



СЕТЕВОЙ КОНТРОЛЛЕР СКУД SPRUT PACS

РУКОВОДСТВО
ПОЛЬЗОВАТЕЛЯ
WEB-ПРИЛОЖЕНИЯ

ОГЛАВЛЕНИЕ

Термины	3
Технические требования к ПО	5
Назначение ПО	6
CAN-сеть и USB-CAN адаптер	7
Установка приложения	7
Первая авторизация	8
Управление пожарной и охранной сигнализацией	9
Меню КОНТРОЛЛЕРЫ И ЗОНЫ	10
Определение сети контроллеров	10
Меню СОТРУДНИКИ.	11
Создание и управление записью сотрудника	11
Типы ключей доступа	11
Создание и редактирование ключей доступа	12
Создание пресета на основании данных сотрудника	12
Меню ЖУРНАЛ СОБЫТИЙ	13
Мониторинг и типы событий	13
Меню РАСПИСАНИЯ.....	15
Меню ПРЕСЕТЫ	16
Создание / редактирование Пресетов	16
Меню СЕРВИС	18
Типы аккаунтов пользователей	18
Создание и управление аккаунтами пользователей.....	20
Создание резервных копий БД	20
Создание резервных копий ключей.....	21
Меню Отчеты	21

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 клиент взаимодействует с WEB-сервером 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 пропуске/отказе пропуска человека по ключу с регистрацией данного события в системе.

Точка прохода - физическое препятствие, оснащённое контроллером доступа и считывателем, которые осуществляют или запрещают доступ в охраняемую зону после проведения процедуры идентификации. Точкой прохода может быть дверь, турникет, шлагбаум, ворота, шлюз и т.п.

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 контроллера / зоны. В системе SPRUT СКУД 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

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ К ПО

Кроссплатформенное WEB-приложение СКУД SPRUT устанавливается на компьютеры пользователя под управлением операционных систем Windows или Unix (Ubuntu, Debian). 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 осуществляется на любых свободных, не занятых портах компьютера, на котором оно запущено. Например, порт по умолчанию для:

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

НАЗНАЧЕНИЕ ПО

WEB-приложение предназначено для:

- конфигурации контроллеров;
- удаленного мониторинга оборудования и событий системы;
- управления расписанием работы контроллеров;
- создание авторизованных ключей для управления доступом людей в различные зоны и отдельные точки прохода.

Каждому контроллеру можно присвоить имя. Несколько контроллеров можно объединить в логические зоны, внутри которых, в зависимости от конфигурации объекта, допускаются другие вложенные зоны.

После установки контроллеров на объекте и построения логических зон в WEB-приложении, пользователь должен 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.

CAN-СЕТЬ И USB-CAN АДАПТЕР

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.

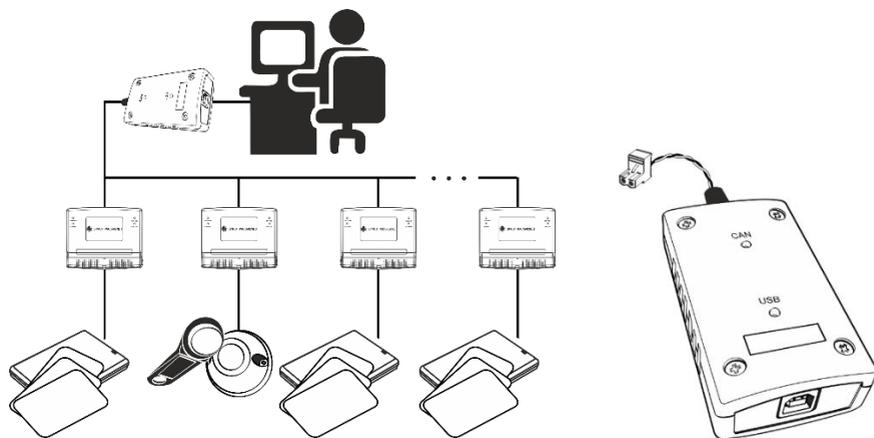


Рисунок 1 CAN-сеть и USB-CAN адаптер

УСТАНОВКА ПРИЛОЖЕНИЯ

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.

ПЕРВАЯ АВТОРИЗАЦИЯ



Рисунок 2 Окно авторизации

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

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.

Управление пожарной и охранной сигнализацией

В боковом меню пользователя Администратор располагаются 2 кнопки, которые выполняют групповые действия для всех контроллеров сразу:

- Постановка на охрану всей сети
- Включение пожарной сигнализации

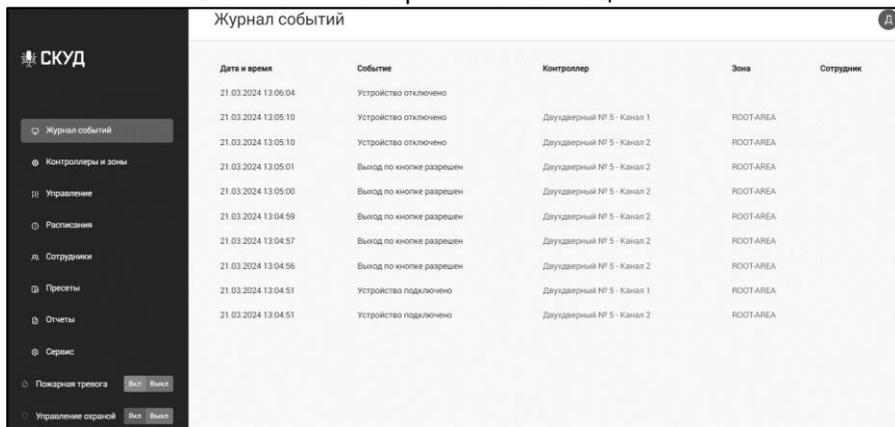


Рисунок 3 Главный экран администратора

Команда постановки на охрану сети имеет высший приоритет над всеми контроллерами и расписанием работы самого контроллера.

При включении пожарной сигнализации все контроллеры отключаются и позволяют проход через себя.

Активирование этих функций защищены дополнительными модальными окнами с подтверждением их включения:

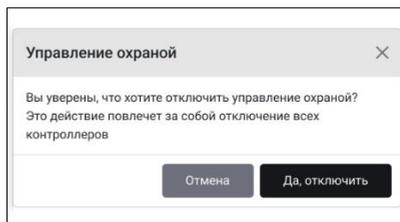
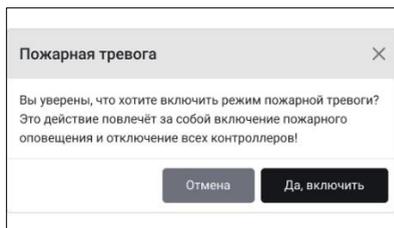


Рисунок 4 Окна подтверждений включения действий верхнего уровня

МЕНЮ КОНТРОЛЛЕРЫ И ЗОНЫ

Определение сети контроллеров

Определение наличия в сети контроллеров происходит автоматически. После сканирования CAN-сети найденные

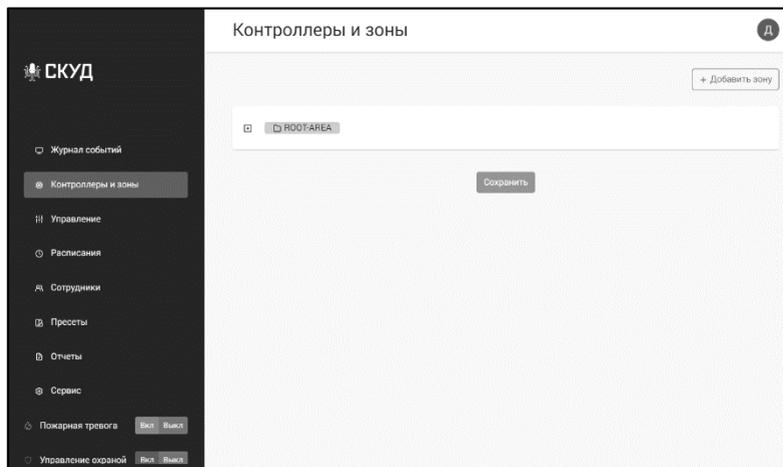


Рисунок 5 Раздел меню Контроллеры и зоны. Сканирование сети

контроллеры записываются в БД. При нахождении контроллеров им присваивается имя по умолчанию, формируемое по маске “Контролер” + “<id>”.

После определения контроллера его имя можно отредактировать. Контроллеры могут работать самостоятельно или объединяться в логические зоны, причем их вложенность может быть неопределенной глубины. Таким образом, зона - это логическое понятие, объединяющее контроллеры с общими свойствами в группы.

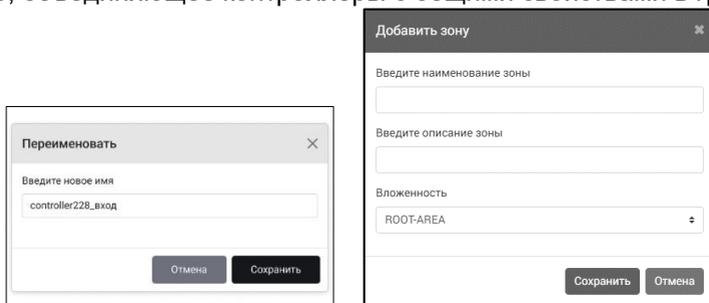


Рисунок 6 Просмотр и редактирование информации о контроллере и зоне

Перемещение контроллеров и зон между собой возможно перетягиванием мышью методом drag and drop.

МЕНЮ СОТРУДНИКИ.

Создание и управление записью сотрудника

Для введения в БД WEB-приложения записи о новом сотруднике в разделе меню СОТРУДНИКИ требуется нажать кнопку «+ добавить сотрудника», после чего раскроется экран карточки сотрудника. Каждая карточка несёт в себе следующую информацию: Фамилия Имя Отчество, дата рождения. Доступ к карточке сотрудника также возможен прямо из списка сотрудников двойным нажатием на записи сотрудника. В правом верхнем углу расположена кнопка управления правами доступа с двумя возможными состояниями: **«Заблокировать сотрудника»** / **«Активировать сотрудника»**.

Типы ключей доступа

В WEB-приложении используется 3 типа ключей доступа:

- **Ключ доступа** - данный тип ключей обеспечивает проход через соответствующие зоны/контроллеры в разрешённое для него по расписанию время, при условии снятия с охраны всей системы.
- **Ключ безопасности** - ключ обеспечивает **постановку** на охрану контроллер/зону, во время, разрешённое 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, разрешённое ему по расписанию.

Создание и редактирование ключей доступа

Ключи доступа создаются в карточке сотрудника и добавляются нажатием кнопки «+ **добавить ключ**». В открывшемся окне вводится вручную либо посредством считывающего устройства уникальный номер ключа с последующим сохранением результатов.



Рисунок 7 Экраны добавления ключа

У одного сотрудника может быть любое количество ключей, с различными типами, правами доступа и расписанием (оптимально не более 5 ключей).

Закрытие карточки сотрудника возвращает к списку сотрудников, которым предоставлены ключи, с отображением текущего состояния прав доступа (**Активен** либо **Заблокирован**).

В системе может быть зарегистрировано до 1000 ключей доступа.

В карточке сотрудника существует кнопка для сохранения набора прав доступа к различным зонам и по различным расписаниям в виде **пресета** для дальнейшего его использования для программирования прав другого пользователя.

Создание пресета на основании данных сотрудника

После выбора типа ключа выбирается соответствующий пресет, с уже заполненными данными по одному из 7 расписаний и маршрутами доступа через зоны/контроллеры для сотрудника. В противном случае вся эта информация заполняется вручную, с последующей возможностью создать из неё пресет (шаблон) для других сотрудников.

ВНИМАНИЕ! Сотрудника или ключ нельзя удалять, можно изменить его активность. При отключении активации у сотрудника пропадает активация всех его ключей, при этом невозможно будет добавить новый ключ или активировать ключ у данного сотрудника. Также есть атрибут активации у самого ключа.

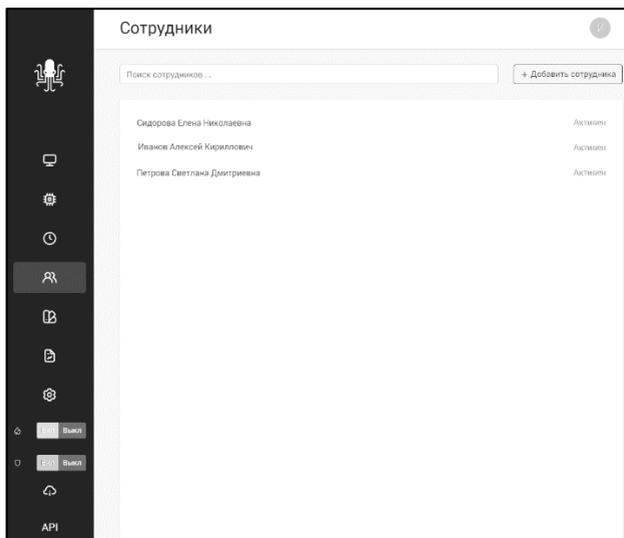


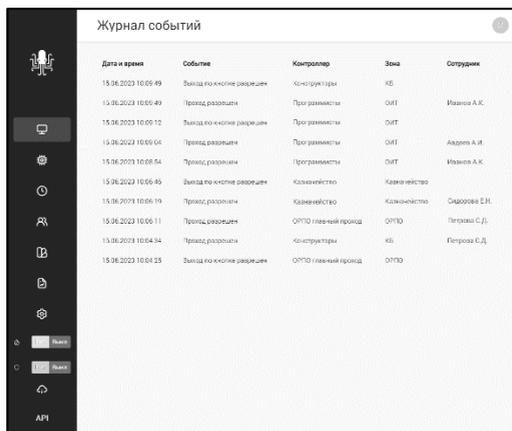
Рисунок 8 Создание и управление пользователями

МЕНЮ ЖУРНАЛ СОБЫТИЙ

Мониторинг и типы событий

Мониторинг событий - главный экран приложения, после авторизации пользователь попадает на него. На нём отображаются все текущие события CAN-сети. В случае отсутствия событий в системе мониторинга выводится соответствующее уведомление.

Количество событий в таблице мониторинга ограничено значением 20 000 сообщений:



Дата и время	Событие	Контроллер	Зона	Ситуация
15.06.2023 10:09:49	Выход по кнопке разрешен	Чис-структуры	КБ	
15.06.2023 10:09:49	Пропуск разрешен	Про-рамессты	СИТ	Иванов А.К.
15.06.2023 10:09:12	Выход по кнопке разрешен	Про-рамессты	СИТ	
15.06.2023 10:09:04	Пропуск разрешен	Про-рамессты	СИТ	Авдеев А.И.
15.06.2023 10:09:04	Пропуск разрешен	Про-рамессты	СИТ	Иванов А.К.
15.06.2023 10:06:46	Выход по кнопке разрешен	Кальвайнство	Кальвайнство	
15.06.2023 10:06:19	Пропуск разрешен	Кальвайнство	Кальвайнство	Сидоров Е.И.
15.06.2023 10:06:11	Пропуск разрешен	ОПТО главный проход	ОПТО	Петрова С.Д.
15.06.2023 10:04:34	Пропуск разрешен	Кальвайнство	КБ	Петрова С.Д.
15.06.2023 10:04:23	Выход по кнопке разрешен	ОПТО главный проход	ОПТО	

Рисунок 9 Экран мониторинга событий

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. Удалённое (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

МЕНЮ РАСПИСАНИЯ

Расписание — это режим работы всей сети CAN, т. е. всех её контроллеров. Всего доступно 7 расписаний для различных групп пользователей. Каждое расписание задаётся на все дни недели. Дни недели могут быть выходными (с запретом доступа) или рабочими, с доступом в указанное рабочее время. Расписания можно редактировать (менять названия, недельный график и время доступа).

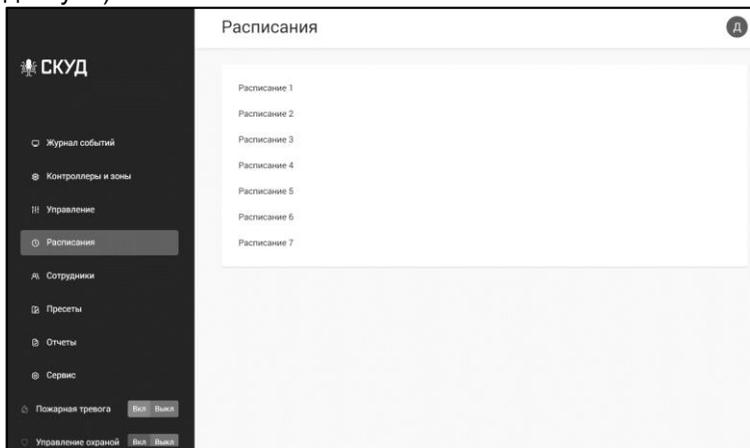


Рисунок 10 Список расписаний

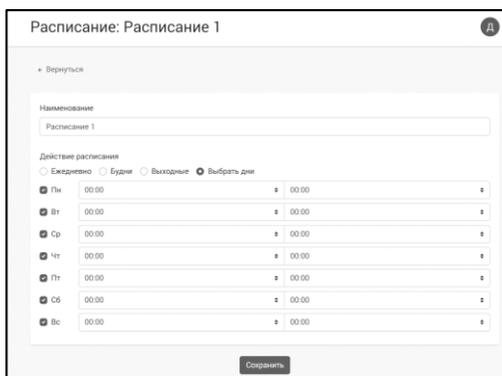


Рисунок 11 Редактирование расписания

МЕНЮ ПРЕСЕТЫ

Создание / редактирование Пресетов

Пресет - это сохранённый шаблон, помогающий быстро запрограммировать свойства ключей доступа для сотрудников с одинаковыми расписаниями и маршрутами следования через зоны/контроллеры. Свойства пресета определяются один раз при вводе прав доступа для ключа сотрудника в карточке Сотрудника (раздел меню Сотрудники) и сохраняются как пресет под своим собственным уникальным названием, удобным для пользователя.

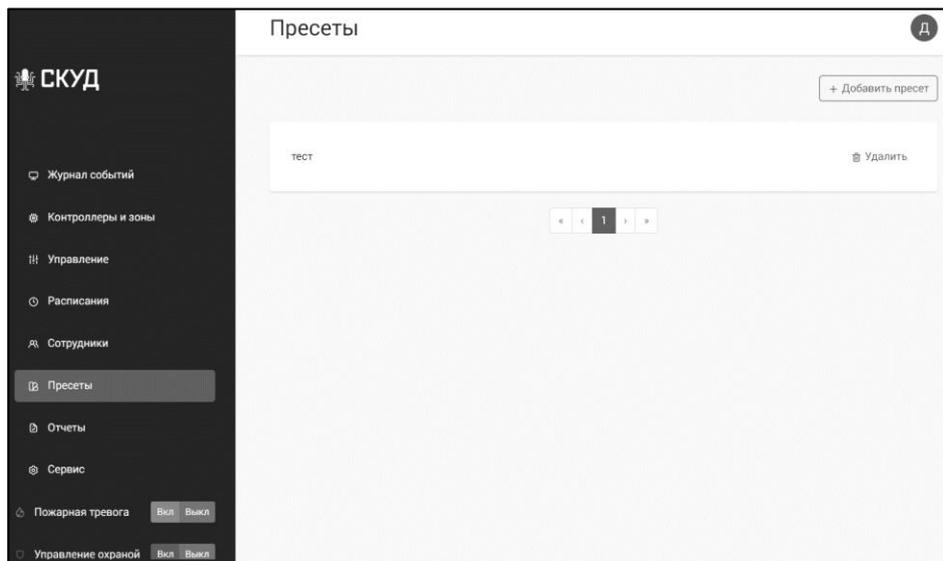


Рисунок 12 Список пресетов

Пресет можно удалять и изменять при этом настройке пользовательских ключей, которые ранее были созданы по данному пресету, не пострадают. Предполагается, что оптимальное число пресетов будет до 30 штук.

Добавить новый пресет

← Вернуться

Наименование
Введите наименование пресета

Расписание
Без расписания

Контроллеры и зоны
 ROOT-AREA

Пн	00:00	⇅	00:00	⇅
Вт	00:00	⇅	00:00	⇅
Ср	00:00	⇅	00:00	⇅
Чт	00:00	⇅	00:00	⇅
Пт	00:00	⇅	00:00	⇅
Сб	00:00	⇅	00:00	⇅
Вс	00:00	⇅	00:00	⇅

Сохранить

Рисунок 13 Создание и редактирование пресета

Добавление и редактирование пресета выглядят одинаково.

МЕНЮ СЕРВИС

Экран настройки представляет собой системный раздел для редактирования прав доступа и обслуживания системы.

На данном экране будет расположен список пользователей, у которых есть аккаунт и доступ в WEB-приложение. Оптимальное количество пользователей системы не более 10. Пользователей можно создавать/удалять и менять информацию о них.

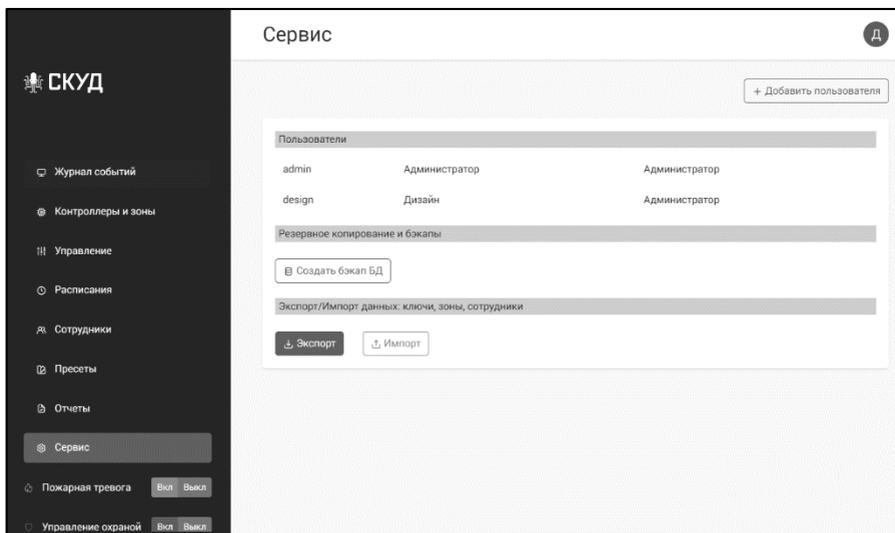


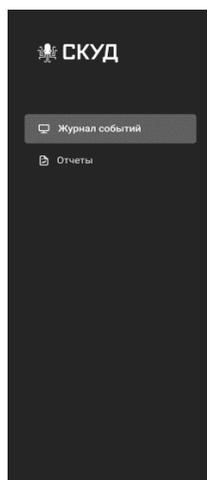
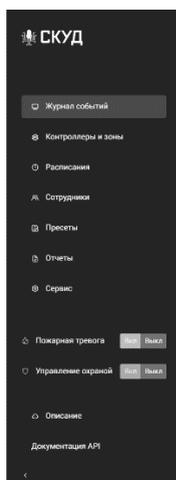
Рисунок 14 Экран меню Сервис

Типы аккаунтов пользователей

Аккаунты пользователей бывают двух типов: Администратор и Пользователь. В аккаунтах с правами доступа Администратор осуществляется первый запуск (аккаунт Admin), создание новых аккаунтов администраторов и пользователей с назначением им паролей. Так же в этом аккаунте производятся настройки параметров программы и отображаются кнопки запуска охранной и пожарной сигнализации.

В аккаунте с правами «Пользователь» возможны только просмотр журнала событий и доступ к отчётам программы.

ВНИМАНИЕ! Восстановление забытого пароля аккаунта пользователя невозможно. Это реализуется через средство восстановления паролей, вызываемого из административного аккаунта, который прошёл успешную авторизацию. Создание пользователей и сброс их паролей доступен только администраторам системы, после их авторизации в системе.



Создание и управление аккаунтами пользователей

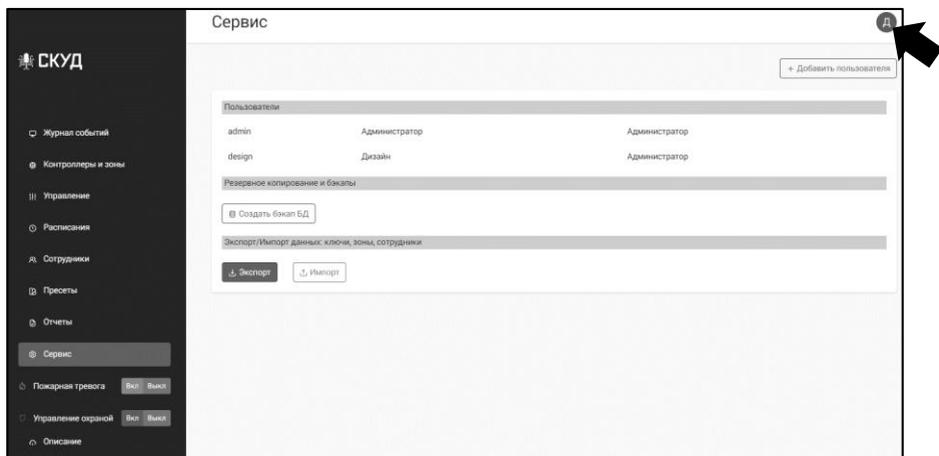


Рисунок 15 Экран меню Сервис и кнопка аватара

По нажатию на кнопку аватара в правом верхнем углу, откроется информация об аккаунте пользователя:

Добавление нового пользователя

← Вернуться

Имя пользователя
Введите ваше имя

Логин
Придумайте логин

Пароль
Придумайте пароль

Повторный ввод пароля
Введите пароль повторно

Тип аккаунта
 Администратор

Сохранить

Рисунок 16 Создание нового пользователя

Создание резервных копий БД

Создание резервных копий может быть выполнена по 2м сценариям:

- Принудительное создание резервной копии (резервной копии БД)
- По расписанию

Принудительное создание резервной копии создаст копию файла базы данных SQLite в директорию установленного ПО каталог **Загрузки**.

Создание резервных копий ключей

Данный метод экспортирует файл в формате txt, со списком ключей, которые существуют во всех контроллерах.

МЕНЮ ОТЧЁТЫ

Благодаря сквозному мониторингу реализован функционал отчётности, в различных разрезах, в том числе и учёт рабочего времени. Для его учёта контроллеры имеют признак “Главный вход” + направление прохода “Вход” / “Выход” или “Проходной”, разница во времени “Входа” и “Выхода” конкретного ключа считается рабочим временем, в случае работы контроллера в режиме “Проходной” учитывается направление прохода, в таком случае учёт рабочего времени должен осуществляться между двумя соседними событиями.

Существуют отчёты (названия могут меняться):

- Учёт рабочего времени
- История прохода по сотруднику (ключу) в разрезе времени.



изготовитель

а/я 7532, Ростов-на-Дону, 344018
(863) 203-58-30

bast.ru — основной сайт
teplo.bast.ru — для тепла и комфорта
dom.bast.ru — решения для дома
skat-ups.ru — интернет-магазин

тех. поддержка: 911@bast.ru
отдел сбыта: ops@bast.ru
горячая линия: 8-800-200-58-30

Формат А5
ФИАШ.425619.039 РЭ

