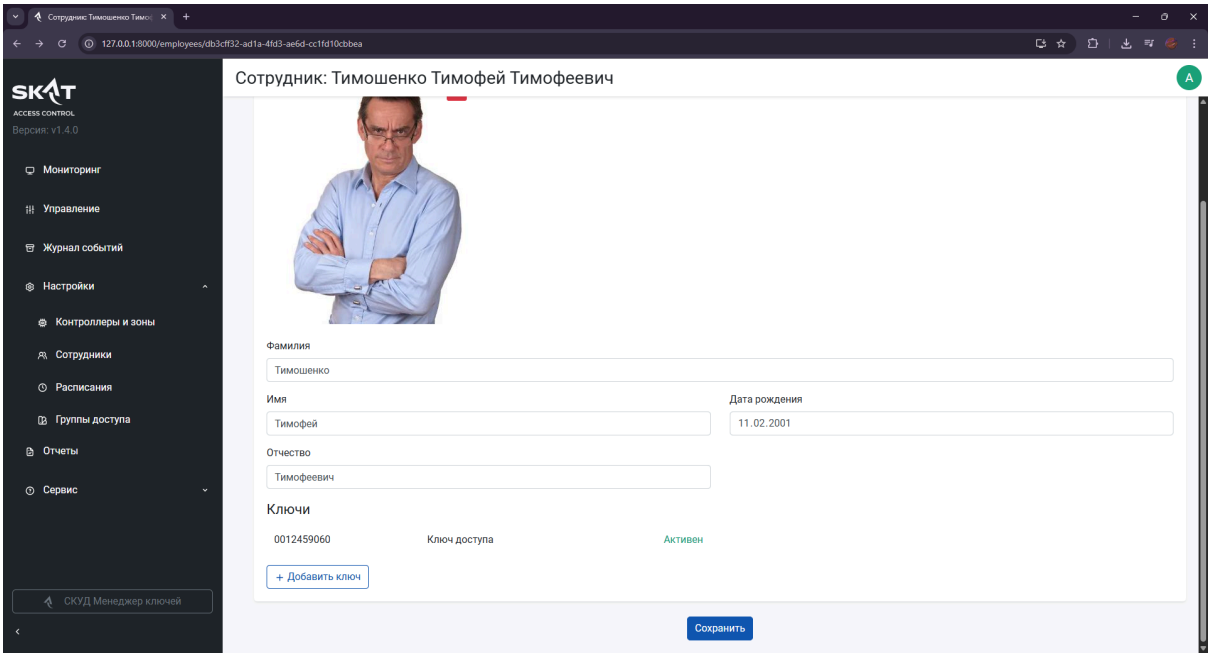
Нажмите на кнопку «+ Добавить ключ» в секции Ключи. Центральным элементом экрана является модальное окно с заголовком «Добавить ключ», которое активировано для привязки физического или виртуального средства доступа к учетной записи пользователя. Заголовок модального окна четко определяет выполняемую операцию — добавление нового ключа. Внутри окна расположена панель навигации с тремя вкладками: «Считыватель», «Клавиатура» и «Карта». В текущий момент активна вкладка «Считыватель». Ниже данной вкладки находится выпадающий список, в котором можно выбрать контроллер, на котором

расположен считыватель. Выбрав считыватель можно будет поднести к нему карту доступа и данные с нее будут автоматически добавлены в окно. Выбран контроллер «Турникет № 5 - Вход».
Под списком расположен текстовый блок с инструкцией «Поднесите ключ к считывателю» и поле ввода, помеченное подсказкой «Номер ключа». В данном поле появиться уникальный идентификатора ключа, который должен быть считан с физического носителя при его поднесении к указанному считывателю. Это обеспечивает точную идентификацию и привязку конкретного физического объекта к учетной записи сотрудника.
В нижней части модального окна размещены две кнопки управления: «Сброс», выполненная в сером цвете, предназначенная для отмены текущей операции и очистки введенных данных, и «Сохранить», выделенная синим цветом, которая фиксирует все внесенные параметры и завершает процесс регистрации ключа в системе.





Ключ был добавлен в систему и отображается как активный. Продолжим настройку ключа кликнув по нему.

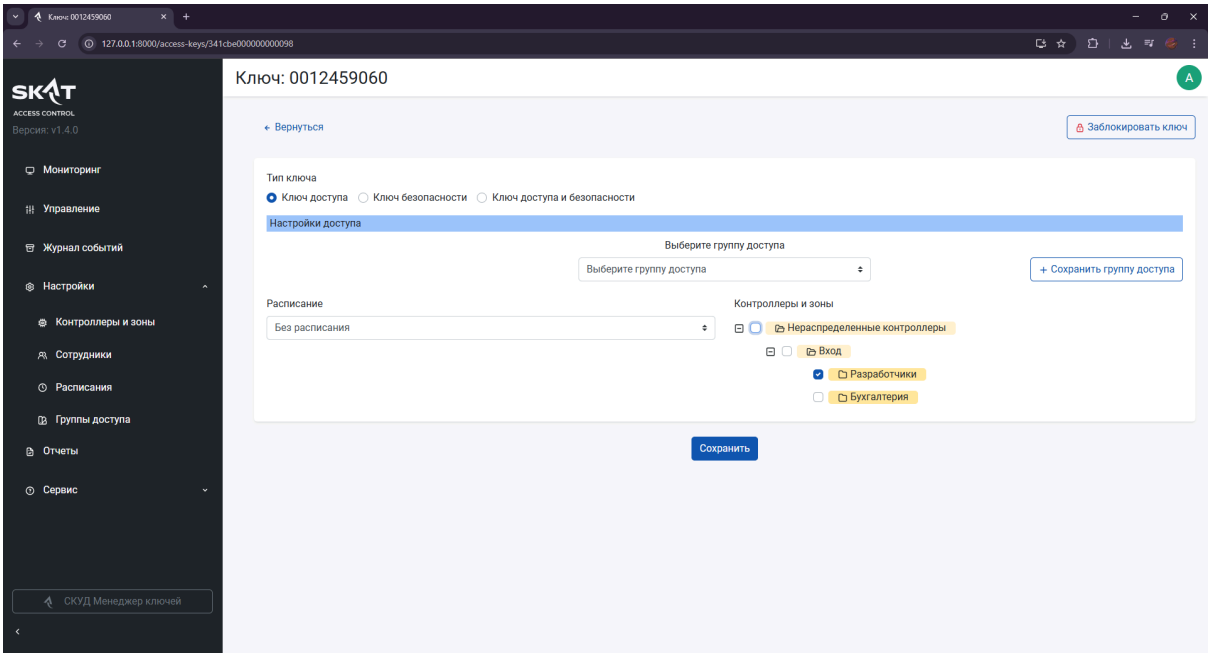


В верхней части страницы, под заголовком, указывающим на объект управления — «Ключ: 0012459060» — расположен элемент навигации «← Вернуться», позволяющий оператору покинуть текущий экран без сохранения изменений и вернуться к предыдущему представлению. Справа от заголовка размещена кнопка «Заблокировать ключ», снабженная иконкой замка, предназначенная для временного или постоянного отключения функциональности данного ключа, что служит инструментом для оперативного реагирования на утерю или несанкционированное использование средства доступа.

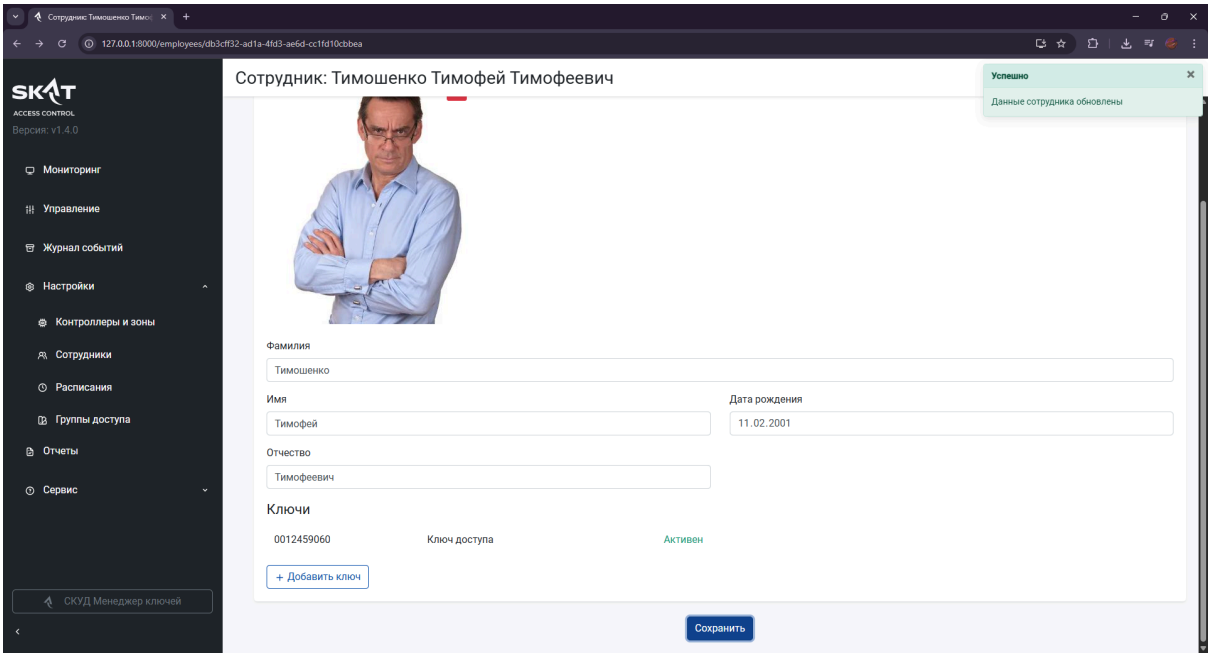
Основное содержимое страницы представляет собой форму настройки, в которой в первую очередь определяется тип ключа. В данном случае активирована радиокнопка «Ключ доступа», что указывает на то, что данный носитель предназначен исключительно для управления проходами через контроллеры системы **(обратитесь к разделу терминов. чтобы увидеть описание ключей)**. Ниже следует секция «Настройки доступа», которая содержит блок управления группами доступа. Здесь расположен выпадающий список «Выберите группу доступа», позволяющий назначить ключу одну из заранее созданных групп, определяющих набор зон и контроллеров, к которым будет предоставлен доступ. Рядом с этим списком находится кнопка «+ Сохранить группу доступа», предназначенная для создания новой группы непосредственно в процессе настройки ключа.

Далее расположены два дополнительных параметра: поле «Расписание», в котором выбрано значение «Без расписания», что означает отсутствие временных ограничений на использование ключа, и секция «Контроллеры и зоны», содержащая чекбокс и ссылку на «Нераспределенные контроллеры». Это указывает на то, что данный ключ пока не привязан ни к одной конкретной зоне или контроллеру и требует дальнейшей конфигурации для полноценного функционирования. Ключи, привязанные к зоне Нераспределенные контролеры не будут работать в системе. Обязательно привяжите ключ к нужной зоне. В текущий момент выбрана зона «Разработчики», что свидетельствует о том, что данный ключ будет иметь право на проход только через устройства, привязанные к этой зоне. Зоны «Нераспределенные контроллеры», «Вход» и «Бухгалтерия» остаются не выбранными, что позволяет точно ограничить область действия ключа.

В нижней части формы размещена кнопка «Сохранить», выполненная в синем цвете, предназначенная для фиксации всех внесенных изменений в конфигурации ключа. Нажмите на нее по окончанию настройки.

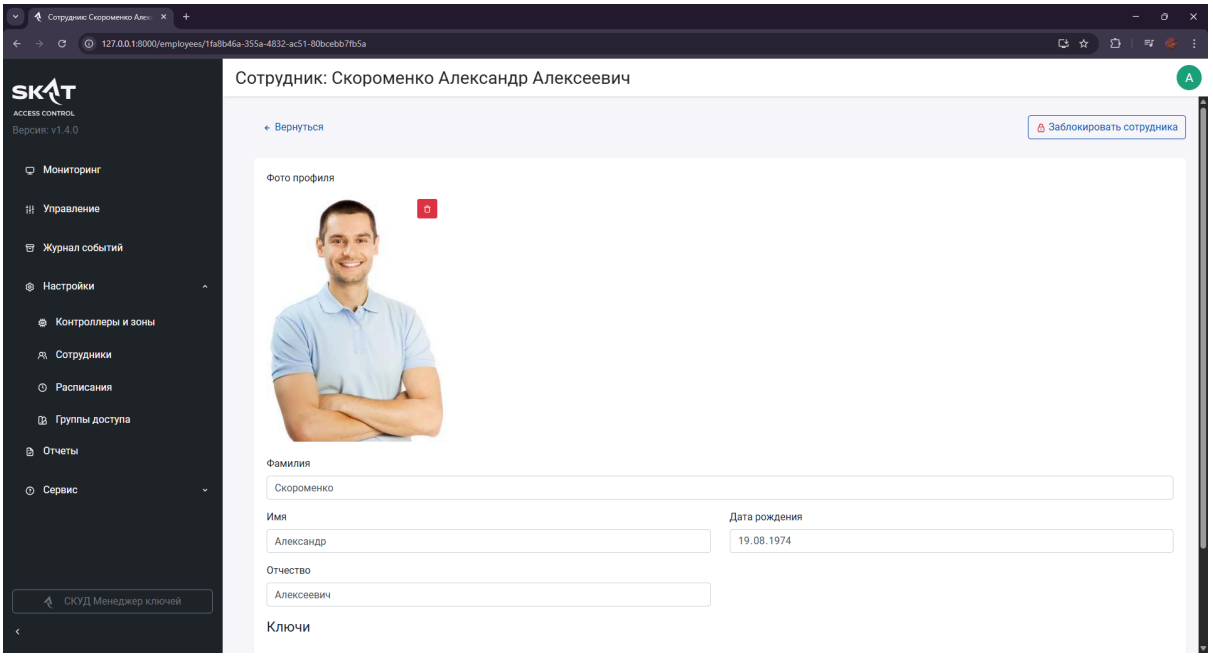


После настройки ключа вернитесь на страницу сотрудника. Убедитесь, что все поля записаны, нужные ключи добавлены в систему и сконфигурированы. Если все пункты были соблюдены, то можно нажимать на кнопку сохранить и переходить к созданию следующего.



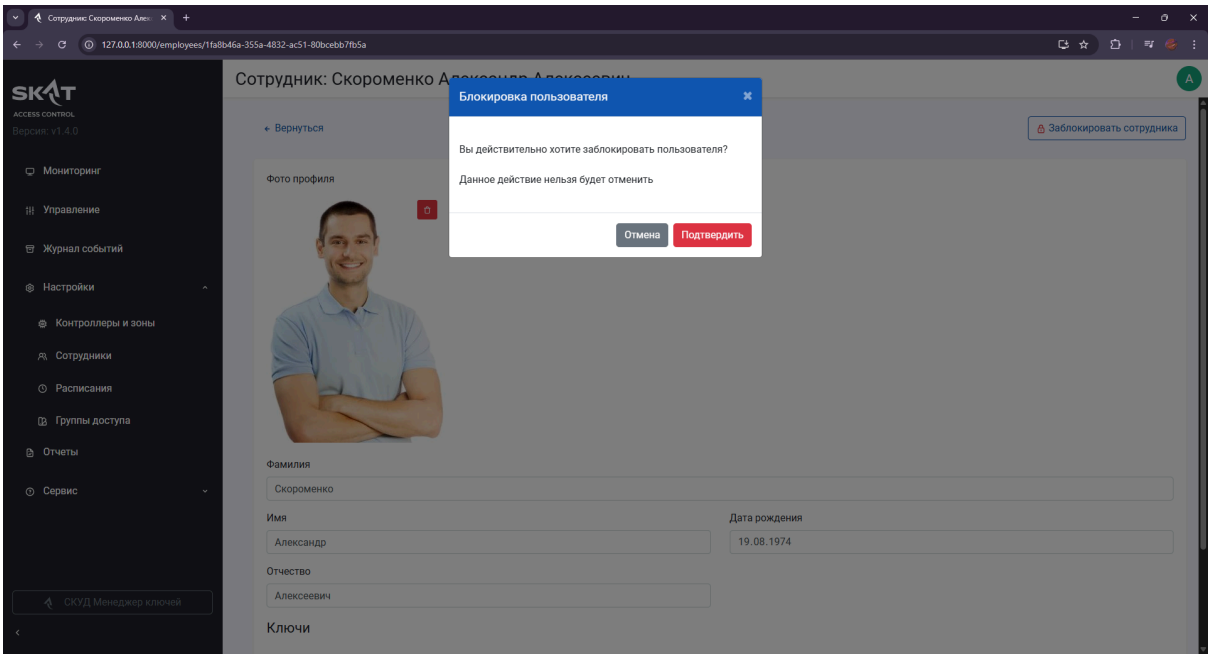
Пример удаления ключа или сотрудника

В верхней части страницы, под заголовком, указывающим на объект управления — «Сотрудник: Скороменко Александр Алексеевич» — расположен элемент навигации «← Вернуться», позволяющий оператору покинуть текущий экран без сохранения изменений и вернуться к списку сотрудников. Справа от заголовка размещена кнопка «Заблокировать сотрудника», выполненная с иконкой замка, которая является ключевым инструментом для немедленного деактивирования учетной записи данного пользователя.

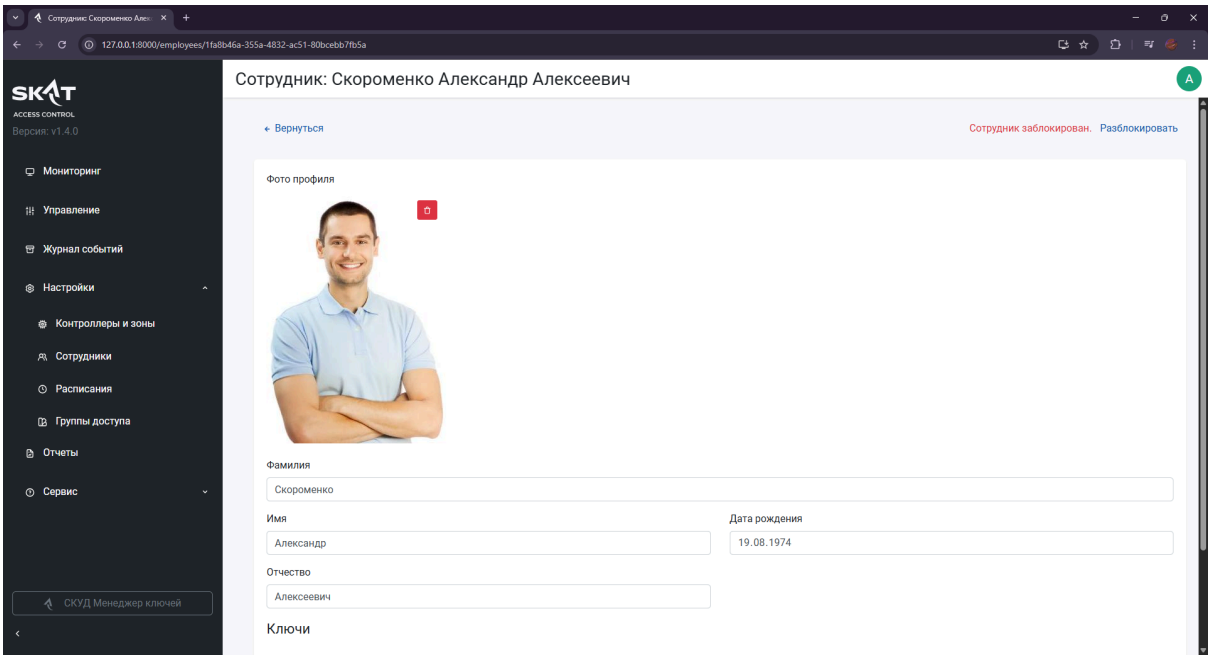


Заголовок модального окна четко определяет выполняемую операцию — блокировку пользователя. Внутри окна размещено текстовое сообщение, состоящее из двух частей. Первая часть представляет собой вопрос: «Вы действительно хотите заблокировать пользователя?» — что служит для подтверждения намерения оператора и предотвращения случайных действий. Вторая часть содержит важное предупреждение: «Данное действие нельзя будет отменить» — что указывает на необратимый характер процедуры блокировки. Это подчеркивает критическую важность данного шага и требует осознанного принятия решения со стороны администратора.

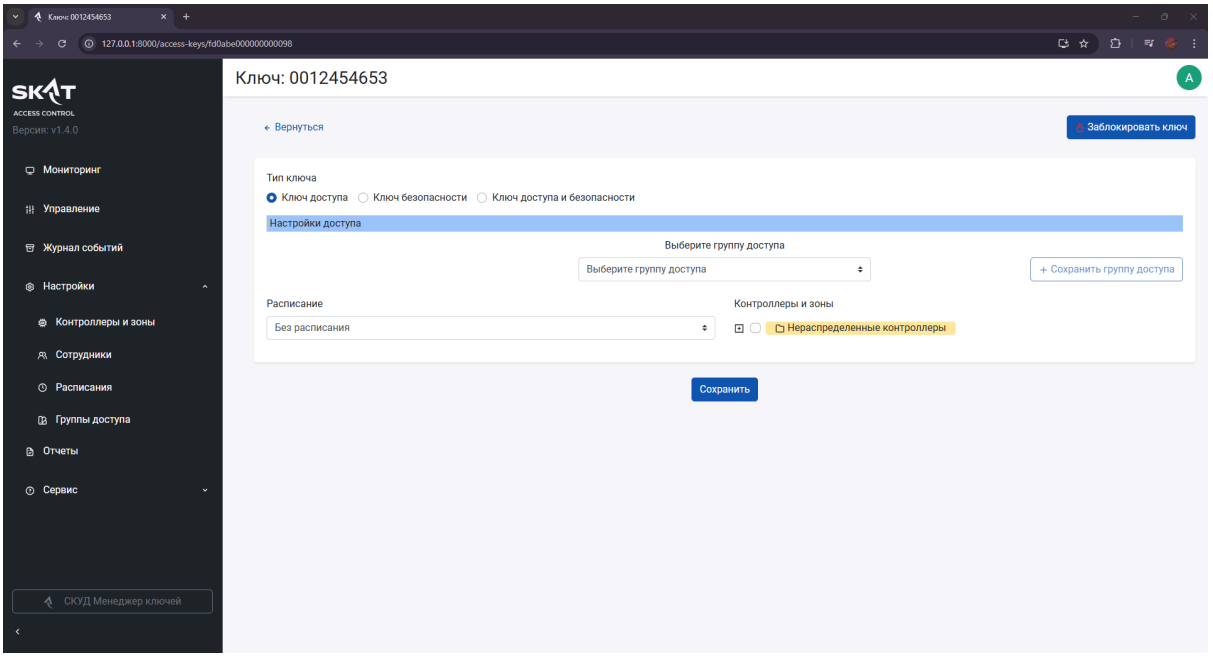
В нижней части модального окна расположены две кнопки управления: «Отмена», выполненная в сером цвете, предназначенная для закрытия окна без выполнения блокировки, и «Подтвердить», выделенная красным цветом, которая инициирует процесс деактивации учетной записи сотрудника в системе. Красный цвет этой кнопки служит визуальным сигналом о серьезности и необратимости действия, что способствует повышению внимательности оператора при его выполнении.



Сотрудника при необходимости можно разблокировать. Справа от заголовка размещено информационное сообщение — «Сотрудник заблокирован» — выполненное красным цветом, что служит явным индикатором текущего статуса учетной записи. Ключ, привязанный к его учетный записи теперь перестал быть активным. Непосредственно рядом с этим сообщением находится ссылка «Разблокировать», выполненная синим цветом, предназначенная для инициации процедуры восстановления доступа данного сотрудника. При этом привязать ключ необходимо будет заново

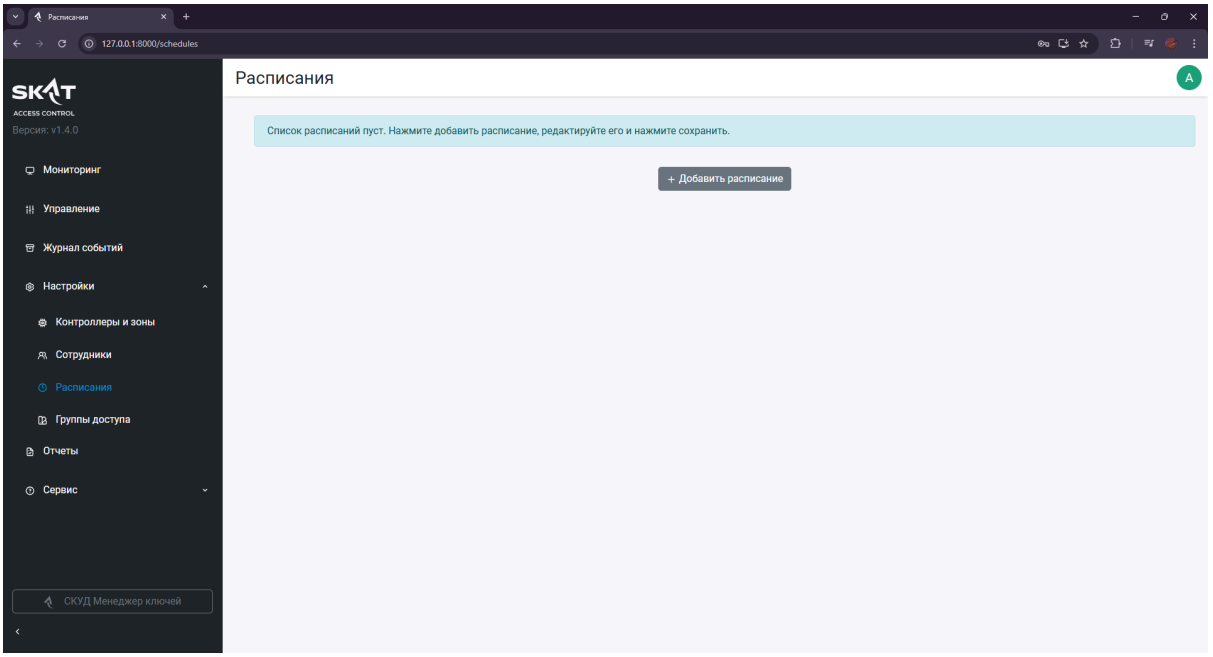


Если ключ карат сотрудника была утеряна, то можно перейти на страницу сотрудника и найти утерянный ключ и кликнуть по нему. Справа от заголовка размещена кнопка «Заблокировать ключ» с соответствующей иконкой замка, предназначенная для немедленного деактивирования функциональности данного средства доступа в случае его утраты, компрометации.



Вкладка Настройки. Расписания

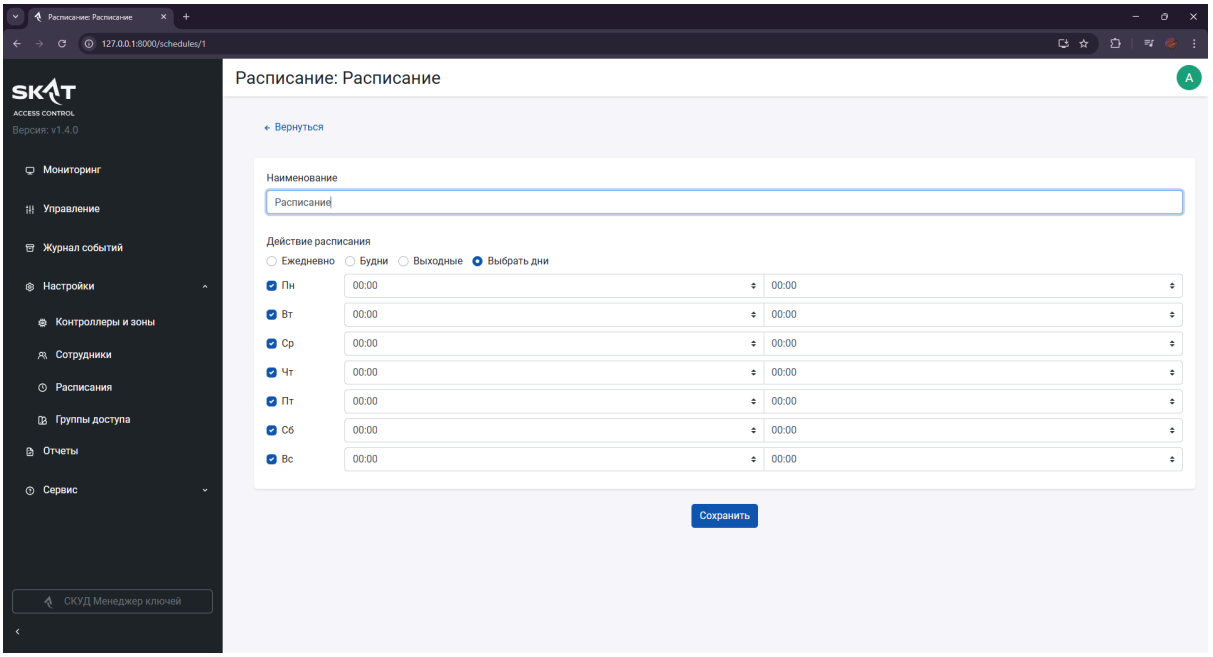
В верхней части страницы, под заголовком «Расписания», расположен информационный блок с текстом: «Список расписаний пуст. Нажмите добавить расписание, редактируйте его и нажмите сохранить». Этот текст служит инструкцией для администратора и указывает на текущее состояние системы — отсутствие созданных расписаний, что является начальной точкой для настройки временных ограничений доступа.
Непосредственно под информационным сообщением размещена кнопка «+ Добавить расписание», выполненная в сером цвете. Добавлять расписания можно до семи штук. Данная кнопка является единственным функциональным элементом на экране и предназначена для инициации процесса создания нового расписания. После ее нажатия система откроет форму для ввода параметров нового временного правила, включающего дни недели, часы начала и окончания действия, а также другие возможные условия.



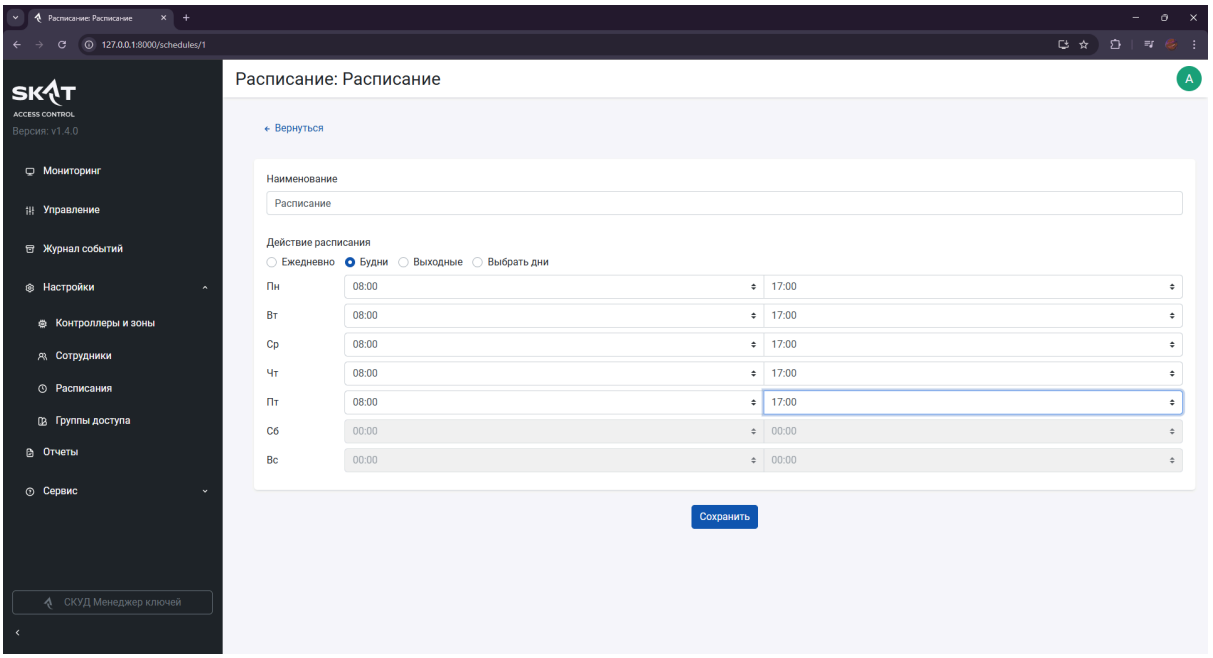
Пример пошаговой настройки расписаний

В верхней части страницы, под заголовком «Добавить новую группу доступа», расположен элемент навигации — ссылка «← Вернуться», позволяющая оператору отменить текущую операцию и вернуться к предыдущему экрану без сохранения введенных данных. Ниже размещена форма конфигурирования, состоящая из нескольких блоков.
Первый блок — «Наименование» — содержит текстовое поле с подсказкой «Введите наименование группы доступа». Это поле предназначено для ввода уникального и описательного имени группы, которое будет использоваться для ее идентификации в системе и в отчетах.
Следующий блок — «Расписание» — содержит выпадающий список, в котором выбрано значение «Без расписания». Это указывает на то, что доступ, предоставляемый данной группой, не будет ограничен временными рамками и будет действителен круглосуточно. В дальнейшем, при наличии созданных расписаний, администратор сможет выбрать конкретное расписание, чтобы ограничить время действия прав доступа.
Ниже расположен блок, содержащий таблицу временных интервалов для каждого дня недели — от понедельника (Пн) до воскресенья (Вс). Каждая строка содержит два поля ввода времени, обозначающие начало и окончание периода доступа. В текущем состоянии все поля установлены в значение «00:00», что соответствует отсутствию активных временных ограничений, поскольку выбрано общее расписание «Без расписания».Непосредственно под

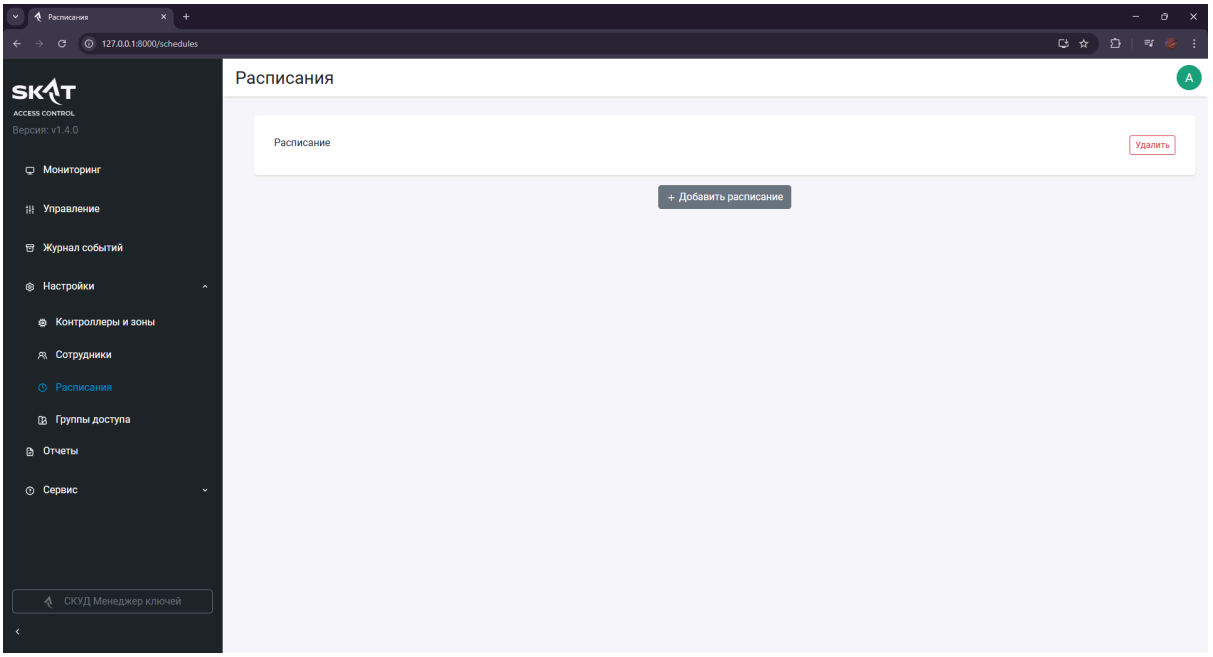
ним находится блок «Действие расписания», содержащий четыре радиокнопки для выбора типа действия: «Ежедневно», «Будни», «Выходные» и «Выбрать дни».



Сконфигурируем расписание. В текущий момент активирована радиокнопка «Будни», что указывает на то, что данное расписание будет применяться только в рабочие дни недели — с понедельника по пятницу. Далее следует таблица, в которой для каждого дня недели — от понедельника (Пн) до воскресенья (Вс) — заданы временные интервалы доступа. Для дней «Будни» (Пн–Пт) установлен единый интервал с 08:00 до 17:00. Для субботы (Сб) и воскресенья (Вс) интервалы установлены в значение «00:00», что соответствует отсутствию доступа в выходные дни, поскольку выбран режим «Будни». По окончании конфигурирования нажмите кнопку «Сохранить».

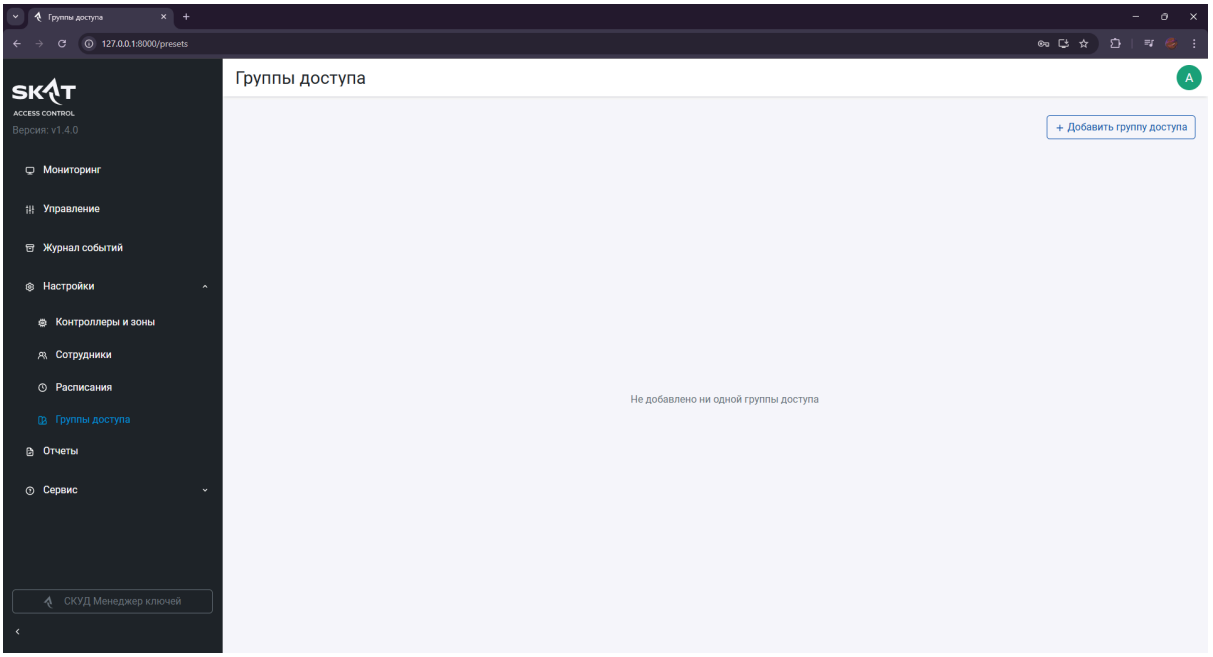


Теперь во вкладке расписании появилось добавленное ранее расписание.

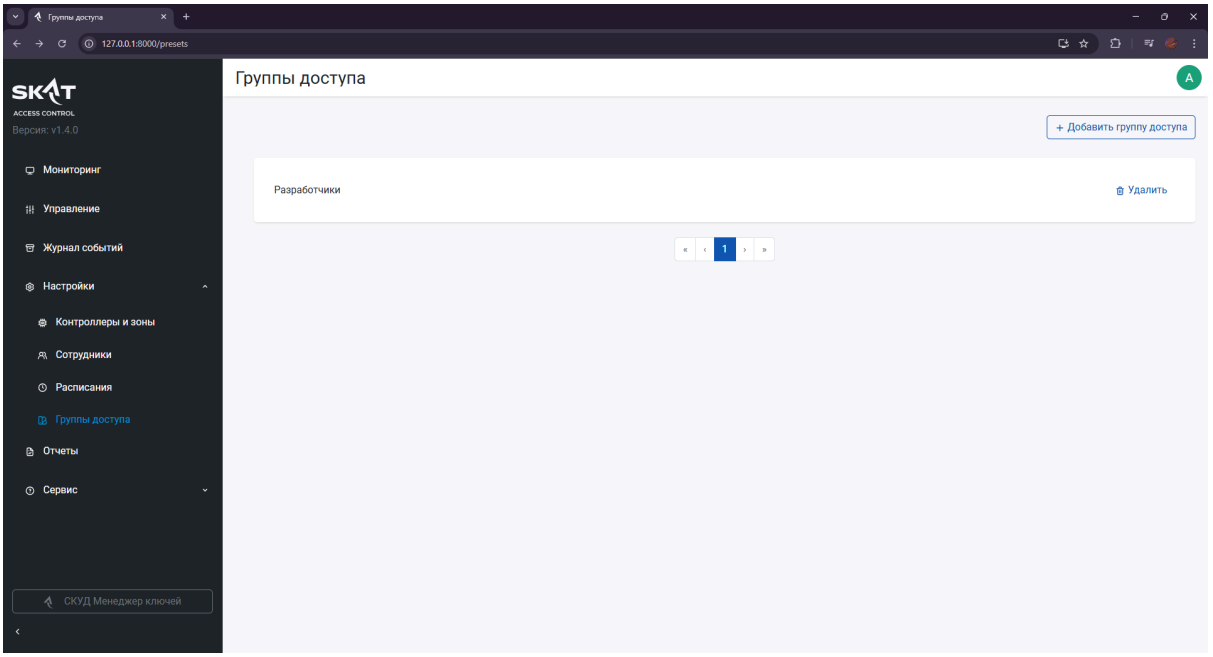

Расписания
127.0.0.1:8000/schedules
SKAT
ACCESS CONTROL
Версия: v1.4.0
Мониторинг
Управление
Журнал событий
Настройки
Контроллеры и зоны
Сотрудники
Расписания
Группы доступа
Отчеты
Сервис
СКУД Менеджер ключей
Расписания
A
Расписание
Удалить
+ Добавить расписание

Вкладка Настройки. Группы доступа

В верхней части страницы, под заголовком «Группы доступа», расположен информационный текст, размещенный по центру основного контента: «Не добавлено ни одной группы доступа». Данное сообщение служит индикатором текущего состояния системы — отсутствия созданных групп, что является начальной точкой для настройки политик доступа. Это указывает на то, что перед назначением прав персоналу необходимо сначала сформировать хотя бы одну группу, определив ее параметры и привязав к ней необходимые зоны и временные группы по необходимости.
Непосредственно под заголовком, в правой части экрана, размещена кнопка «+ Добавить группу доступа», выполненная в синем цвете. Данная кнопка является единственным функциональным элементом на экране и предназначена для инициации процесса создания новой группы. После ее нажатия система откроет форму для ввода наименования группы, выбора расписания и назначения зон, к которым будет предоставлен доступ.



При появлении хотя бы одной группы в интерфейсе будет отображаться ее название



Пример настройки группы доступа

Нажмите на кнопку Добавить группы доступа. Откроется новое окно. В верхней части страницы, под заголовком «Добавить новую группу доступа», расположен элемент навигации — ссылка «← Вернуться», позволяющая оператору отменить текущую операцию и вернуться к предыдущему экрану без сохранения введенных данных. Ниже размещена форма конфигурирования, состоящая из нескольких блоков.

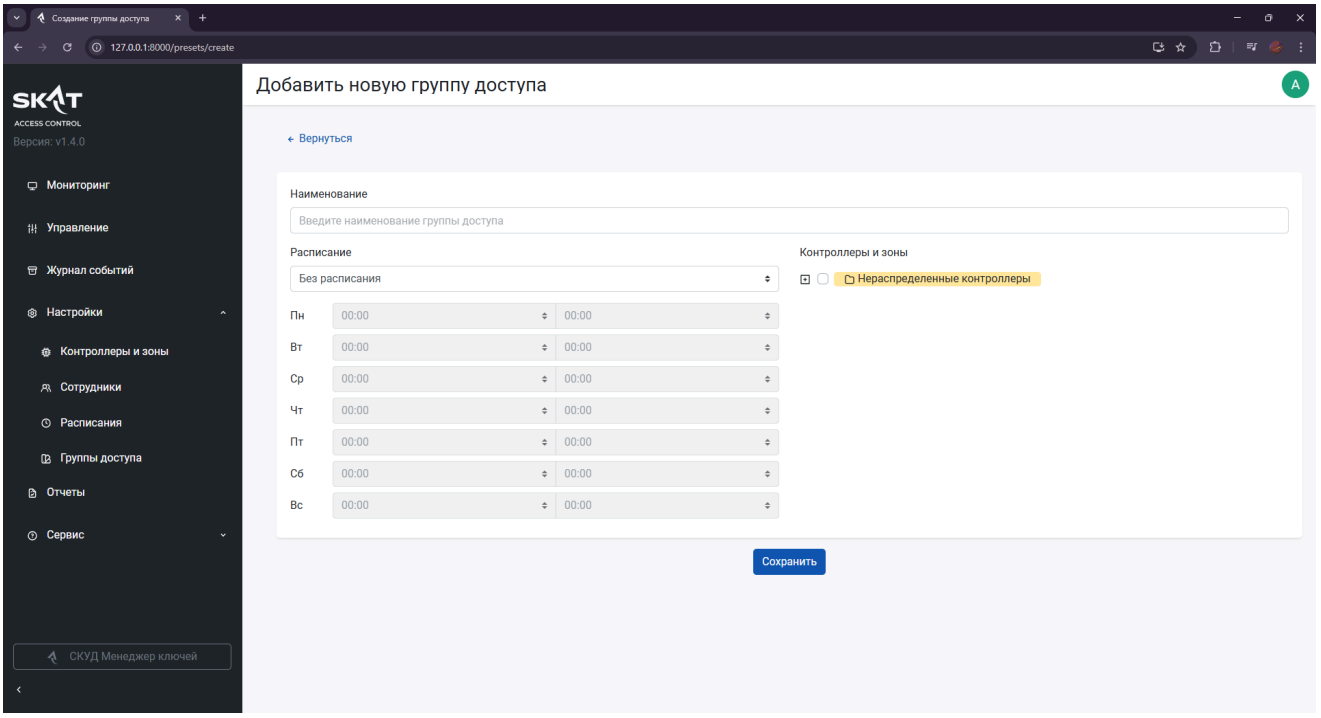
Первый блок — «Наименование» — содержит текстовое поле с подсказкой «Введите наименование группы доступа». Это поле предназначено для ввода уникального и описательного имени группы, которое будет использоваться для ее идентификации в системе и в отчетах.

Следующий блок — «Расписание» — содержит выпадающий список, в котором выбрано значение «Без расписания». Это указывает на то, что доступ, предоставляемый данной группой, не будет ограничен временными рамками и будет действителен круглосуточно. В дальнейшем, при наличии созданных расписаний, администратор сможет выбрать конкретное расписание, чтобы ограничить время действия прав доступа.

Ниже расположен блок, содержащий таблицу временных интервалов для каждого дня недели — от понедельника (Пн) до воскресенья (Вс). Каждая строка содержит два поля ввода времени, обозначающие начало и окончание периода доступа. В текущем состоянии все поля установлены в значение «00:00», что соответствует отсутствию активных временных ограничений, поскольку выбрано общее расписание «Без расписания».

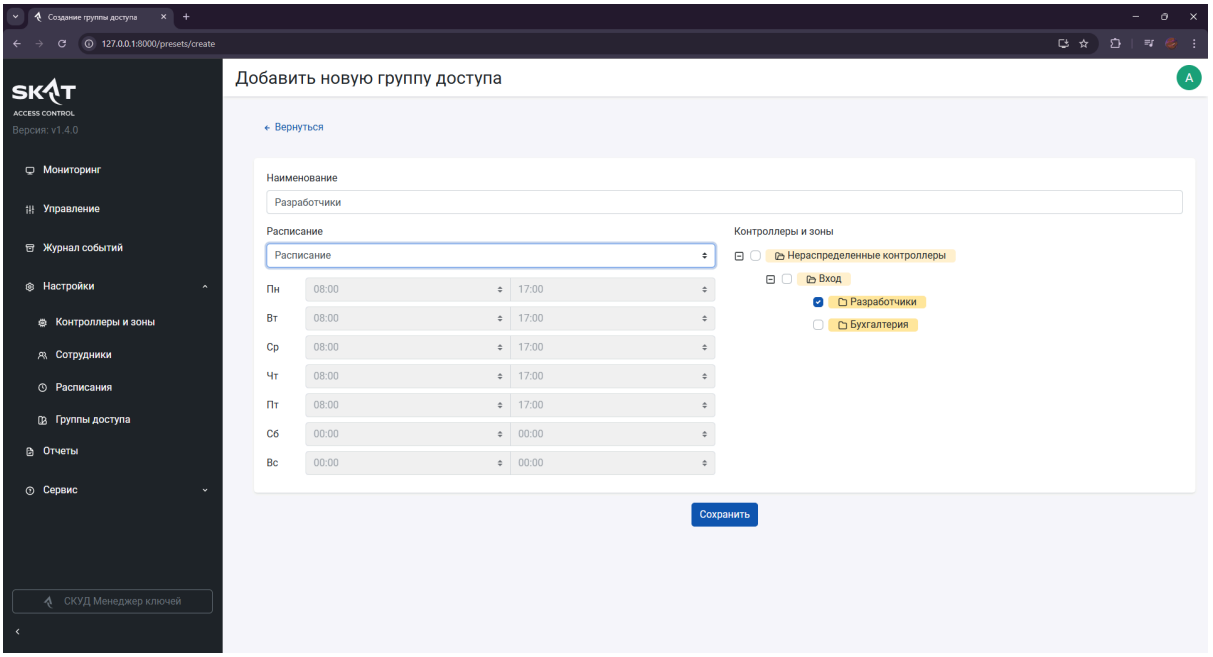
Правее расположена секция «Контроллеры и зоны», содержащая чекбокс и ссылку на «Нераспределенные контроллеры». Это указывает на то, что при создании новой группы доступа необходимо явно назначить ей одну или несколько зон безопасности или контроллеров, к которым будет предоставлен доступ. В данный момент ни одна зона не выбрана, что требует дополнительной конфигурации перед сохранением группы.

В нижней части формы размещена кнопка «Сохранить», выполненная в синем цвете, которая служит для фиксации всех внесенных параметров и создания новой группы доступа в системе.



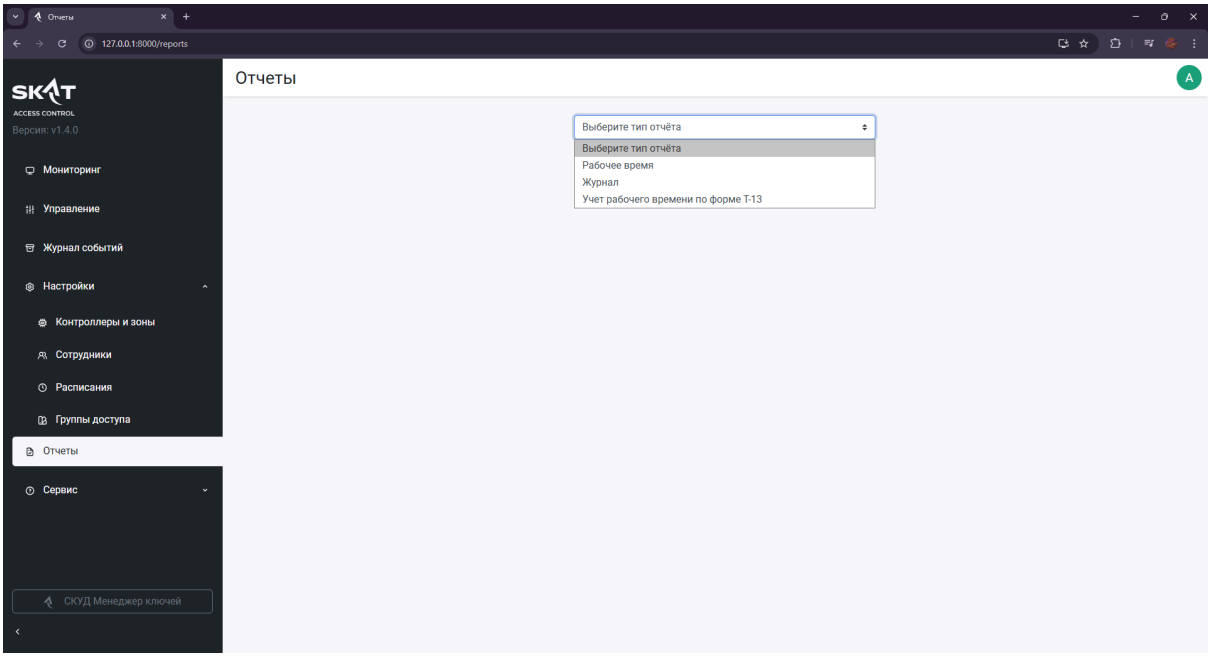
Сконфигурируем группу доступа по нужным задач. В верхней части страницы, под заголовком «Добавить новую группу доступа», расположен элемент навигации — ссылка «← Вернуться», позволяющая оператору отменить текущую операцию и вернуться к предыдущему экрану без

сохранения внесенных изменений. Ниже размещена форма конфигурирования, содержащая все необходимые параметры для определения характеристик новой группы.
Первое поле — «Наименование» — заполнено текстом «Разработчики», что указывает на назначение данной группы для персонала, относящегося к отделу разработки. Это имя будет использоваться для идентификации группы в системе, в отчетах и при назначении прав доступа **(при создании или конфигурации сотрудника можно указать созданные группы доступа)**.
Следующий блок — «Расписание» — содержит выпадающий список, в котором выбрано значение «Расписание» **(создание расписания смотрите в блоке ...)**. Это означает, что доступ, предоставляемый данной группе, будет ограничен временными рамками, определенными в выбранном расписании. Ниже этого списка представлена таблица временных интервалов для каждого дня недели. Для рабочих дней — с понедельника по пятницу — установлен единый интервал с 08:00 до 17:00. Для субботы и воскресенья интервалы установлены в значение «00:00», что соответствует отсутствию доступа в выходные дни, согласно выбранному расписанию.
Правее расположена секция «Контроллеры и зоны», где администратор может назначить конкретные зоны, к которым будет предоставлен доступ. В данном случае активирован чекбокс напротив зоны «Разработчики», что указывает на то, что данная группа будет иметь право на проход только через устройства, привязанные к этой зоне. Зоны «Нераспределенные контроллеры», «Вход» и «Бухгалтерия» остаются не выбранными, что позволяет точно ограничить область действия группы.



Вкладка Отчеты

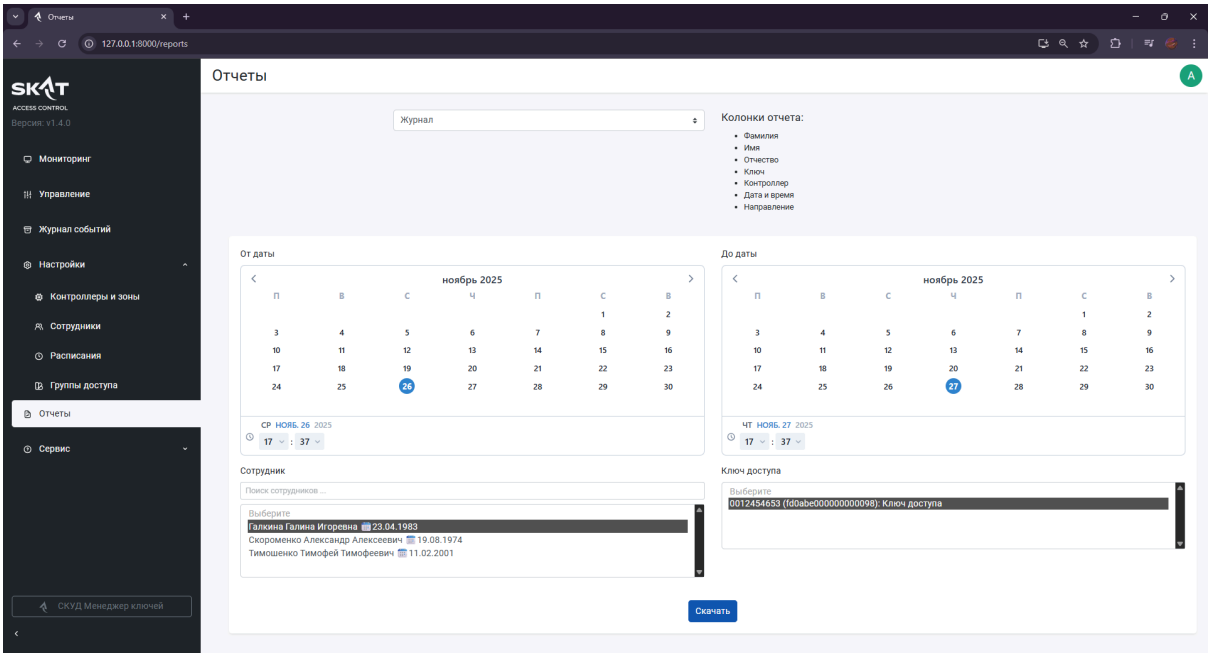
В верхней части страницы, под заголовком «Отчеты», расположен выпадающий список с меткой «Выберите тип отчёта». Этот элемент управления служит начальной точкой для инициации процесса генерации отчета и позволяет оператору выбрать конкретный вид аналитической информации, необходимой для текущих задач.
Основное содержимое страницы представляет собой пустую область, что свидетельствует о том, что до момента выбора типа отчета система не имеет данных для отображения. Нажав на выпадающий список он раскроется. В нем отображается перечень доступных типов отчетов: «Рабочее время», «Журнал» и «Учет рабочего времени по форме Т-13». Этот элемент управления служит начальной точкой для инициации процесса генерации отчета и позволяет оператору выбрать конкретный вид аналитической информации, необходимой для текущих задач. Выбор одного из этих пунктов активирует соответствующую форму фильтрации и параметров, после чего система сформирует и отобразит результат.



Пример выгрузки отчета

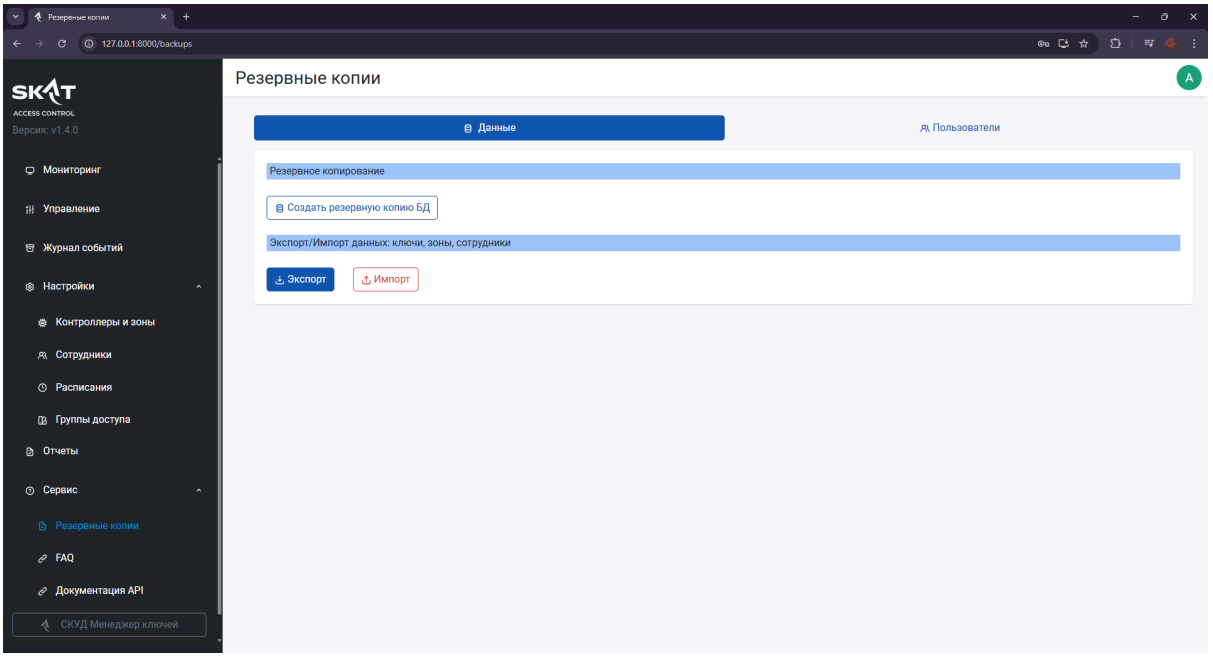
(Примечание) Для корректного формирования отчета необходимо отметить контроллер, который контролирует проход через внешний периметр. На вкладке Настройки. Контроллеры и зоны выберите необходимый контроллер, отметь его как проход внешнего периметра. Если это один контроллер, то настройте его каналы на вход и выход. Если два разных контроллера, отметьте каждый из них как главный проход и по необходимости отметь один как вход, а другой как выход. Остальным контроллерам нет необходимости настраивать каналы и конфигурировать их как выходы и входы. Могут остаться без контроля направления.
Выбрав нужный формат продолжим настройку. В верхней части страницы, под заголовком «Отчеты», расположен выпадающий список с выбранным значением «Журнал». Справа от него указано содержание колонок, которые будут включены в итоговый отчет: «Фамилия», «Имя», «Отчество», «Ключ», «Контроллер», «Дата и время» и «Направление». Это позволяет оператору заранее оценить структуру выходных данных и обеспечивает прозрачность формируемой аналитической информации.
Ниже размещены два календаря для выбора временного интервала отчета — «От даты» и «До даты». В обоих календарях выбран ноябрь 2025 года. В левом календаре выделен день 26 ноября (среда), а в правом — 27 ноября (четверг). Под каждым календарем расположены поля

для уточнения времени, установленные на 17:37. Такая конфигурация указывает на формирование отчета за период с 26 ноября 2025 года, 17:37, по 27 ноября 2025 года, 17:37. Далее следуют два блока фильтрации: «Сотрудник» и «Ключ доступа». В блоке «Сотрудник» представлен выпадающий список с полем поиска, в котором выделена запись «Галкина Галина Игоревна», можно выбрать любого другого сотрудника. Это указывает на то, что отчет будет сформирован только для данного сотрудника. В блоке «Ключ доступа» также представлен выпадающий список, в котором выбран конкретный ключ с идентификатором «0012454653 (fd0abe000000000098)», описанный как «Ключ доступа», выберите нужный ключ, поскольку у сотрудников их можно добавлять и не один. Это позволяет сузить анализ до событий, связанных с использованием именно этого физического или виртуального носителя.
В нижней части формы размещена кнопка «Скачать», выполненная в синем цвете, которая служит для инициации процесса генерации и экспорта отчета в выбранном формате. Отчет будет выгружен в формате xlsx.

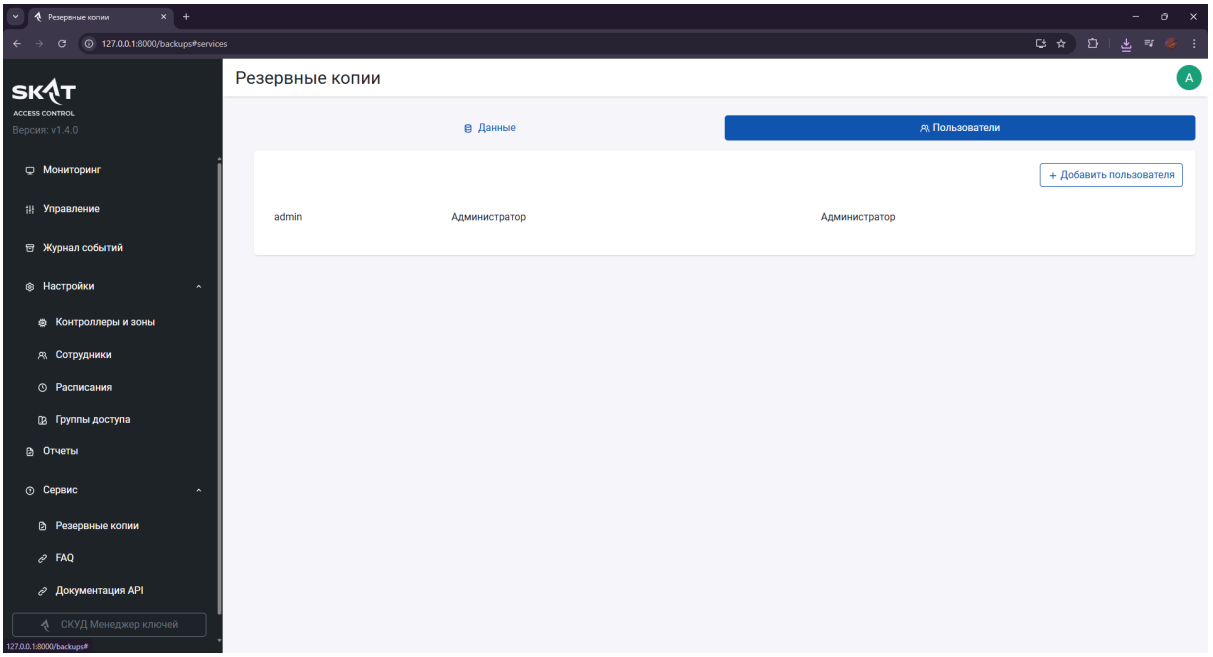


Вкладка Сервис. Резервные копии

В верхней части страницы, под заголовком «Резервные копии», расположен переключатель вкладок с двумя опциями: «Данные» и «Пользователи». В текущий момент активна вкладка «Данные», что указывает на то, что операции будут производиться с основной конфигурацией системы — ключами, зонами, контроллерами и другими параметрами доступа.
Основное содержимое страницы структурировано на две секции. Первая секция — «Резервное копирование» — содержит единственную кнопку «Создать резервную копию БД», снабженную иконкой базы данных. Данная функция предназначена для инициации процесса создания полной архивной копии всех конфигурационных данных системы, что позволяет в случае сбоя или необходимости миграции восстановить систему в предыдущее рабочее состояние.
Вторая секция — «Экспорт/Импорт данных: ключи, зоны, сотрудники» — предоставляет инструменты для обмена данными между системами или для ручного восстановления конкретных компонентов. Здесь расположены две кнопки: «Экспорт», выполненная в синем цвете и снабженная иконкой стрелки вниз, предназначенная для экспорта выбранных данных в файл; и «Импорт», выполненная в красном цвете и снабженная иконкой стрелки вверх, предназначенная для загрузки и восстановления данных из ранее созданного файла.



В верхней части страницы расположен переключатель вкладок с двумя опциями: «Данные» и «Пользователи». В текущий момент активна вкладка «Пользователи», что указывает на то, что операции будут производиться с учетными записями администраторов системы.
Основное содержимое страницы представляет собой список существующих пользователей. В данном случае отображена единственная запись — пользователь с логином «admin», которому присвоена роль «Администратор». Эта информация представлена в виде строки, содержащей три столбца: логин пользователя, его полное имя или описание роли («Администратор») и повторение роли в третьем столбце, что может служить для дополнительной идентификации или упрощения фильтрации в более крупных системах.
Справа от списка пользователей размещена кнопка «+ Добавить пользователя», выполненная в синем цвете. Данная кнопка предназначена для инициации процесса создания новой учетной записи администратора, что позволяет расширить круг лиц, имеющих доступ к управлению системой, и обеспечить резервирование административных полномочий.



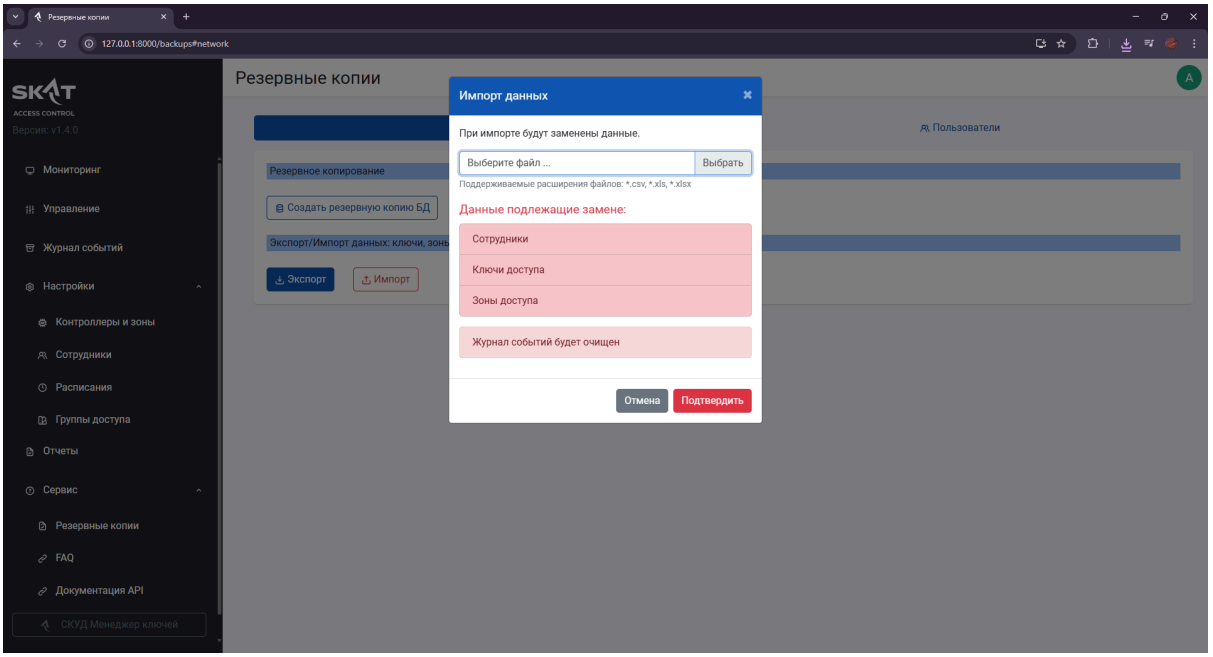
Пример импорта базы данных

Нажмите на кнопку Импорт. Откроется новое окно. Заголовок модального окна четко определяет выполняемую операцию — импорт данных. Ниже расположен текстовое сообщение: «При импорте будут заменены данные», что служит важным предупреждением для пользователя о необратимом характере данной процедуры. Это указывает на то, что все существующие записи в системе, относящиеся к импортируемым категориям, будут перезаписаны содержимым файла.

Под этим сообщением размещено поле для выбора файла, содержащее подсказку «Выберите файл...» и кнопку «Выбрать», предназначенную для открытия диалогового окна системы управления файлами. Ниже указано, какие форматы файлов поддерживаются для импорта: *csv, *xls, *xlsx.

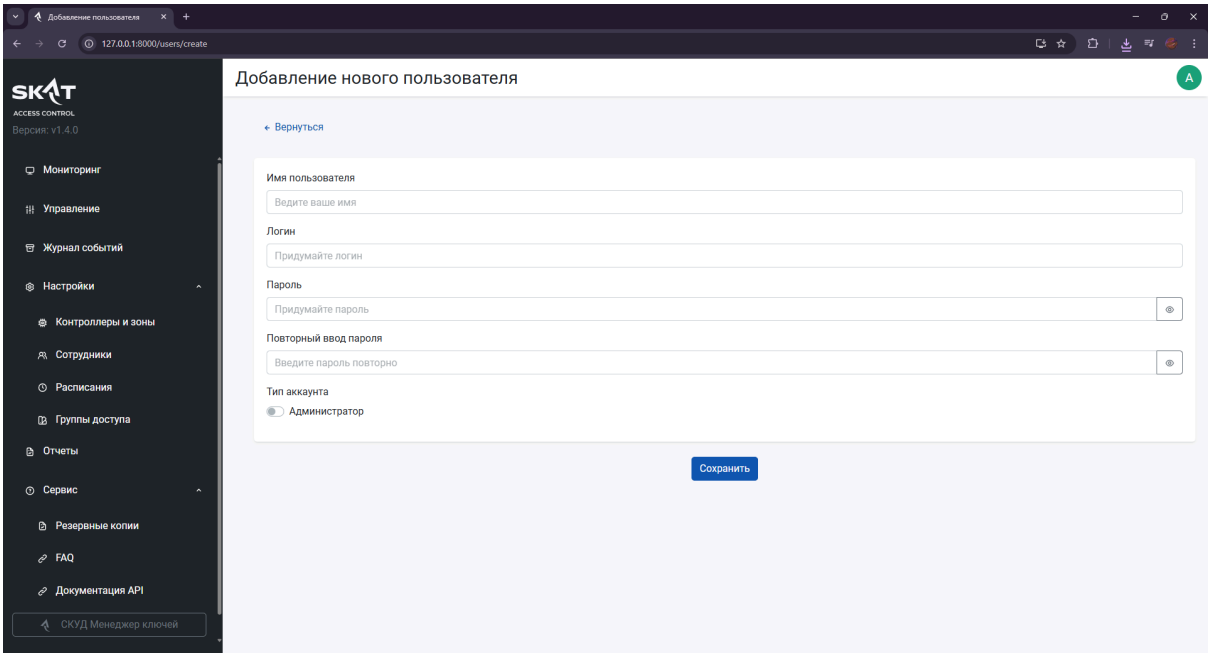
Далее следует секция с заголовком «Данные подлежащие замене:», выделенная светло-розовым фоном. В ней перечислены категории данных, которые будут затронуты процессом импорта: «Сотрудники», «Ключи доступа» и «Зоны доступа». Эти пункты указывают на то, что импорт приведет к обновлению или замене всех записей в соответствующих таблицах базы данных. Непосредственно под ними размещена дополнительная информация: «Журнал событий будет очищен», что подчеркивает серьезность операции — все исторические записи о проходах и событиях будут удалены, что необходимо учитывать при планировании восстановления.

В нижней части модального окна расположены две кнопки управления: «Отмена», выполненная в сером цвете, предназначенная для закрытия окна без выполнения импорта, и «Подтвердить», выделенная красным цветом, которая инициирует процесс импорта выбранных данных в систему. Красный цвет этой кнопки служит визуальным сигналом о критичности действия и необходимости тщательной проверки перед его выполнением.



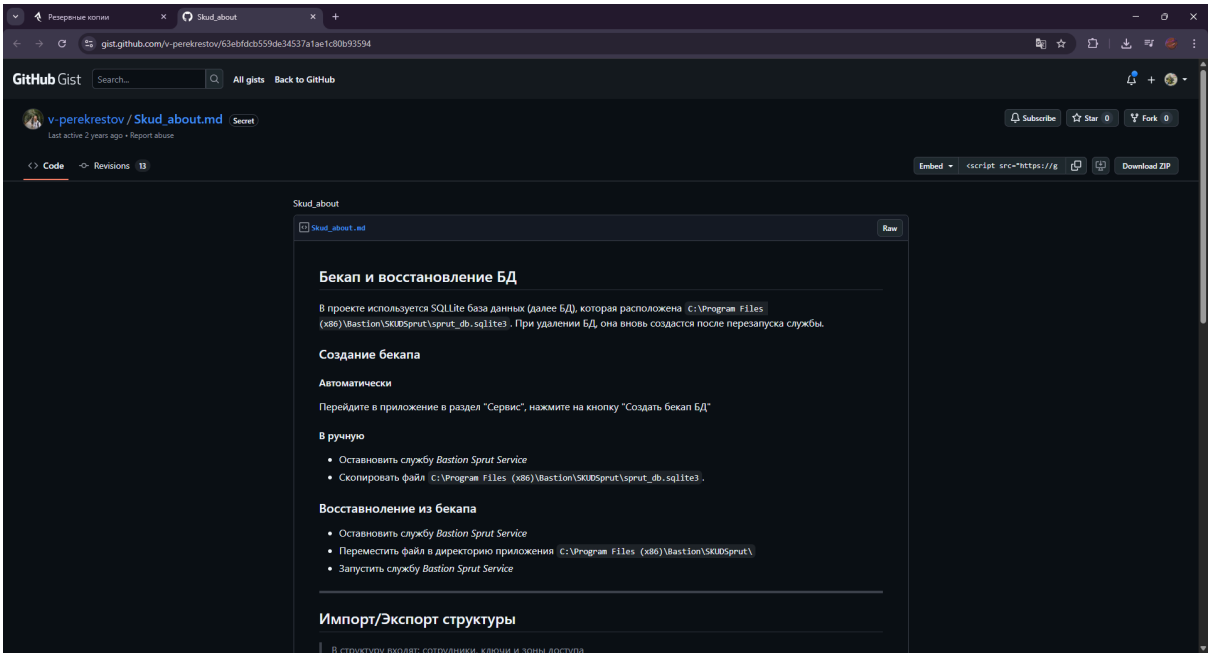
Пример добавления нового пользователя

В верхней части страницы, под заголовком «Добавление нового пользователя», расположен элемент навигации — ссылка «← Вернуться», позволяющая оператору отменить текущую операцию и вернуться к предыдущему экрану без сохранения введенных данных. Ниже размещена форма ввода персональной информации, состоящая из нескольких полей.
Первое поле — «Имя пользователя» — содержит подсказку «Введите ваше имя» и предназначено для ввода отображаемого имени, которое будет использоваться для идентификации пользователя в системе. Второе поле — «Логин» — с подсказкой «Придумайте логин» — служит для определения уникального идентификатора, по которому пользователь будет входить в систему. Третье поле — «Пароль» — с подсказкой «Придумайте пароль» — предназначено для задания секретного кода доступа. Справа от этого поля расположена иконка глаза, позволяющая временно отобразить введенный текст для проверки его корректности. Четвертое поле — «Повторный ввод пароля» — с подсказкой «Введите пароль повторно» — служит для подтверждения пароля и предотвращения ошибок при вводе.
Ниже этих полей находится блок «Тип аккаунта», содержащий переключатель типа toggle с меткой «Администратор». В данный момент переключатель находится в неактивном состоянии, что указывает на то, что создаваемый пользователь не будет иметь прав администратора. Это позволяет гибко настраивать уровень доступа в зависимости от роли пользователя.
В нижней части формы размещена кнопка «Сохранить», выполненная в синем цвете, которая служит для фиксации всех внесенных данных и создания новой учетной записи в системе.


Добавление пользователя
127.0.0.1:8000/users/create
SKAT
ACCESS CONTROL
Версия: v1.4.0
Мониторинг
Управление
Журнал событий
Настройки
Контроллеры и зоны
Сотрудники
Расписания
Группы доступа
Отчеты
Сервис
Резервные копии
FAQ
Документация API
СКУД Менеджер ключей
Добавление нового пользователя
A
Вернуться
Имя пользователя
Ведите ваше имя
Логин
Придумайте логин
Пароль
Придумайте пароль
Повторный ввод пароля
Введите пароль повторно
Тип аккаунта
Администратор
Сохранить

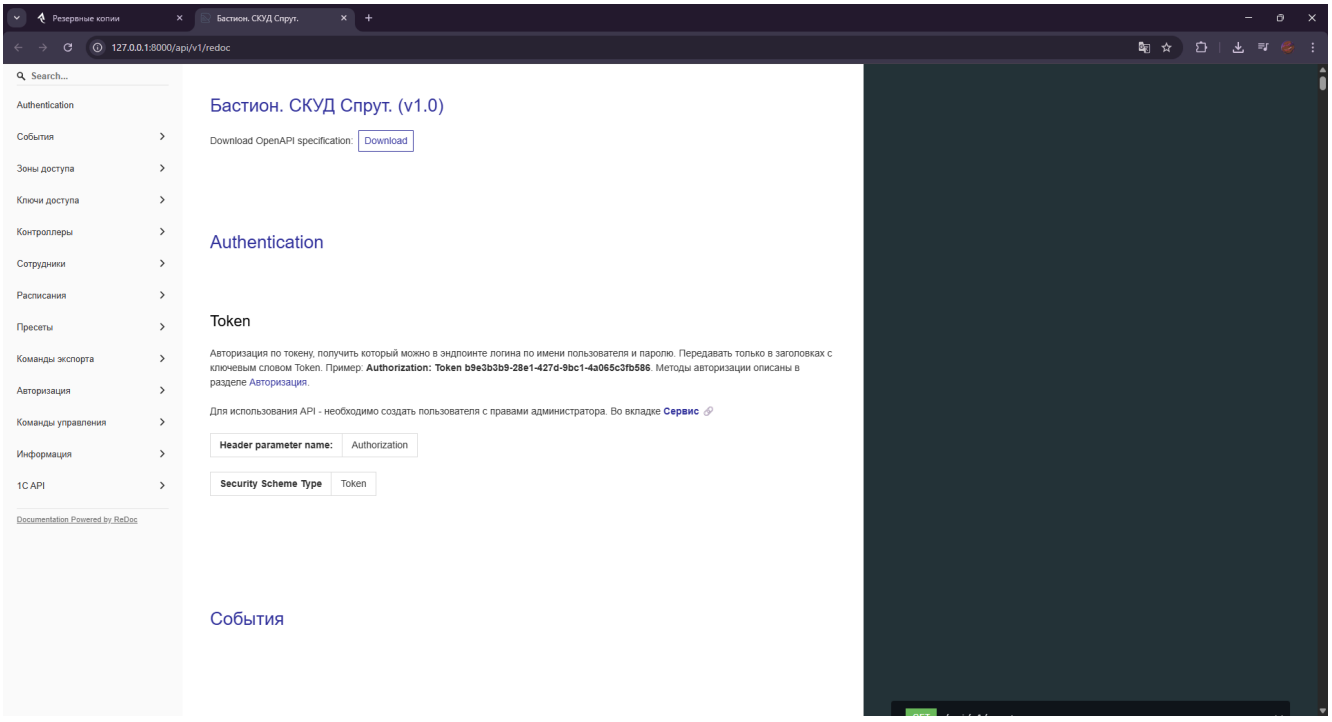
Вкладка Сервис. FAQ

При нажатии на вкладку Сервис. FAQ откроется документ. Основное содержимое документа структурировано под заголовком «Бекап и восстановление БД». В нем указано, что в проекте используется база данных SQLite. Далее следует раздел «Создание бекапа», в котором описаны два способа резервного копирования. Первый — автоматический: пользователю предлагается перейти в раздел «Сервис» внутри приложения и нажать кнопку «Создать бекап БД». Второй — ручной: требует остановки службы Bastion Sprut Service и последующего копирования файла базы данных вручную по указанному пути. Раздел «Восстановление из бекапа» содержит инструкции для восстановления системы из ранее созданной резервной копии. Ниже расположен еще один раздел — «Импорт/Экспорт структуры».



Вкладка Сервис. Документация API

В левой части экрана расположен навигационный боковой панель, содержащий список разделов документации: «Authentication», «События», «Зоны доступа», «Ключи доступа», «Контроллеры», «Сотрудники», «Расписания», «Пресеты», «Команды экспорта», «Авторизация», «Команды управления», «Информация» и «1С API». Каждый пункт снабжен стрелкой, указывающей на возможность раскрытия подразделов или перехода к детальной информации по соответствующему функционалу.
Основное содержимое страницы начинается с заголовка «Бастион. СКУД Спрут. (v1.0)». Непосредственно под ним размещена ссылка для скачивания спецификации OpenAPI в формате JSON или YAML — кнопка «Download» — что позволяет разработчику получить машинно-читаемую версию документации для автоматизации процессов интеграции.
Первый основной раздел — «Authentication» — содержит описание механизма аутентификации. Подзаголовок «Token» поясняет, что авторизация осуществляется по токену, который выдается в результате обращения к эндпоинту логина с использованием имени пользователя и пароля. Указано, что токен должен передаваться исключительно в заголовках HTTP-запросов с ключевым словом «Authorization», приведен пример корректного формата заголовка. Также отмечено, что для использования API необходимо создать пользователя с правами администратора, что может быть выполнено в разделе «Сервис» пользовательского интерфейса системы.
Ниже представлены таблицы с параметрами безопасности: «Header parameter name» со значением «Authorization» и «Security Scheme Type» со значением «Token», что формализует требования к авторизации для всех методов API.



Перепрошивка устройства

Приложение. Настройка системы с нуля

Для настройки системы контроля и управления доступом (СКУД) с нуля, при условии, что физическая установка и подключение контроллеров к сети уже выполнены, необходимо выполнить следующие шаги, начиная с настройки программного обеспечения (ПО):

1. Установка и запуск ПО "СКУД SKAT": Установите серверное программное обеспечение "СКУД SKAT" на персональный компьютер, соответствующий техническим требованиям, указанным в документе. Запустите приложение.
2. Подключение контроллеров к сети (CAN): Убедитесь, что все контроллеры подключены к общей двухпроводной CAN-шине. **Помните**, потребуется использовать CAN-USB преобразователь для подключения сети к ПК с установленным ПО.
3. Обнаружение контроллеров: После подключения контроллеров к CAN-шине и запуска ПО, они должны быть автоматически обнаружены и подключены к системе. В интерфейсе ПО появятся уведомления о подключении, для этого смотрите Журнал событий. На вкладке "Настройки. Контроллеры и зоны" все обнаруженные, но еще не распределенные контроллеры будут находиться в специальной зоне под названием "Нераспределенные контроллеры".
4. Создание логических зон: Перейдите на вкладку "Настройки. Контроллеры и зоны". Здесь необходимо создать логические зоны безопасности, соответствующие физическому расположению точек доступа (например, "Вход", "Бухгалтерия", "Производство"). Это делается с помощью кнопки "Добавить зону".
5. Назначение контроллеров зонам: Из зоны "Нераспределенные контроллеры" перетащите каждый контроллер в соответствующую ему логическую зону. Это важно, так как контроллеры в зоне "Нераспределенные контролеры" не будут получать обновления и ключи доступа сотрудников.
6. Конфигурация контроллеров: Для каждого контроллера, находящегося уже в назначенной зоне, нажмите кнопку "Изменить". Здесь можно настроить:
    - Наименование и описание: Указать уникальное имя (например, "Турникет №1") и место установки.
    - Режим работы: Выбрать тип устройства (например, "Турникет", "Шлагбаум", "Однодверный").
    - Направление прохода: Для контроллеров с двумя считывателями (например, турникет) настроить направление для Channel 1 и Channel 2 (например, "Вход", "Выход", "Без контроля направления").
7. Создание групп доступа: На вкладке "Настройки. Группы доступа" создайте группы, определяющие, к каким зонам и контроллерам имеет доступ сотрудник. Назначьте этим группам соответствующие зоны и контроллеры, а также расписания. (необязательно)
8. Создание расписаний: На вкладке "Настройки. Расписания" создайте временные шаблоны (например, "Рабочее время", "Смена 1"), указав дни недели и время действия. (необязательно)
9. Создание сотрудников: Перейдите на вкладку "Настройки. Сотрудники". Нажмите "Добавить сотрудника" и введите персональные данные (ФИО, дата рождения и т.д.).
10. Добавление и настройка ключей: После создания сотрудника, перейдите к добавлению ключа (карта, брелок). Это можно сделать на вкладке "Настройки. Сотрудники", кликнув по сотруднику и выбрав "Добавить ключ". Укажите номер ключа. Кликнув по добавленному ключу, можно настроить его тип ("Ключ доступа", "Ключ безопасности", "Универсальный ключ") и привязать к конкретным группам доступа, что **обязательно**.
11. Назначение прав доступа: Свяжите сотрудников (через их ключи) с группами доступа, а группы доступа — с расписаниями. Это определит, кто, куда и когда может пройти.
12. Проверка и мониторинг: Используйте вкладки "Мониторинг" и "Журнал событий", чтобы отслеживать текущее состояние системы, проходы, тревоги и другие события.

Таким образом, процесс сводится к запуску ПО, интеграции обнаруженных контроллеров в иерархию зон, их детальной настройке, созданию пользователей и ключей, а также определению прав доступа через группы и расписания.

Приложение. Частые вопросы?

1. Добавил ключ, но система не пропускает? - Проверьте, что ключ имеет привязку к нужной зоне (в сетевом режиме). В автоном режиме попробуйте запрограммировать ключ еще раз, возможно повреждение считывателя или поломка карты доступа.
2. Контроллер издает периодически звуковую индикацию? - Проверьте то на линии считывателя нет короткого замыкания (звуковой сигнал будет издаваться с периодичностью в 5 секунд)
3. Контроллер издает длительный звуковой сигнал? - Проверьте, что к каналу со считывателем подключена перемычку между SENS и GND или соединение подключенного датчика.
4. Контроллер не реагирует на поднесение карты? - Проверьте, что пожарный шлейф подключен и целостность линии не нарушена или контакт перемычки в К1, при отсутствии подведенного шлейфа.
5. Новые события не отображаются в журнале событий? - Проверьте соединение на линии CAN. Можно проверить на вкладке Контроллеры и зоны состояние контроллеров. Контроллеры, находящиеся на линии отображены с зеленой иконкой.
6. Нет нужного типа контроллера (турникета, шлагбаума и т.д) - проверьте перемычки на плате и сверьте его с описанием внутри руководства
7. Отчет выгружается пустой? - проверьте настройку контроллеров во вкладке Контроллеры и зоны. У контролеров на входе\выходе объекта должна быть отмечена галочка внешний периметр. Настроены вход и выход. У остальных контроллеров - нет (не должно быть настроено)!
8. Возникает ошибка при постановке объекта на охрану - проверьте целостность линии охранного шлейфа
9.