GUARDSaaS

Облачная СКУД GuardSaaS

Руководство пользователя

iron Logic

2026

Оглавление

О СЕРВИСЕ GUARDSAAS 5

Что такое SaaS? 5
СКУД просто и недорого 5
Варианты использования 5
Каковы преимущества SaaS? 5
Безопасность данных SaaS 5
Хранение данных 6
Что происходит при отключении интернета или электричества? 6

РЕГИСТРАЦИЯ 7

СОСТАВ ОБОРУДОВАНИЯ ДЛЯ РАБОТЫ С GUARDSAAS 7

НАСТРОЙКА ОБОРУДОВАНИЯ ДЛЯ РАБОТЫ В СИСТЕМЕ GUARDSAAS 8

Настройка конвертера Z-397 (мод. Web) 8
Настройка IP-контроллеров *Z-5R (мод. Web), Z-5R (мод. Web BT)*, *Matrix-II (мод. E K Wi-Fi)* и *Z-5R (мод. Wi-Fi)* 9

ВХОД В АККАУНТ 10

Восстановление логина/пароля 10
Потеря доступа к аккаунту 10
Защита учетной записи от потери или кражи 10

ВКЛАДКА «ОБОРУДОВАНИЕ» 11

Список конвертеров 11
Добавить новый конвертер 11
Не получается зарегистрировать конвертер. 12
Проверка настройки конвертера (IP-контроллера) ***12***
Почему конвертер Z-397 (мод. WEB) не «видит» контроллеры? 13
Детали (Параметры конвертера) 14
Ключ шифрования ***14***
Описание ***14***
Таймзона ***15***
Удалить ***15***
Синхронизация 15
Синхронизировать всё ***15***
Синхронизация. Зачем и когда ее делать ***15***
Список контроллеров 16
Подключение контроллеров 16
Кнопка «Параметры» (Параметры контроллера) 17
Кнопка «Объекты» 18
Кнопка «Режимы» 19
Текущий режим ***19***
Расписание режимов ***19***
Кнопка «Камеры» 20
Кнопка «Открыть дверь» 20
Кнопка «Синхронизировать контроллер» 21
Обновление прошивок оборудования 22
Рекомендуемые версии прошивок 22
Инструкция по прошивке конвертера Z-397 (мод. WEB) 22
Инструкция по прошивке контроллеров Z-5R (мод. Net), Z-5R (мод. Net 8000), Z-5R (мод. Net 16000), Matrix-II (мод. E K Net), Matrix-VI (мод. EH K Net) 23
Инструкция по прошивке IP-контроллеров Z-5R (мод. Web), Z-5R (мод. Web BT), Matrix-II (мод. E K Wi-Fi), Z-5R (мод. Wi-Fi) 23
Проблемы связи оборудования с сервером 23
Решение проблемы связи Конвертера Z-397 (мод. Web) (модуля связи IP-контроллеров) 24
Решение проблемы связи Контроллеров 24

ВКЛАДКА «ОБЪЕКТЫ» 25

Добавление объекта 25
Контроллеры 25
Временные зоны 26

ВКЛАДКА «ОТДЕЛЫ» 28

Добавление отдела 28
Распорядок работы 28
Управление доступом 29

Кнопка «Посмотреть» ... 30
Кнопка «Редактировать» ... 30
Кнопка «Удалить» ... 31
Почему некоторые отделы в списке отмечены красным цветом? ... ***31***

ВКЛАДКА «СОТРУДНИКИ» ... **32**

Добавление сотрудников ... 32
Редактирование сотрудников ... 33
Кнопка «Записать карты в контроллеры» ... 34
Удаление сотрудников ... 34
Восстановление удаленных сотрудников ... 34
Назначение карты ... 36
Ручной ввод номера карты ... 37
Автоматический ввод карты ... 38
Ввод карты через USB считыватель ... 39
Групповое редактирование карт ... 41
Групповое удаление выбранных сотрудников с картами ... ***41***
Групповое редактирование карт у выбранных сотрудников ... ***41***
Деактивация карты ... 42
Удаление карты ... 42
Возможные проблемы при назначении карт и работе с ними ... 43
Проблемы с синхронизацией карт ... ***43***
Не получается зарегистрировать новую карту ... ***43***
Не отображается код карты при поднесении к считывателю ... ***43***
После регистрации новой карты она не открывает дверь ... ***43***
Почему некоторые сотрудники в списке отмечены красным цветом? ... ***44***
Как узнать, какому сотруднику принадлежит карточка? ... ***44***
Импорт/ Экспорт сотрудников ... 45
Импорт ... 45
Экспорт ... 46

ВКЛАДКА «КАБИНЕТ» ... **47**

Общие настройки ... 47
Настройки отчетов ... 48
Рекомендации по настойке отчетов ... 49
Ключ доступа (для получения отчетов без логина) ... 50
Настройка уведомлений ... 51
Получение отчета по HTTP запросу ... 55
Пользователи ... 56
Добавление пользователей системы ... 56
Мой счёт ... 57
Пополнить счёт ... 58
Обещанный платёж ... 59
Поделиться балансом ... 60
Сообщения ... 60
Шлюз СМС ... 60
СМС через шлюз Вашего мобильного оператора ... 61
Использование СМС шлюза с собственным логином ... 61
Прямые СМС ... 61
Списание оплаты за СМС и возврат денег ... 61

ВКЛАДКА «ОТЧЁТЫ» ... **62**

События ... 63
Отчёт «События» ... 63
Добавление события вручную ... ***63***
Редактирование событий ... ***65***
Удаление событий ... ***65***
Отчёт «Фотоверификация» ... 66
Табель ... 67
Отчёт «Табель» ... 67
Отчёт «Приходы и уходы» ... 68
Статистика ... 69
Отчёт «Статистика» ... 69
Отчёт «Посещаемость» ... 70
Отчёт «Дисциплина» ... 70
Отчёт «Использование карт» ... 71
Перемещения ... 71
Отчёт «Перемещения» ... 71
Отчёт «Посещения» ... 71

Отчёт «На объекте» ... 71
ВСПОМОГАТЕЛЬНЫЕ ОТЧЕТЫ ... 72
Отчёт «Права доступа» ... 72
НАИБОЛЕЕ ЧАСТЫЕ ПРОБЛЕМЫ С ОТЧЕТАМИ ... 72
Дата и время событий указаны наперёд (из будущего) ... 72
Смещение времени событий ... 72
В списке событий не показывает фамилию сотрудника ... 72
«Ключ не найден», но Имя сотрудника указано ... 73
Отчеты пустые, не показывается информация ... 73
В отчетах «Табель», «Приходы и уходы» и других нет данных за текущий день, или они неполные. ... 73
ВКЛАДКА «ГЛАВНАЯ» ... 74
НОВОСТИ ... 74
ИНФОРМАЦИЯ ... 75
СМЕНА ПАРОЛЯ АККАУНТА ... 75
ИНТЕГРАЦИЯ GUARDSAAS И СИСТЕМ ВИДЕОНАБЛЮДЕНИЯ ... 76
КАМЕРЫ ... 76
УНИВЕРСАЛЬНЫЙ HTML ... 77
MYSPOTCAM ... 78
IVIDEON ... 79

О сервисе Guardsaas

Что такое SaaS?

SaaS (Software as a Service) - это модель использования бизнес-приложений в качестве интернет-сервисов. SaaS приложения работают на сервере SaaS-провайдера, а пользователи получают к ним доступ через интернет-браузер. Пользователь не покупает SaaS-приложение, а арендует его - платит за его использование некоторую сумму в месяц. Таким образом достигается экономический эффект, который считается одним из главных преимуществ SaaS. SaaS провайдер заботится о работоспособности приложения, осуществляет техническую поддержку пользователей, самостоятельно устанавливает обновления. Таким образом, пользователь меньше думает о технической стороне вопроса, а сосредотачивается на своих бизнес-целях.

СКУД просто и недорого

Контроль доступа и учет рабочего времени.
Без установки сервера и ПО:

- 1 дверь - 1 контроллер;
- от 1 до 16 точек прохода на 1 конвертер;
- до 2,000 / 5,000 / 8,000 карт в зависимости от типа контроллера;
- подключение удаленных точек прохода по IP, WiFi, 3G;
- управление через Интернет;
- АВТОНОМНАЯ работа оборудования - не нужен сервер на объекте;
- отчеты о проходах и контроль рабочего времени, фото верификация;
- уведомления по email и СМС.

Варианты использования

- Офис (офисный центр с арендаторами с разделением доступа).
- Жилой дом / домофон (многоквартирный, несколько подъездов).
- Паркинги.
- Распределенные помещения (офисы, магазины, склады) с общим управлением.
- Неприспособленные помещения (подвалы, чердаки).
- Школы (СМС родителям при проходе ребенка).
- Учет рабочего времени БЕЗ управления доступом.
- Спортивные и др. клубы (карты с ограничением по времени/числу проходов).
- Гостиницы.

Каковы преимущества SaaS?

Основные преимущества SaaS над традиционным программным обеспечением:

- более низкая стоимость владения;
- более короткие сроки внедрения;
- низкий порог входа (можно быстро и бесплатно протестировать);
- задачи по поддержке и обновлению системы полностью ложатся на плечи SaaS-провайдера;
- полная мобильность пользователя, ограниченная лишь «интернет-покрытием»;
- поддержка географически распределенных компаний и удаленных сотрудников;
- низкие требования к мощности компьютера пользователя;
- кроссплатформенность.

Безопасность данных SaaS

Безопасность является важным фактором для компьютерных систем, особенно SaaS. SaaS провайдер имеет все возможности и делает все необходимое, чтобы данные, хранимые у него клиентами, находились в полной безопасности. Для этого он предпринимает ряд мер и процедур, таких как:

- регулярное резервное копирование данных;
- шифрование данных и каналов связи;

- ограниченный доступ к данным;
- профессиональная настройка файрволов и другого программного обеспечения серверов;
- регулярные аудиты по безопасности.

То есть технологически SaaS провайдер в подавляющем большинстве случаев может обеспечить большую сохранность и безопасность данных, чем конечный пользователь.

Хранение данных

- Данные хранятся в полностью безопасном дата-центре в России;
- Обмен данными с сервером происходит по защищенному протоколу https;
- Данные хранятся в реляционной базе, поддерживающей их целостность;
- Установлена процедура регулярного резервного копирования;
- Доступ пользователей к данным происходит только при условии аутентификации с подтверждением логина по электронной почте.

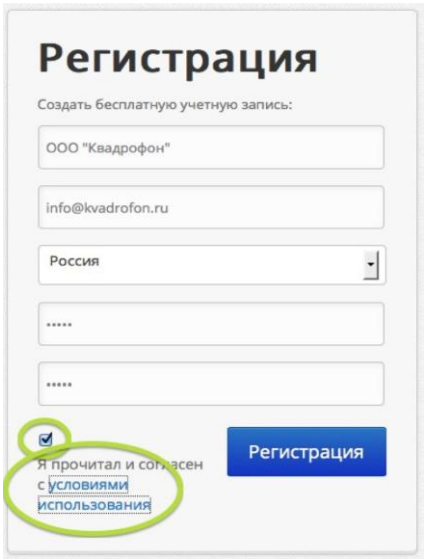
Специфика GuardSaaS в том, что оборудование работает независимо (offline). Соединение с сервером нужно только для того, чтобы изменять настройки системы (прописывать и удалять карты из памяти контроллеров) и для передачи на сервер журналов (логов) событий. Таким образом, при временном нарушении связи с сетью безопасность и работоспособность системы не страдает.

Что происходит при отключении интернета или электричества?

Как ведет себя система при чрезвычайных ситуациях, например, отключении интернета или электричества?

При отключении связи с сервером контроллеры продолжают работать, записывая происходящие события во внутреннюю память. Размер памяти зависит от типа контроллера, и может быть от 2 до 32 тысяч событий. При появлении связи с сервером накопленные события передаются на сервер. Если отключение связи было продолжительное время, то внутренняя память может переполнится, и часть событий может пропасть. Если во время обрыва связи пропадает питание контроллера, то накопленные события пропадают. Поэтому, для надежности рекомендуется обеспечить контроллеры системой бесперебойного питания. При появлении питания система возвращается к нормальной работе автоматически.

Регистрация



Для начала работы с системой GuardSaaS нужно зарегистрироваться. Вам необходимо иметь действующий ящик электронной почты, зарегистрированный с территории России или СНГ. IP-адрес компьютера должен совпадать со страной регистрации. Затем проведите регистрацию в app.guardsaas.ru на эту электронную почту.

РЕГИСТРАЦИЯ ДОЛЖНА ПРОВОДИТЬСЯ БЕЗ ВКЛЮЧЕННОГО VPN!!!

Перейдите по ссылке https://app.guardsaas.ru/register/ и введите:

- Ваше имя или название организации
- Адрес электронной почты
- Вашу страну
- Пароль

Прочитайте правила (условия использования) и поставьте галочку рядом с «Я прочитал…». Затем нажмите кнопку «Регистрация». Система примет данные и отправит электронное письмо по указанному Вами адресу. Чтобы продолжить регистрацию, Вам необходимо найти это письмо и перейти по ссылке, которая в нем содержится. Вы автоматически войдете в систему.

На этом регистрация окончена. Запомните или запишите Ваш логин (E-mail) и пароль.

Запомните ссылку https://app.guardsaas.ru/ для последующего входа в систему.

Состав оборудования для работы с GuardSaaS

Список оборудования зависит от количества точек прохода. На каждую точку прохода устанавливается контроллер с 1-м или 2-мя считывателями (снаружи и внутри помещения) и замок при необходимости (магнитный, электромеханический или электрозащелка). Контроллер может быть либо обычный сетевой (**Matrix-II (мод. E K Net)**, **Matrix-III (мод. MF K Net)**, **Matrix-VI (мод. NFC K Net)**, **Matrix-VI (мод. EH K Net)**, **Z-5R (мод. Net)**, **Z-5R (мод. Net 8000)**, **Z-5R (мод. Net 16000)**, **Guard (мод. Net)**, **Z-Eurolock**.) либо IP-контроллер (**Z-5R (мод. Web)**, **Z-5R (мод. Web BT)**, **Matrix-II (мод. E K Wi-Fi)**, **Z-5R (мод. Wi-Fi)**). Выбирается контроллер исходя из удобства монтажа и подключения проводов. IP-контроллеры могут работать по сети ethernet или подключаться к точке доступа Wi-Fi.

См. https://ironlogic.ru/il_new.nsf/htm/ru_net_controllers

Для обычных контроллеров нужен как минимум один Web-конвертер (**Z-397 (мод. Web)**) на офис. Контроллеры подключаются к конвертеру по витой паре (RS-485) с соблюдением Общих рекомендаций по монтажу.

См. https://ironlogic.ru/il_new.nsf/htm/ru_converts

Считыватели выбираются исходя из типа ключей и требуемого уровня безопасности. Бывают простые (Em-marine), защищенные (Mifare), биометрические. Есть считыватели с кодовой панелью (matrix IV), позволяют вместо карты (или в дополнение к ней) использовать пин код.

См. https://ironlogic.ru/il_new.nsf/htm/ru_readers

Настройка оборудования для работы в системе GuardSaaS

Перед подключением конвертера Z-397 (мод. Web) или IP-контроллеров Z-5R (мод. Web), Z-5R (мод. Web BT), Matrix-II (мод. E K Wi-Fi) и Z-5R (мод. Wi-Fi) их нужно настроить на работу с сервером GuardSaas.

Настройка конвертера Z-397 (мод. Web)

Конвертер **Z-397 (мод. Web)** нужно подключить к компьютеру USB кабелем и отредактировать файл CONFIG.CFG, который находится на виртуальном диске конвертера.
[COMMON]
MODE=WEB
!!! Должен быть установлен только режим WEB, а не WEB+SERVER.

[NETWORK]
USE_DHCP=1 (**1 – адрес назначает роутер; 0 – фиксированный IP-адрес**)
LOCAL_IP=192.168.1.100 (**адрес конвертера в локальной сети при USE_DHCP=0**)
NETMASK=255.255.255.0
GATEWAY=192.168.1.1 (**адрес шлюза(роутера) в локальной сети при USE_DHCP=0**)
DNS=192.168.1.1 (**адрес DNS сервера при USE_DHCP=0**)
!!! Эти параметры должны соответствовать настройкам Вашей локальной сети – адрес роутера (GATEWAY), маска сети, DNS сервер. В качестве DNS сервера можно использовать как адрес роутера, так и известные адреса публичных серверов. (например: **77.88.8.88**)

[WEB]
USE_PROXY=0 (**не включается**)
SERVER=hw.guardsaas.ru (**!!!** Правильный адрес сервера **hw.guardsaas.ru**)
PORT=80
PATH=/data.php
CONNECT_PERIOD=10 (**интервал соединения с Web-сервером в секундах**)
PASSWORD=ab974088d09d4dc3 (**пароль по умолчанию**) Пароль для доступа к данным на Web-сервере. **При изменении пароля в контроллере, он должен быть изменен и в аккаунте.**
MAX_EVENTS=1 (**Число событий в контроллерах, при котором происходит досрочная отправка данных на Web-сервер до истечения интервала передачи.**)

После настройки извлеките конвертер правильным образом из ПК, нажав предварительно «Извлечь» в Панели задач или «Проводнике». Затем отключите кабель из гнезда USB. Подключите конвертер к локальной сети и пробуйте зарегистрировать его в сервисе Guardsaas.

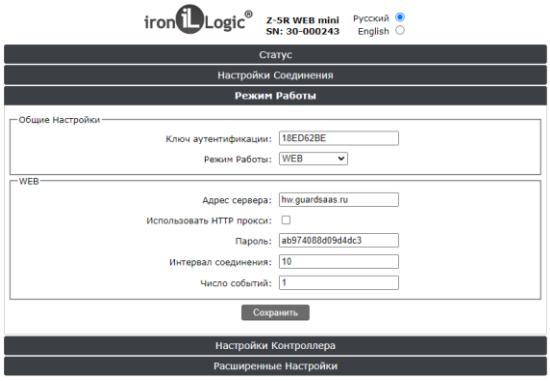
Ну путайте адрес сервера Guardsaas:

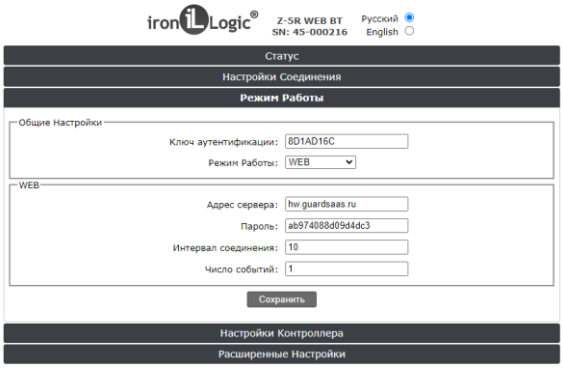
- для конвертера и IP-контроллера – это **hw.guardsaas.ru**;
- для пользователя аккаунта – это **app.guardsaas.ru**;

Убедитесь, что набираете правильный пароль (AUTH_key, состоящий из 8-ми символов) при регистрации в аккаунте, он написан на конвертере и в файле конфигурации.

Настройка IP-контроллеров
Z-5R (мод. Web), Z-5R (мод. Web BT),
Matrix-II (мод. E K Wi-Fi) и *Z-5R (мод. Wi-Fi)*

Режим **Web** обеспечивает связь с «облачным» сервисом. Для настройки режима работы **Web** необходимо войти в WEB-интерфейс контроллера и задать следующие параметры:

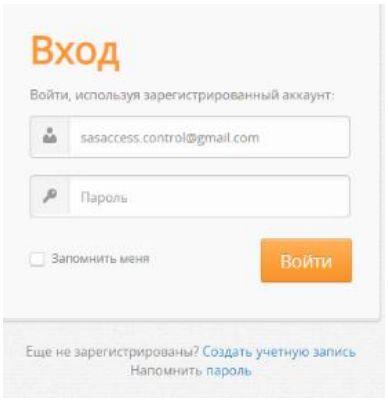




Ключ аутентификации: Первоначальный пароль для регистрации контроллера в аккаунте Guardsaas. (AUTH_key, состоящий из 8-ми символов, написанных на бирке IP-контроллера)
Режим работы: WEB.
Адрес сервера: hw.guardsaas.ru
Порт: 80 (или 81).
Путь: /data.php
Использовать HTTP прокси: флаг не ставится.
Пароль: по умолчанию - ab974088d09d4dc3 (Пароль для доступа к данным на Web-сервере. **(При изменении пароля в контроллере, он должен быть изменен и в аккаунте.)**
Интервал передачи: 10 (Интервал соединения с Web-сервером в секундах.)
Число событий: 1 (Число событий в контроллерах, при котором происходит досрочная отправка данных на Web-сервер до истечения интервала передачи.)
После настроек всех параметров необходимо нажать кнопку «**Сохранить**» и перезагрузить IP-контроллер по питанию.

Вход в аккаунт

Зайдите в аккаунт по адресу app.guardsaas.ru и в окне авторизации введите логин и пароль:

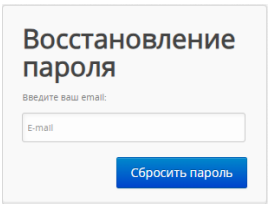


Восстановление логина/пароля

Если вы потеряли или забыли пароль, воспользуйтесь процедурой восстановления пароля на странице логина (ссылка «Напомнить пароль» под окном авторизации).



В окне «Восстановление пароля» введите адрес электронной почты, на который Вам придет письмо со ссылкой для задания нового пароля. Затем нажмите кнопку «Сбросить пароль».



Если Вы забыли логин, напишите нам письмо на адрес support@ironlogic.ru с указанием серийного номера любого Вашего конвертера (IP-контроллера).

Потеря доступа к аккаунту

Основание для использования аккаунта - владение электронной почтой и паролем. Основание для использования оборудования - знание его серийного номера и пароля.
Мы не имеем возможности и права вмешиваться в вопросы владения оборудованием и аккаунтом и также обязаны защищать права владельца логина.
При регистрации нового аккаунта **Вы должны** позаботиться о том, чтобы доступ к нему был только у владельца и **основной адрес аккаунта был адресом реального владельца** аккаунта и оборудования. Если аккаунт имеет логин постороннего лица, мы ничего не сможем сделать для восстановления доступа к этому аккаунту, если постороннее лицо сменит пароль или логин.

Защита учетной записи от потери или кражи

Простые правила помогут Вам восстановить учетную запись при утере доступа:
1) Убедитесь, что электронная почта основного аккаунта принадлежит Вам (владельцу аккаунта), а не постороннему лицу. Адрес электронной почты основного аккаунта показан на главной странице приложения в панели «Информация» справа вверху. В случае необходимости, незамедлительно измените адрес на собственный.
2) Введите дополнительно актуальный номер телефона, желательно мобильного и адрес электронной почты, принадлежащий Вам в поле Телефон профиля аккаунта. Мы сможем в этом случае подтвердить новый логин по дополнительному адресу или телефону.

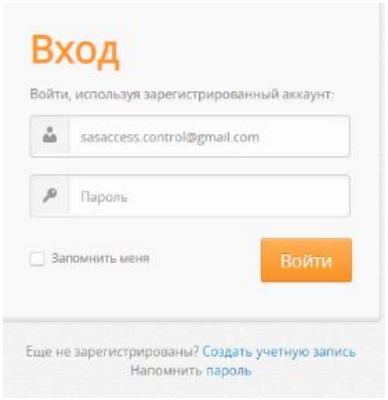
Вкладка «Оборудование»

Список конвертеров

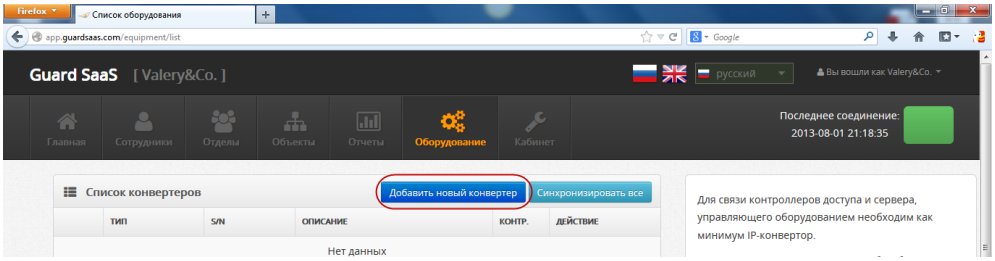
Добавить новый конвертер

Сначала нужно зарегистрировать конвертер (IP-контроллер) в аккаунте app.guardsaas.ru. Каждый конвертер (IP-контроллер) имеет свой уникальный серийный номер. Кроме этого, для каждого конвертера задается начальный пароль, который необходимо знать при регистрации. (По умолчанию это ключ аутентификации (AUTH_key) конвертера (IP-контроллера).

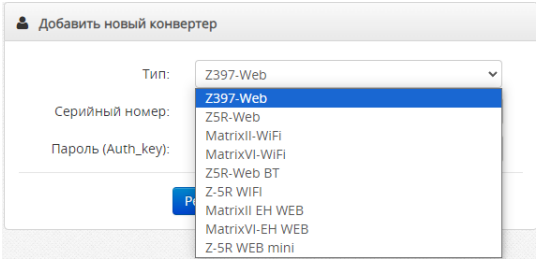
Зайдите в аккаунт, введя логин и пароль:



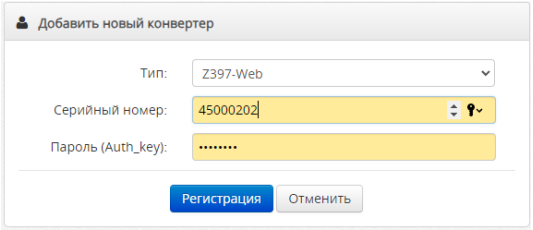
Чтобы зарегистрировать новый конвертер, откройте раздел «Оборудование» и кликните «Добавить новый конвертер». Ваш конвертер при этом должен быть подключен к сети Интернет и настроен на работу с сервисом.



Выберите тип конвертера (IP-контроллера) из выпадающего списка в окне «Тип»:

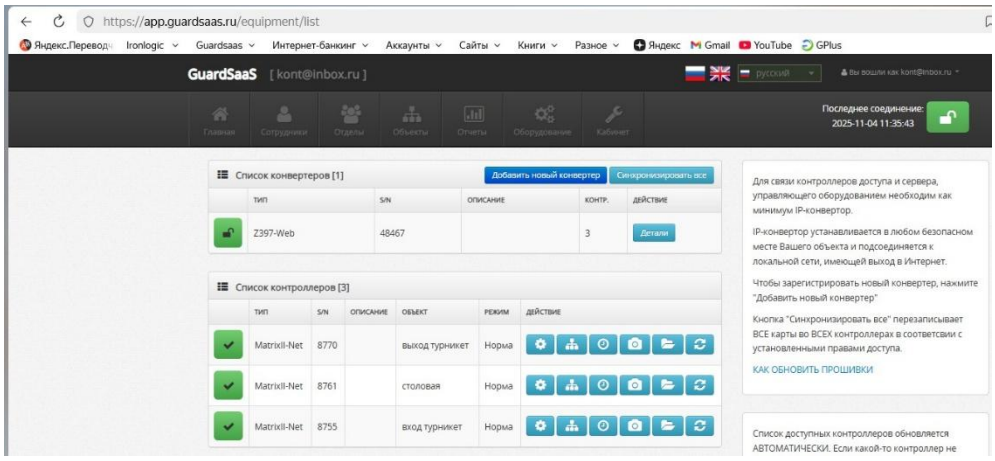


Введите серийный номер конвертера (IP-контроллера) и пароль (ключ аутентификации), который должен быть написан на конвертере (IP-контроллере) и в паспорте к нему. **Серийный номер вводится без пробелов и тире**. Кликните по кнопке «Регистрация».



При нормальной работе, правильно настроенный конвертер должен подключиться автоматически, и также должны появиться в списке все подключенные к этому конвертеру (IP-контроллеру) контроллеры.

В дальнейшем, рекомендуется сменить пароль (auth_key) конвертера, чтобы исключить возможность захвата управления оборудованием.

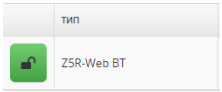


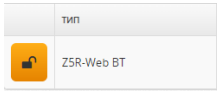
Если конвертер не определился, нужно проверить его соединение с интернетом.

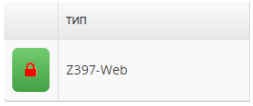
Состояние конвертера в аккаунте можно определить по цвету квадрата слева от типа конвертера.

Зеленый цвет – конвертер в режиме онлайн.

Оранжевый цвет – конвертер в режиме оффлайн.







*Если в конвертере **Z-397 (мод. WEB)** переключатель «lock/unlock» установлен в положение «Lock», нужно переключить в положение «unlock».* В аккаунте конвертер будет отображаться с замкнутым замком красного цвета. ***Связь с конвертером будет заблокирована и конвертер не будет передавать события из контроллеров и в контроллеры нельзя будет записать карты.***

Не получается зарегистрировать конвертер.

Прежде, чем регистрировать конвертер в системе, его **нужно подключить к сети Интернет**. Прежде, чем подключать конвертер к сети Интернет, его нужно **настроить.** Если конвертер не был подключен к сети, или не был правильно настроен на наш сервер, Вы получите ошибку «**Неизвестный серийный номер конвертера**» или «**Этот конвертер не настроен на наш сервер**» при его регистрации. Если Вы получили ошибку «**Такой номер уже существует**», это означает, что конвертер или IP-контроллер с таким серийным номером уже зарегистрирован на другом аккаунте. Для регистрации на новом аккаунте конвертер (IP-контроллер) нужно удалить в предыдущем аккаунте.

Основная ошибка - указание неправильного имени нашего сервера в конфигурации конвертера (IP-контроллера). Правильное имя сервера – **hw.guardsaas.ru**

Проверка настройки конвертера (IP-контроллера)

1) Проверьте доступность интернета в локальной сети конвертера (IP-контроллера). Подключитесь своим компьютером к локальной сети и откройте страницу http://hw.guardsaas.ru/test.html. Если в ответ нет сообщения «Successful Connect!», то ищите проблему в настройках сети.

2) Если получили «Successful Connect!», то смотрите настройки конвертера (IP-контроллера):

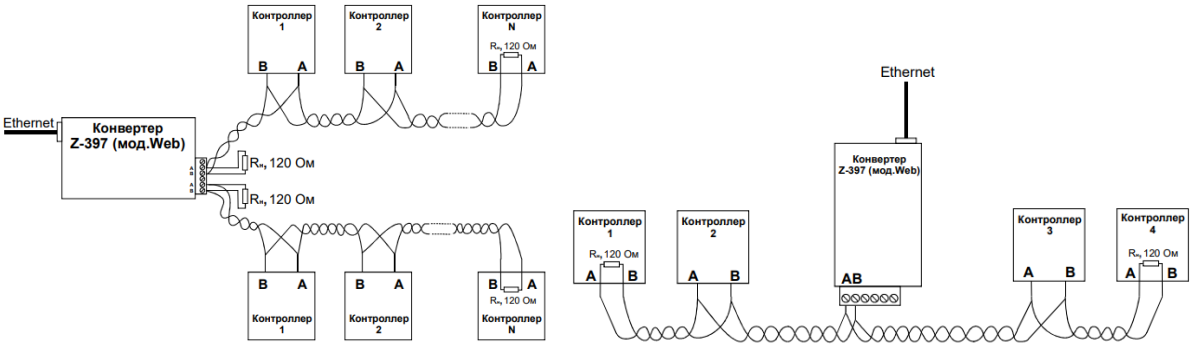
- конвертер (IP-контроллер) должен иметь актуальную прошивку (firmware);
- режим конвертера (IP-контроллера) должен быть **WEB**;
- имя сервера **hw.guardsaas.ru**;
- порт **80** или **81**;
- путь **/data.php**;
- правильность адреса роутера (default gateway). (Адрес по умолчанию 192.168.1.1. Иногда бывает, что адрес 192.168.0.1 или даже другой.);
- работу DHCP - присваивается ли правильный IP-адрес конвертеру (IP-контроллеру);

- убедитесь, что конвертер (IP-контроллер) виден в локальной сети роутера, используя программу Find для ПК или IP Find для android;
- DNS сервер 77.88.8.88 может не поддерживаться в вашей сети - проверьте. Попробуйте DNS сервер провайдера.
- конвертер (IP-контроллер) **не должен** использовать Proxy Server.

Почему конвертер Z-397 (мод. WEB) не «видит» контроллеры?

После успешного добавления конвертера Z-397 (мод. WEB) в систему GuardSaaS у вас может быть такая ситуация, что подключенные контроллеры не отображаются в списке. Ниже приведены возможные причины и способы решения данной проблемы.
В первую очередь нужно убедиться в отсутствии обрыва по линии RS-485 и наличия связи между конвертером и контроллерами. На данный момент проще и удобнее всего диагностировать связь с помощью программы Guard Light (https://ironlogic.ru/il_new.nsf/htm/ru_guardlight). Если контроллеры не видимы и не определяются в программе Guard Light, то дело в отсутствии связи или неправильном подключении контроллеров. Если же контроллеры видны в программе Guard Light и выполняют сетевые команды, то дело скорее всего в настройках конвертера или старой версии его прошивки.

Причина:
Ошибки при подключении контроллеров.
Решение:
Убедитесь, что контроллеры подключены к конвертеру правильно:
1) провода «A», «B», «GND» линии RS-485 подключены соответственно, не перепутаны местами;
2) нагрузочное сопротивление 120 Ом подключено в соответствии со схемой включения конвертера (конвертер либо в конце линии, либо в середине);
3) все контролеры и конвертер объединены по GND.
Правила монтажа расписаны в статье «Общие рекомендации по монтажу СКУД»: https://ironlogic.ru/il_new.nsf/htm/ru_new_08.11.2023
В руководстве по эксплуатации к конвертеру **Z-397 (мод. Web)** на странице 4 показаны две схемы включения конвертера.



Причина:
Специфическая конфигурация локальной сети, в которой работает конвертер.
В некоторых сетевых конфигурациях, специфические настройки, наличие прокси сервера или антивирусного ПО могут препятствовать нормальной работе конвертера. Конвертер является стандартным клиентом сети TCP/IP. Для его нормальной работы не нужна сложная настройка. Он может работать как с динамическим, так и со статическим IP адресом. В обычном режиме конвертер настраивается на работу по 80 порту. Конечно, условием работы конвертера является наличие для него доступа к сети Интернет. Тем не менее, иногда даже при наличии связи с сервером, конвертер не может полноценно работать из-за сложной конфигурации локальной сети и способа выхода в Интернет, а также при наличии в сети программ, манипулирующих сетевым трафиком.
Решение:
Обновить прошивку конвертера. В последней версии прошивки улучшена поддержка сетевых протоколов, позволяющая решить указанную проблему в большинстве случаев.

Альтернативным является следующий способ решения проблемы:
Откройте файл CONFIG.CFG и в разделе [WEB] измените порт 80 на порт 81.
[WEB]
...
PORT=81

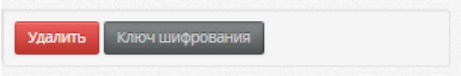
Причина:
Изменен пароль конвертера, используемый для шифрования данных.
Решение:
Зайдите в «Оборудование» и для необходимого конвертера нажмите кнопку «Детали». Далее справа над блоком «Параметры конвертера» нажмите кнопку «Пароль». В появившемся окне введите 16-значный пароль, который вы можете найти в файле CONFIG.CFG в разделе [WEB]:
[WEB]
...
PASSWORD= ab974088d09d4dc3 (**по умолчанию**)
Файл CONFIG.CFG можно найти на флеш-диске, который определяется в системе при подключении конвертера через кабель USB.

Детали (Параметры конвертера)

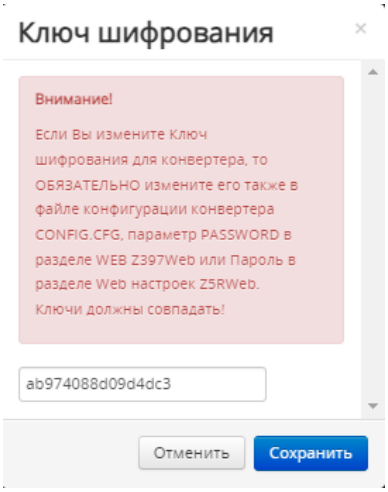
После подключения конвертера, рекомендуется настроить его параметры, кликнув по кнопке «Детали» (название или расположение и часовой пояс (Таймзона) и т.п.).

Ключ шифрования

По кнопке «Ключ шифрования» можно отредактировать этот ключ.

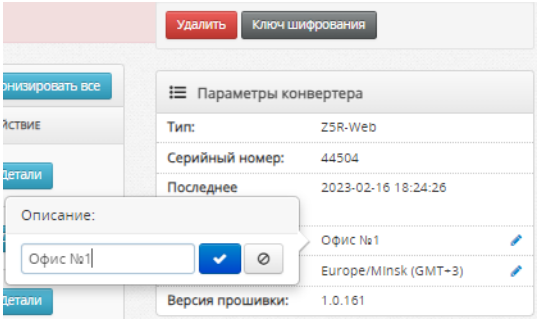


По умолчанию ключ шифрования - ab974088d09d4dc3 (Пароль для доступа к данным на Web-сервере. **(При изменении ключа шифрования в аккаунте, он должен быть изменен и в настройках конвертера (IP-контроллера).**



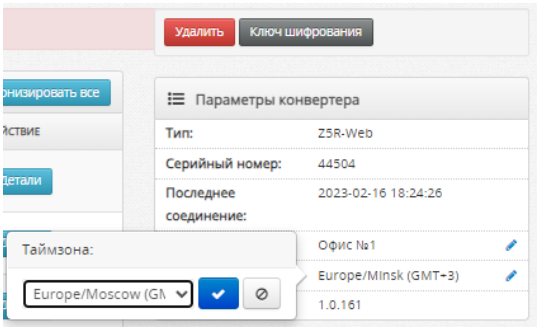
Описание

В описании можно записать имя конвертера и его место расположения.



Таймзона

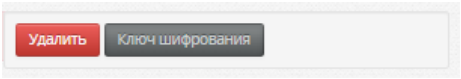
Часовой пояс необходим для корректной работы распределенных систем.



Для изменения таймзоны конвертера нужно выбрать конвертер в разделе «Конвертеры» и кликнуть левой кнопкой мыши по кнопке «Детали». Нажать на карандашик напротив строки «Таймзона:». Далее разворачиваем появившееся окно «Таймзона:» и выбираем нужную таймзону. Затем сохраняем её, нажав левой кнопкой мыши на синюю кнопку с белой галкой.

Удалить

Кнопкой «Удалить» можно удалить конвертер из системы.

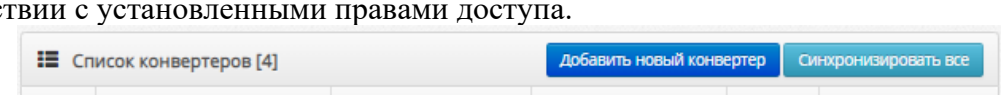


Перед удалением конвертера из аккаунта для его переноса на другой аккаунт нужно предварительно обесточить контроллеры, подключенные к этому конвертеру, затем удалить контроллеры в аккаунте. После этого можно удалять конвертер и переносить в другой аккаунт.

Синхронизация

Синхронизировать всё

Кнопкой «Синхронизировать все» выполняется полная синхронизация всех контроллеров в системе. Перезаписываются ВСЕ карты во ВСЕХ контроллерах в соответствии с установленными правами доступа.



Синхронизация. Зачем и когда ее делать.

Синхронизацию запускать нужно только при замене контроллеров или необходимости переписать ВСЕ карты в контроллеры. Это длительная процедура может продолжаться несколько минут или десятков минут, в зависимости от количества карт.

В нормальной ситуации карты автоматически записываются в контроллеры. При этом в течение некоторого времени значок контроллера показывает обмен информацией (крутятся стрелки) и может указываться информационное сообщение **«Ожидают синхронизации № карт-кодов»**. Число кодов обычно постоянно меняется (уменьшается), отражая процесс записи. Когда запись в контроллер закончилась, значок становится нормальным, в виде галочки в большинстве случаев, либо в виде значка режима контроллера (блокировка, свободный проход).

Если стрелки продолжают крутиться, значит, запись новой информации в контроллер не закончилась. При чрезмерно длительной процедуре, которая не заканчивается и при этом число не уменьшается, нужно искать проблему в связи контроллера с конвертером, либо в самом контроллере.

Если значок контроллера зеленый, то попробуйте перезагрузить его путем выключения/включения питания. Если это не решает проблему, то вероятна неисправность контроллера.

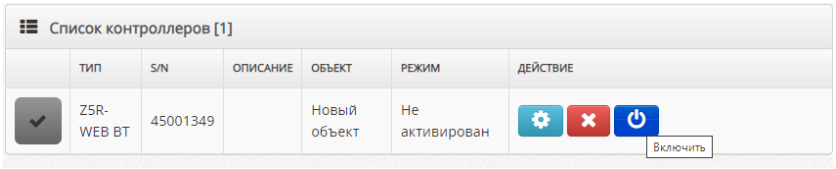
Если значок контроллера оранжевый, то с ним нет связи.

Список контроллеров

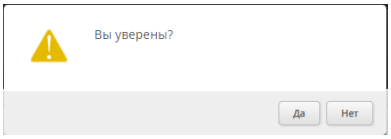
Подключение контроллеров

Список доступных контроллеров обновляется АВТОМАТИЧЕСКИ. Если какой-то контроллер не виден в списке, скорее всего связь по 485 линии с ним отсутствует. Вы можете отключать или включать контроллеры при необходимости. Количество доступных контроллеров ограничено. По умолчанию доступно до 16 контроллеров, подключенных к 1 конвертеру.

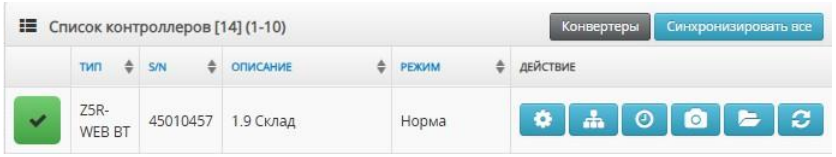
При подключении конвертера (IP-контроллера) новые контроллеры находятся в неактивном режиме. Их нужно активировать кнопкой «Включить» в «Списке контроллеров».



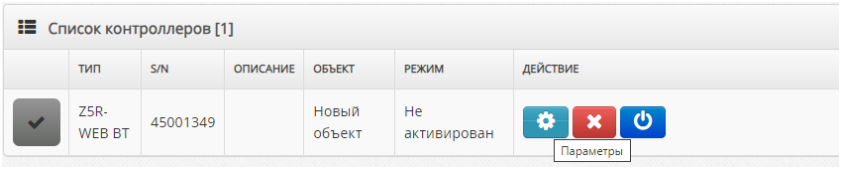
Появится окно предупреждения, в котором нужно кликнуть по кнопке «Да».



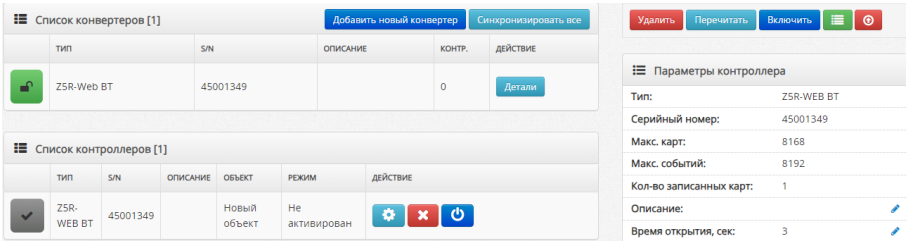
Контроллер подключится к системе.



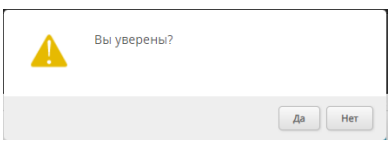
Также контроллеры можно активировать кнопкой «Включить» в «Параметрах контроллера». Для этого нужно кликнуть по кнопке «Параметры» в списке контроллеров на подключаемом контроллере.



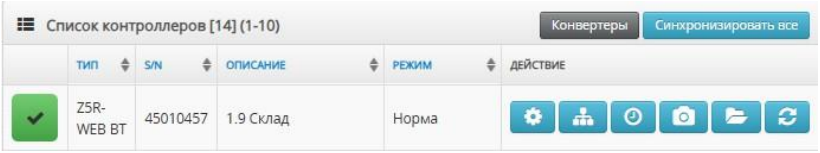
Откроется окно «Параметры контроллера» в котором нужно кликнуть по кнопке «Включить».



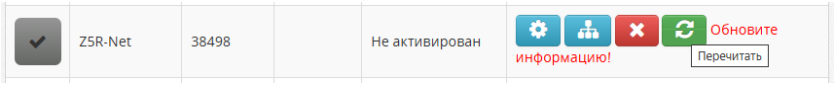
Появится окно предупреждения, в котором нужно кликнуть по кнопке «Да».



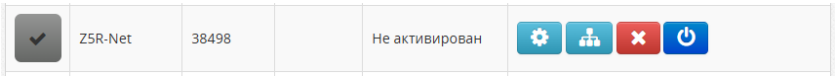
Контроллер подключится к системе.



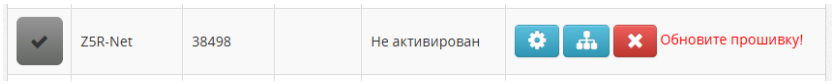
Если система не смогла вычитать информацию о контроллере или в контроллере старая прошивка, то кнопки «Включить» не будет. Контроллер будет отображаться с фразой «Обновите информацию» и кнопкой «Перечитать».



В случае, если информация в контроллере просто не вычиталась, нужно нажать кнопку «Перечитать». После перечитывании информации с контролера его можно активировать кнопкой «Включить» в «Списке контроллеров».



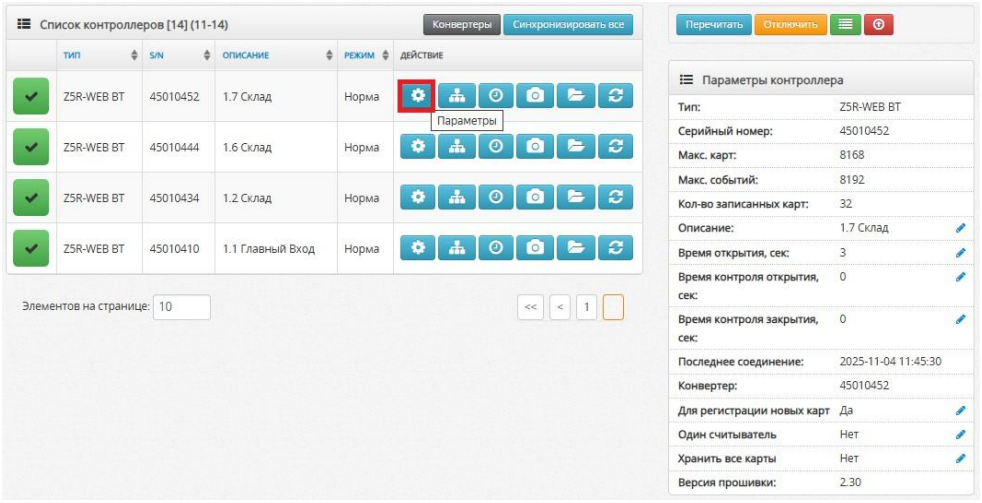
При попытке установки контроллера со старой прошивкой, после вычитывании информации из контроллера, появится сообщение «обновите прошивку».



Обновить прошивку можно через ПО Guard Commander или ПО Guard Light. Для этого нужно в настройках файла конфигурации конвертера (web-интерфейса IP-контроллера) изменить режим работы с WEB на SERVER.

Кнопка «Параметры» (Параметры контроллера)

В окне «Параметры контроллера» можно настроить дополнительные параметры каждого контроллера.



Доступны следующие параметры:

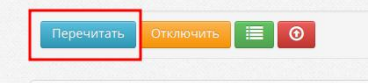
- **Описание** – введите описание контроллера.
- **Время открытия** – введите время, в течение которого подается или снимается напряжение с замка, от 0,1 до 25,5 сек.
- **Время контроля открытия** – введите время, в течение которого ожидается штатное открытие двери, от 0,1 до 25,5 сек. 0 – нет контроля.
- **Время контроля закрытия** – введите время после открывания двери, в течение которого она должна быть закрыта, от 0,1 до 25,5 сек. 0 – нет контроля.
- **Для регистрации новых карт** – Если выбрать «Да», то данный контроллер можно использовать для регистрации новых карт в системе.
- **Один считыватель** – Если выбрать «Да», то к данному контроллеру подключен только один считыватель (первое событие в системе будет вход, а следующее - выход). Если выбрать «Нет», то к данному контроллеру подключено два считывателя (на вход и выход)
- **Хранить все карты** – Если выбрать «Да», то данный контроллер будет хранить все карты. Если выбрать «Нет», то данный контроллер будет хранить только те карты, у которых есть доступ к контроллеру. Рекомендуется устанавливать флаг «Нет».

Всем нужно иметь ввиду, что в связи с очень медленным процессом обмена данными с контроллерами, и для оптимизации работы сервера, сервер хранит образ данных каждого контроллера у себя на сервере. Синхронизация сравнивает данные в базе с образом контроллера и посылает только изменения в сам контроллер. Если Вы меняете расположение контроллера, его подключение, пишете в него карты напрямую, сервер об этом не знает и процесс синхронизации «сбивается».

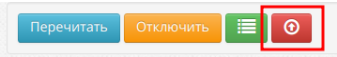
Если вы заменяете контроллер, ставите новый контроллер на старое место и пр., для исправления синхронизации нужно:

1) Вычитать все данные и карты из контроллера:

- кликните по кнопке «Перечитать»;



- после окончания, подождите пару минут, затем кликните по кнопке «Вычитать все карты»;



- когда в зеленом квадрате, слева от типа контроллера, появится галочка, запустите синхронизацию контроллера.



2) Проверить общее количество и количество карт в памяти контроллера.

Эту процедуру крайне рекомендуем делать при установке новых контроллеров на сервер.

Состояние контроллера можно определить по цвету квадрата слева от типа контроллера.

Зеленый цвет – контроллер в режиме онлайн

Оранжевый цвет – контроллер в режиме оффлайн



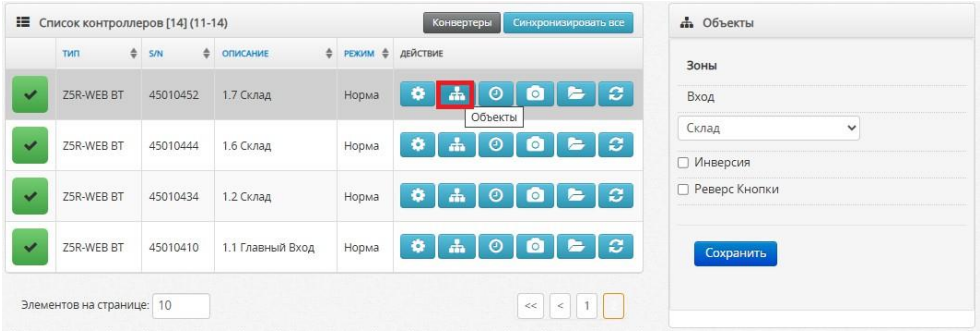
В списке контроллеров предоставлена следующая информация: тип, серийный номер, описание, название объекта, состояние. В некоторых случаях, контроллер можно деактивировать. Для этого нажмите кнопку «Параметры» конкретного контроллера, затем нажмите «Отключить». После этого действия события выбранного контроллера не будут отображены в отчетах. После деактивации контроллер может быть также удален.

Ваше оборудование настроено, и Вы можете приступить к вводу сотрудников и назначению карт.

Кнопка «Объекты»

Привязать контроллеры к объектам можно двумя способами: в подразделе «Контроллеры» на вкладке «Объекты» или на вкладке «Оборудование» - «Контроллеры» кнопкой «Объекты».

Следует учитывать, что в новых аккаунтах объекты назначаются контроллерам на вкладке «Оборудование» - «Контроллеры» кнопкой «Объекты».



Если данная опция не нужна, то её можно выключить во вкладке «Кабинет» - «Общие настройки» - «Смежные зоны доступа», сняв флаг напротив этой опции.

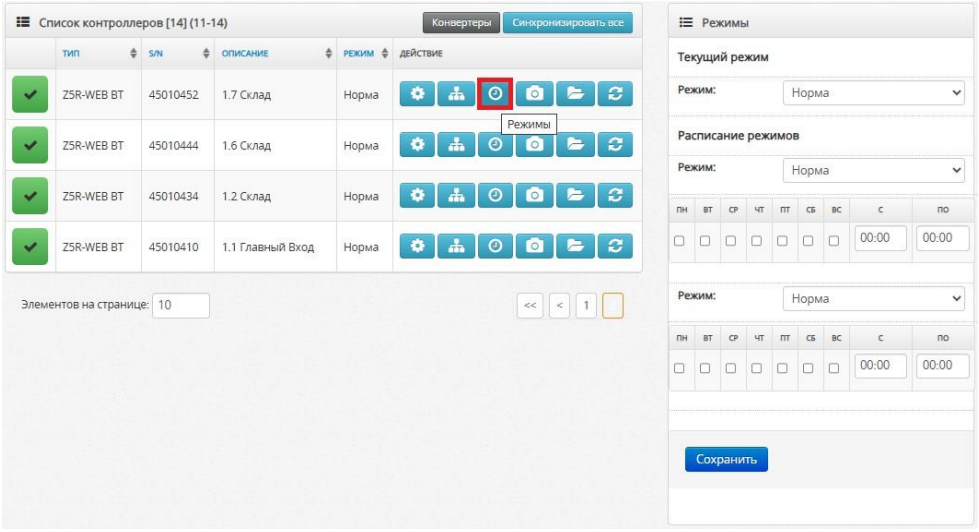
В окне «Объекты» выберите только ту внутреннюю зону контроллера, который установлен в данном помещении и управляют доступом к нему.

Инверсия — это логический обмен местами входа и выхода. Используйте для смежных помещений или при ошибках монтажа.

Реверс кнопки — это тоже инверсия, но для событий прохода по кнопке.

Кнопка «Режимы»

Для работы с режимами кликните по кнопке «Режимы» на выбранном контроллере.



Откроется окно подраздела «Режимы». В этом окне можно установить вручную текущий режим работы контроллера (норма, блокировка, ожидание свободного прохода, свободный проход). Также можно установить нужный режим в расписании режимов по времени и дню недели.

Норма – рабочий режим по умолчанию.

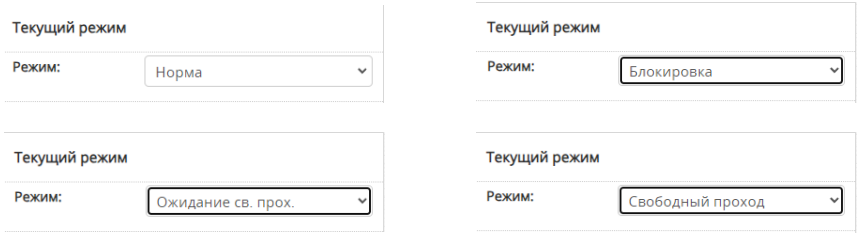
Блокировка – режим блокировка прохода по картам.

Ожидание свободного прохода – режим, ожидания карты прохода для перехода в режим «Свободный проход».

Свободный проход – режим свободного прохода через дверь (турникет), замок обесточен.

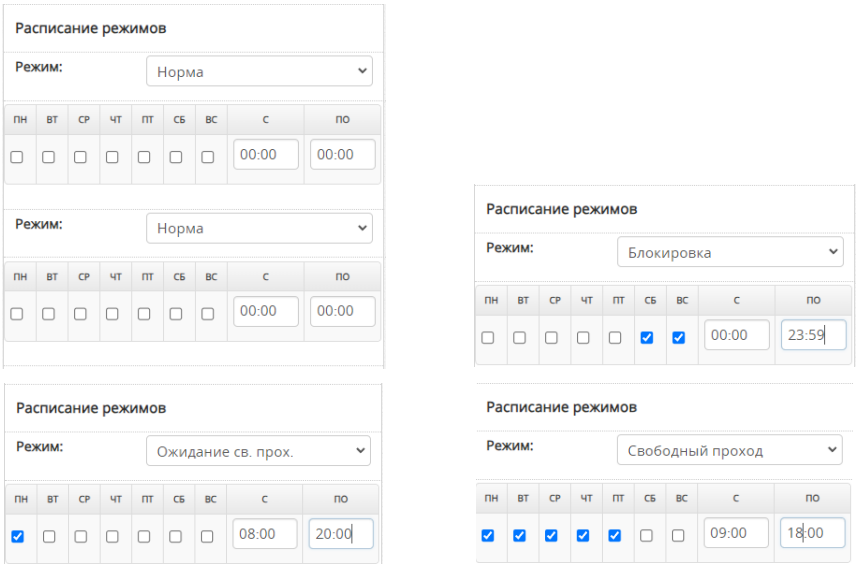
Текущий режим

В «Текущем режиме» можно установить вручную нужный режим работы контроллера, также и вернуть режим «Норма». Если режим установлен в подразделе «Режимы», то и отключить его можно только через этот подраздел.



Расписание режимов

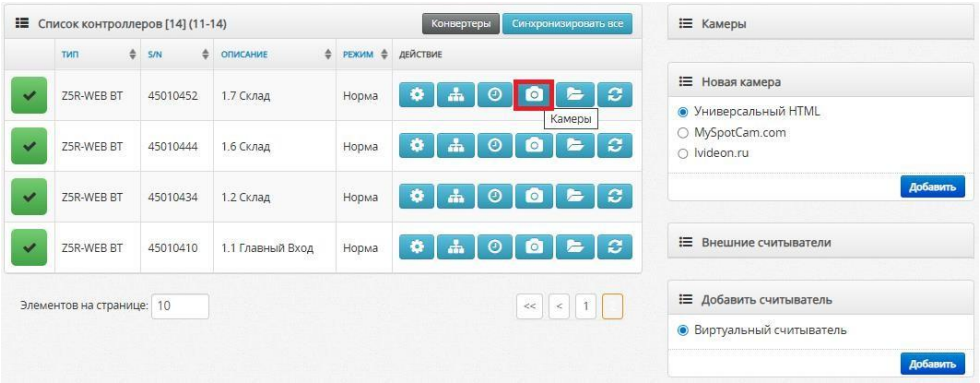
В окне «Расписание режимов» можно установить автоматическое переключение в нужный режим работы контроллера по расписанию, учитывая дни недели и время включения режима. Можно установить два режима для включения по расписанию. Если режим установлен в подразделе «Режимы», то и отключить его можно только через этот подраздел.



Не все прошивки контроллеров поддерживают включение режимов. Для Matrix-II (мод. Net) и Z-5R (мод. Net) прошивка с поддержкой режимов должна быть версии 2.10 и выше. Необходимо обновление прошивки. Мы можем в большинстве случаев обновить прошивку удаленно.

Кнопка «Камеры»

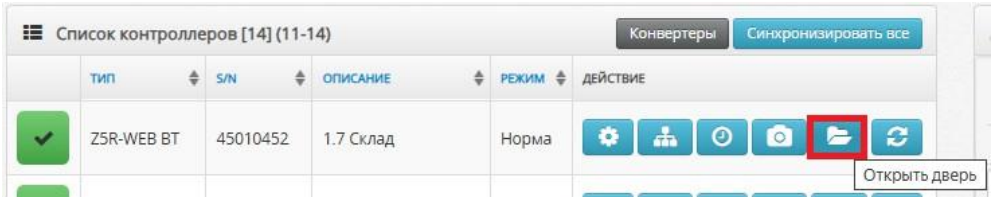
Для привязки видеокамеры к контроллеру нужно кликнуть по кнопке Камеры».



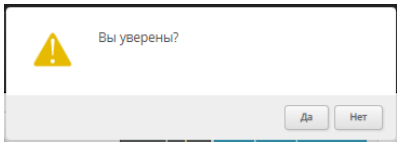
Далее в окне «Новая камера» выбирается тип камеры: «Универсальный HTML», «MySpotCam.com», «Ivideon.ru». После выбора типа камеры нужно кликнуть по кнопке «Добавить».

Кнопка «Открыть дверь»

Кнопка «Открыть дверь» позволяет удаленно открыть дверь выбранного контроллера.



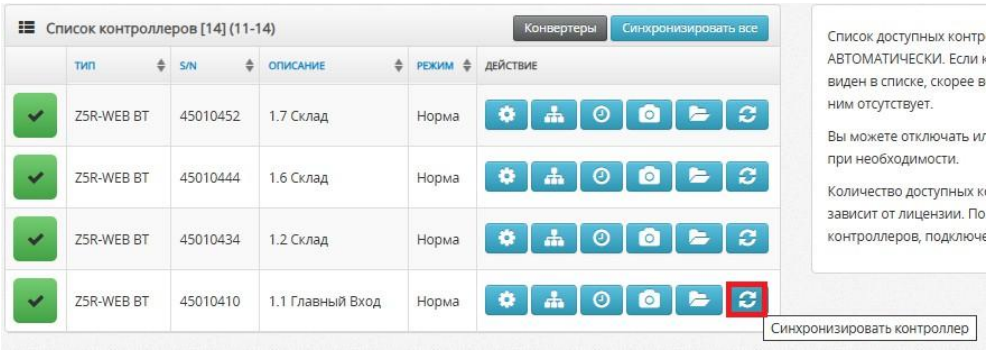
После нажатия на кнопку появится окно предупреждения «Вы уверены?», в котором нужно подтвердить действие, нажав на кнопку «Да».



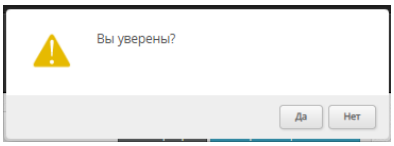
Затем команда на открытие будет направлена контроллеру с отображением на экране.

Кнопка «Синхронизировать контроллер»

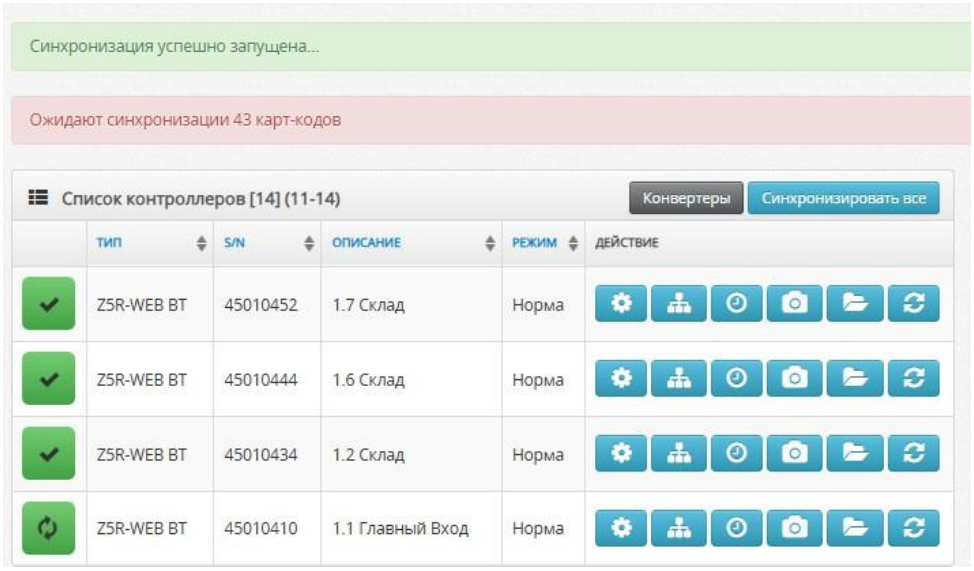
Кнопка «Синхронизировать контроллер» предназначена для синхронизации выбранного контроллера после отключения или других операций с контроллером.



После нажатия на кнопку появится окно предупреждения «Вы уверены?» в котором нужно выбрать «Да».

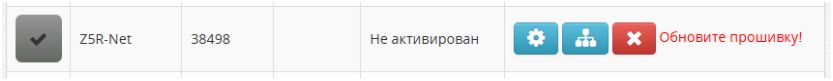


Затем команда на синхронизацию будет направлена контроллеру с отображением на экране.



Обновление прошивок оборудования

Система рекомендует обновить прошивку контроллера. Не все прошивки работают правильно с GuardSaaS. Если конкретная прошивка не поддерживается системой или замечены проблемы при ее использовании, в списке контроллеров Вы увидите сообщение «Обновите прошивку». Система при этом работает.



Обновить прошивку можно через ПО Guard Commander или ПО Guard Light. Для этого нужно в настройках файла конфигурации конвертера изменить режим работы с WEB на SERVER.

Рекомендуемые версии прошивок

Оборудование		Версия
Z-397 (мод. Web)		3.0.75 +
Z-5R (мод. Net)		2.21 +, 3.17 ext +
Z-5R (мод. Net 8000)		2.25 +
Z-5R (мод. Net 16000)		3.4 +
Matrix-II (мод. E K Net)		2.25 +
Matrix-III (мод. MF K Net)		2.8_c
Matrix-VI (мод. NFC K Net)		3.4 +, 2.13 +
Matrix-VI (мод. EH K Net)		2.4 +
Guard (мод. Net)		1.15 Дверь, 1.11 Турникет, 1.21 Шлагбаум, 1.11 Шлюз
Z-Eurolock		11 +
Z-5R (мод. Web)	Модуль связи	1.0.169
	Модуль контроллера	3.48
Z-5R (мод. Web BT)	Модуль связи	1.45+
	Модуль контроллера	2.38+
Matrix-II (мод. E K Wi-Fi)	Модуль связи	1.79+
	Модуль контроллера	2.52+
Z-5R (мод. Wi-Fi)	Модуль связи	1.79+
	Модуль контроллера	2.52+

Прошивки загружайте с сайта производителя https://ironlogic.ru/.Также можно некоторые прошивки скачать по ссылке из таблицы.

Инструкция по прошивке конвертера Z-397 (мод. WEB)

1. Подключите конвертер к компьютеру по USB кабелю.
2. Запишите в корень появившегося диска новую прошивку (рядом с файлом CONFIG.CFG).
3. Корректно отключите диск и кабель.
4. Подключите внешнее питание. Конвертер обновит прошивку самостоятельно.

Мы имеем возможность обновлять прошивки конвертеров* Z-397 (мод. WEB) *удаленно. Конвертер должен быть на связи с сервером.

Для этого, напишите нам заявку на адрес support@ironlogic.ru, указав:

1) Ваш логин.
2) Серийный номер конвертера.

3) Конвертер при этом должен находиться в состоянии UNLOCK (переключатель на корпусе) и подключен к серверу Guardsaas.

Инструкция по прошивке контроллеров Z-5R (мод. Net), Z-5R (мод. Net 8000), Z-5R (мод. Net 16000), Matrix-II (мод. E K Net), Matrix-VI (мод. EH K Net)

1. Переключите конвертер, к которому подключены контроллеры, в режим «SERVER».
2. Скачайте и установите программу Guard Light или Guard Commander.
3. Запустите программу Guard Light или Guard Commander.
4. Подключитесь к конвертеру и контроллеру в программе и по Руководству к ПО Guard Light или Руководству к ПО Guard Commander выполните обновление прошивки. (Режим SERVER)

Мы имеем возможность обновлять прошивки контроллеров* Z-5R (мод. Net), Z-5R (мод. Net 8000), Z-5R (мод. Net 16000), Matrix-II (мод. E K Net), Matrix-VI (мод. EH K Net) *(только этих!) удаленно.

Для этого, напишите нам заявку на адрес support@ironlogic.ru, указав:

1) Ваш логин.
2) Серийные номера конвертера и нужных контроллеров в его линии.
3) Конвертер при этом должен находиться в состоянии UNLOCK (переключатель на корпусе).

Инструкция по прошивке IP-контроллеров Z-5R (мод. Web), Z-5R (мод. Web BT), Matrix-II (мод. E K Wi-Fi), Z-5R (мод. Wi-Fi)

Инструкция по прошивке контроллеров Z-5R (мод. Web)
Инструкция по прошивке контроллера Z-5R (мод. Web BT) через WEB-интерфейс
Инструкция по прошивке контроллера Matrix-II (мод. E K Wi-Fi)/Matrix-II Wi-Fi через web-интерфейс
Инструкция по прошивке контроллера Matrix-II (мод. E K Wi-Fi)/Matrix-II Wi-Fi через microUSB
Инструкция по прошивке контроллера Z-5R (мод. Wi-Fi) через web-интерфейс
Инструкция по прошивке контроллера Z-5R (мод. Wi-Fi) через microUSB

Мы также можем обновить прошивки удаленно при условии рабочего состояния IP-контроллеров и версий прошивок модулей связи не ниже указанных.

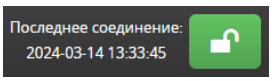
Z-5R (мод. Web) – 1.0.164
Z-5R (мод. Web BT) – 1.29
Matrix-II (мод. E K Wi-Fi) – 1.59
Z-5R (мод. Wi-Fi) – 1.59

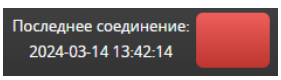
Для этого, напишите нам заявку на адрес support@ironlogic.ru, указав:

1) Ваш логин.
2) Серийные номера нужных IP-контроллеров.
3) IP-контроллер при этом должен находиться в рабочем состоянии и подключен к серверу Guardsaas.

Проблемы связи оборудования с сервером.

В системе GuardSaaS оборудование само периодически выходит на связь с сервером.





Если конвертер не связывается с сервером в течение нескольких минут, то индикатор связи становится **оранжевым** (**красным**) и время последнего соединения не меняется. Если индикатор связи **оранжевый** (**красный**) и по крайней мере индикатор одного из **конвертеров** оранжевый, то этот конвертер не связывается с сервером. При отсутствии связи новые карты не попадают в контроллеры и не работают. Также на сервер не приходит информация о проходах.

Решение проблемы связи Конвертера Z-397 (мод. Web)

(модуля связи IP-контроллеров)

1) Перезагрузите конвертер путем временного отключения питания.
2) Проверьте интернет в локальной сети конвертера (IP-контроллера). Подключитесь своим компьютером к локальной сети и откройте в браузере страницу http://hw.guardsaas.ru/test.html. Если в ответ нет сообщения «Successful Connect!», то ищите проблему в настройках сети.
3) Если получили «Successful Connect!», то смотрите настройки конвертера (IP-контроллера):
- конвертер (IP-контроллер) должен иметь актуальную прошивку (firmware);
- режим конвертера (IP-контроллера) должен быть **WEB**;
- имя сервера **hw.guardsaas.ru**;
- порт **80** или **81**;
- путь **/data.php**;
- правильность адреса роутера (default gateway). (Адрес по умолчанию 192.168.1.1. Иногда бывает, что адрес 192.168.0.1 или даже другой.);
- работу DHCP - присваивается ли правильный IP-адрес конвертеру (IP-контроллеру);
- убедитесь, что конвертер (IP-контроллер) виден в локальной сети роутера, используя программу Find для ПК или IP Find для android;
- DNS сервер 77.88.8.88 может не поддерживаться в сети - проверьте. Попробуйте DNS сервер провайдера.
- конвертер (IP-контроллер) **не должен** использовать Proxy Server.

Решение проблемы связи Контроллеров

Если индикаторы конвертеров зеленые, а одного или нескольких **контроллеров** оранжевые, это значит, что связи нет по линии RS-485 между этим контроллером и его конвертером. Попробуйте для начала перезагрузить контроллер и конвертер путем временного отключения питания. Если проблема не решиться, то ищите обрыв провода. Если обрыва нет, то вероятен выход из строя контроллера. В этом случае нужно заменить контроллер.

Вкладка «Объекты»

Чтобы упросить настройку правил доступа, в GuardSaaS введено понятие Объект. Объекты — это независимые помещения, в которые регулируется доступ. Как минимум, в системе должен существовать один объект.

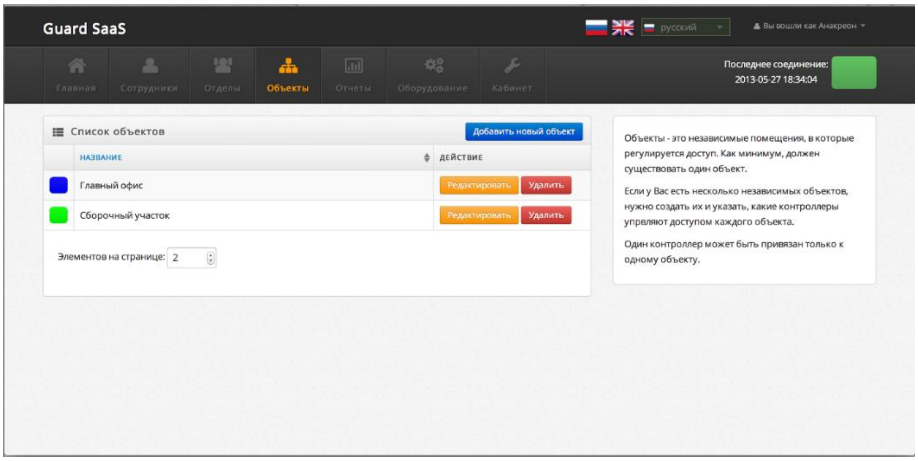
Один контроллер может быть привязан к нескольким объектам, если они смежные, то есть контроллер установлен в переходе между объектами.

Если у Вас есть несколько независимых объектов, нужно создать их и указать, какие контроллеры управляют доступом каждого объекта.

Для каждого объекта назначаются контроллеры, управляющие доступом в помещения объекта. Все настройки контроллеров одного объекта одинаковые.

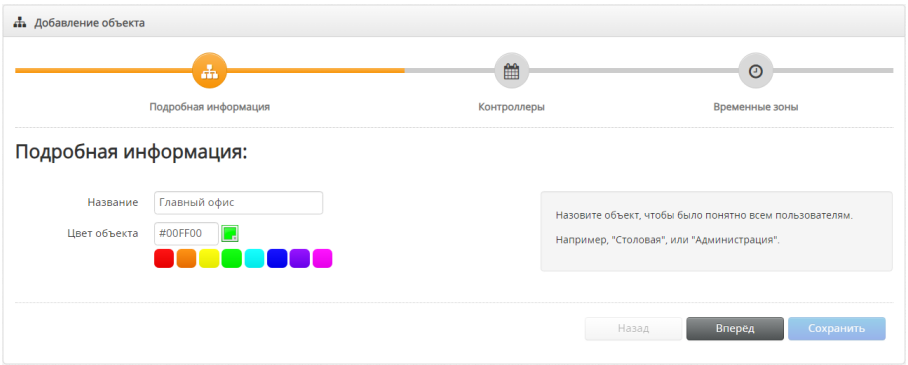
Добавление объекта

Для управления объектами, перейдите на вкладку «Объекты». По умолчанию создается один объект. Вы можете задать свое наименование объекта и/или создать новые объекты.



Вы можете создать новый объект, удалить или редактировать существующий объект. Для создания объекта нажмите кнопку «Добавить новый объект».

При создании/редактировании объекта задается название объекта, а также цвет, который облегчает дальнейшую работу с отчетами. Назовите объект, чтобы было понятно всем пользователям. Например, "Столовая" или "Администрация".



Для продолжения нажмите на кнопку «Вперед» внизу экрана.

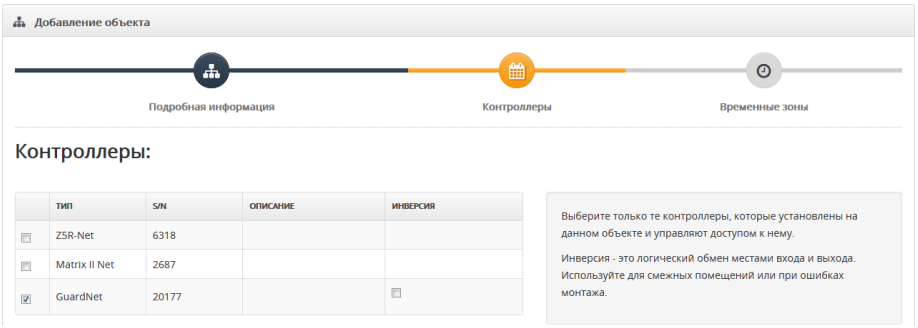
Контроллеры

В подразделе «Контроллеры» выберите только те контроллеры, которые установлены в данном помещении и управляют доступом к нему. Можно один контроллер выбирать для 2-х помещений. В этом случае помещения считаются смежными. Для одного из помещений нужно обязательно указать инверсию подключения считывателей.

Инверсия — это логический обмен местами входа и выхода. Используйте для смежных помещений или при ошибках монтажа считывателей.

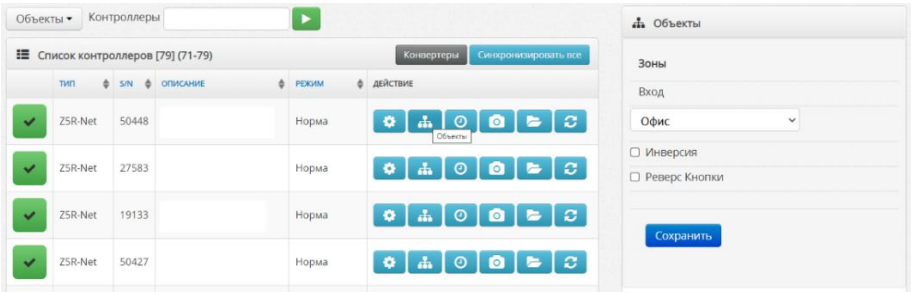
Реверс кнопки — это тоже инверсия, но для событий прохода по кнопке.

После изменения списка выбранных контроллеров обязательно сделайте полную синхронизацию в разделе «Оборудование»!

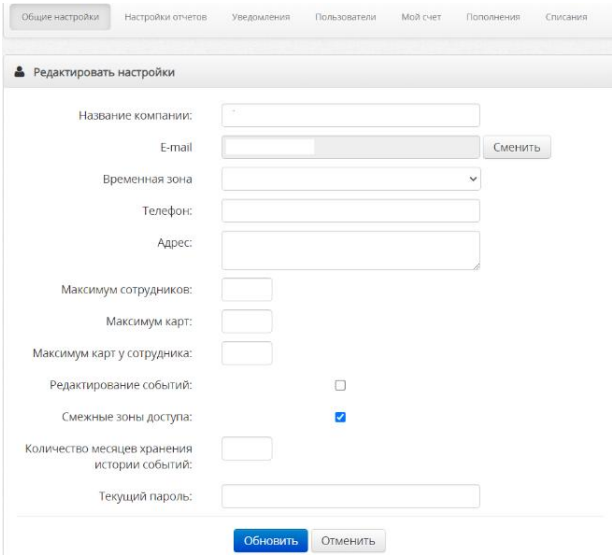


Привязать контроллеры к объектам можно двумя способами: на вкладке «Объекты» в подразделе «Контроллеры» или на вкладке «Оборудование» - «Контроллеры» кнопкой «Объекты».

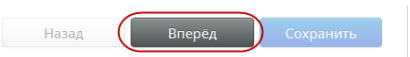
Следует учитывать, что в новых аккаунтах объекты назначаются контроллерам на вкладке «Оборудование» - «Контроллеры» кнопкой «Объекты».



Если данная опция не нужна, то её можно выключить во вкладке «Кабинет» - «Общие настройки» - «Смежные зоны доступа», сняв флаг напротив этой опции.



Для продолжения нажмите на кнопку «Вперед» внизу экрана.



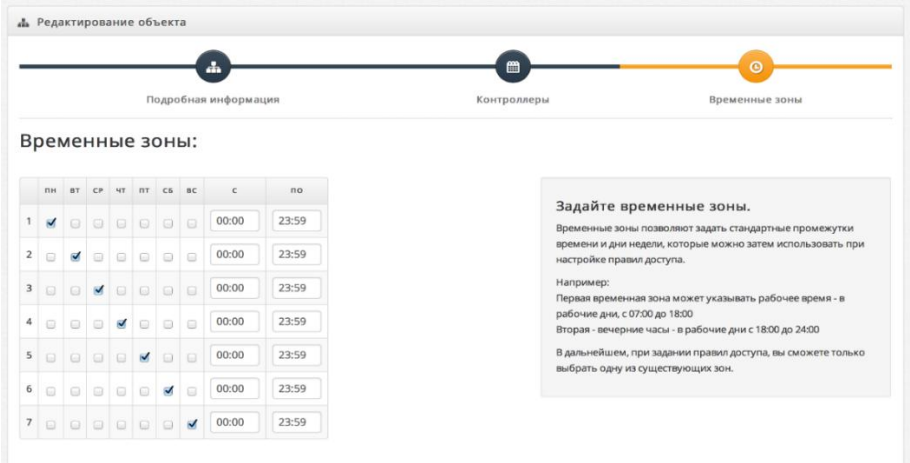
Временные зоны

Далее задайте необходимые временные зоны. Временные зоны позволяют задать стандартные промежутки времени и дни недели, которые можно затем использовать при настройке правил доступа.

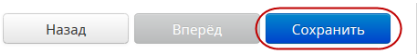
Например:

Первая временная зона может указывать рабочее время - в рабочие дни, с 07:00 до 18:00. Вторая - вечерние часы - в рабочие дни с 18:00 до 24:00

В дальнейшем, при задании правил доступа, вы можете выбрать только одну из существующих зон.



Чтобы сохранить изменения, нажмите кнопку «Сохранить».

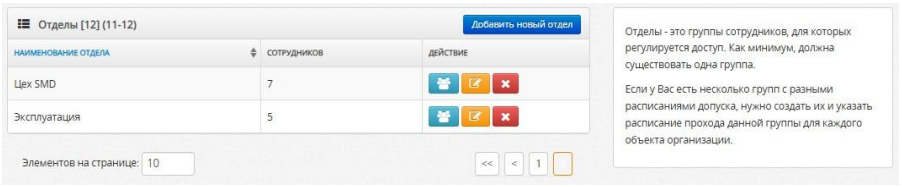


После сохранения информации настройка объектов закончена, и Вы можете приступить к вводу сотрудников и назначению карт.

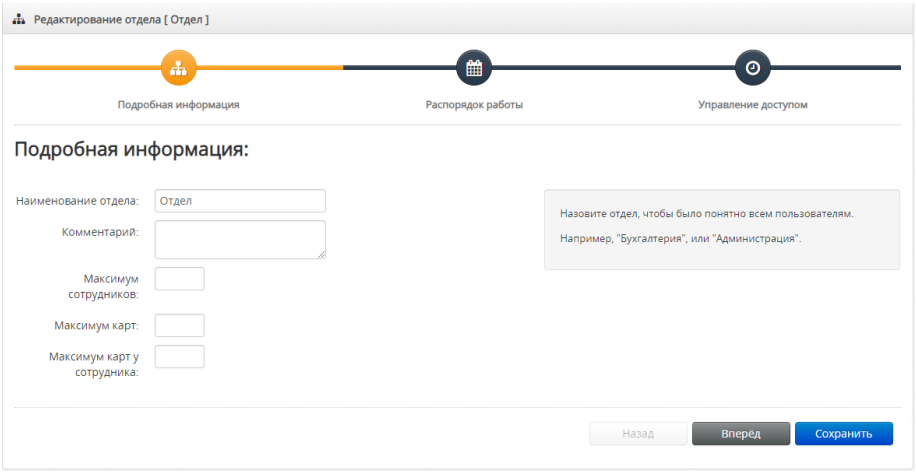
Вкладка «Отделы»

Добавление отдела

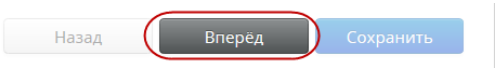
Отделы — это группы сотрудников, для которых регулируется доступ. Как минимум, должна существовать одна группа (отдел). Если у Вас есть несколько групп с разными расписаниями допуска, нужно создать их и указать расписание прохода данной группы для каждого объекта организации. Для управления группами сотрудников перейдите на вкладку «Отделы».



Вы можете создавать, удалять или редактировать Отделы. Для создания отдела нажмите кнопку «Добавить новый отдел». Сначала нужно ввести название отдела. Назовите отдел так, чтобы было понятно всем пользователям, например, «Бухгалтерия», или «Администрация».



Для продолжения нажмите на кнопку «Вперед» внизу экрана.



Распорядок работы

Распорядок используется для контроля трудовой дисциплины, но не ограничивает время доступа. По этим данным можно получать отчеты о посещаемости и времени, проведенном сотрудником на работе. В подразделе «Распорядок работы» можно ввести данные для контроля рабочего времени. Эти параметры будут использовании при создании отчетов.

Дополнительно представлены следующие параметры:

Ранний приход – время (в мин.), на сколько раньше начала рабочего дня допустимо появление работника. По умолчанию, 30 минут.

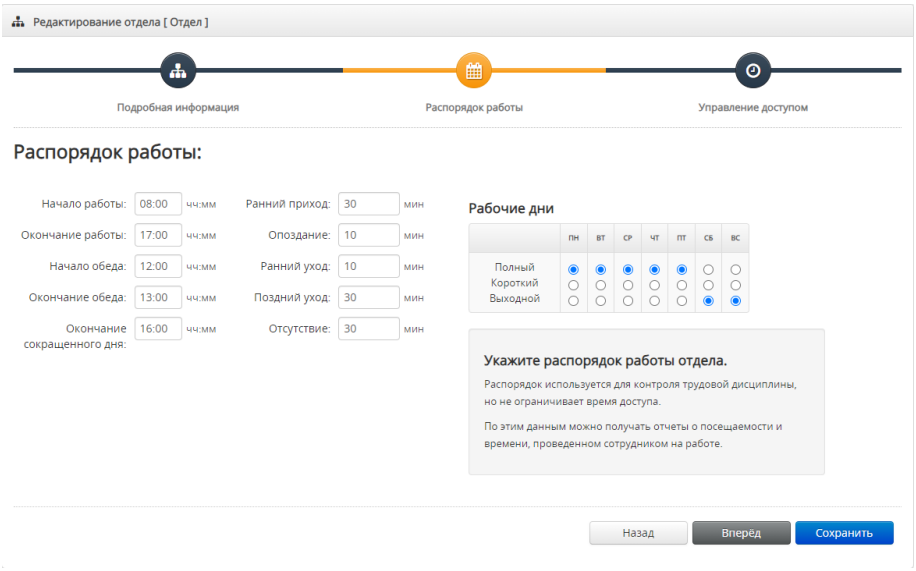
Опоздание – время (в мин.), на сколько позже начала рабочего дня допустимо появление работника. По умолчанию, 10 минут.

Ранний уход – время (в мин.), на сколько раньше окончания рабочего дня допустим уход работника. По умолчанию, 10 минут.

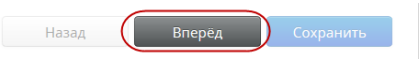
Поздний уход – время (в мин.), на сколько позже окончания рабочего дня допустим уход работника. По умолчанию, 30 минут.

Отсутствие – время (в мин.), на сколько суммарно допустимо отсутствие работника на рабочем месте в рабочее время в течение дня. По умолчанию, 30 минут.

По этим данным можно получать отчеты о посещаемости и времени, проведенном сотрудником на работе.



Для продолжения нажмите на кнопку «Вперед» внизу экрана.



Управление доступом

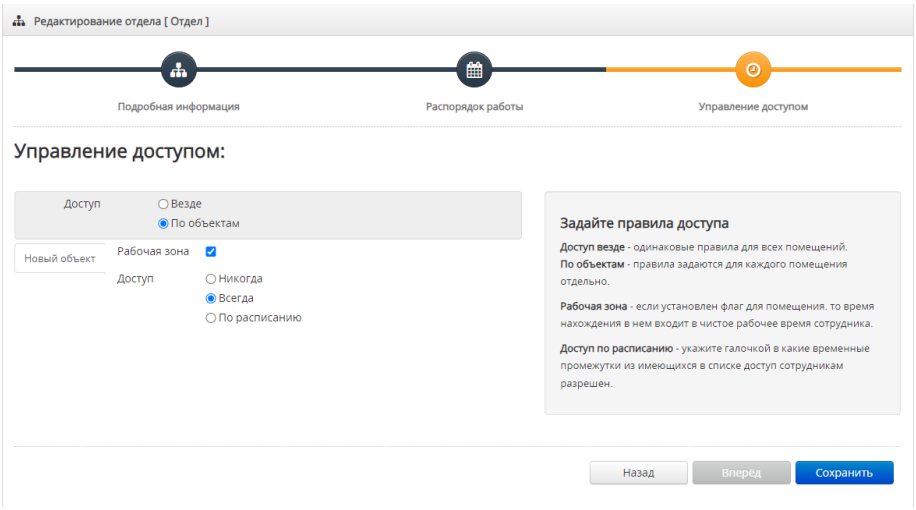
В подразделе «Управление доступом» можно задавать параметры доступа всех сотрудников отдела в каждое помещение.

Доступ везде - одинаковые правила для всех помещений.

По объектам - правила задаются для каждого помещения отдельно.

Рабочая зона - если установлен флаг для помещения, то время нахождения в нем входит в чистое рабочее время сотрудника.

Доступ по расписанию - укажите галочкой в какие временные промежутки из имеющихся в списке доступ сотрудникам разрешен.



Верхнее меню «Доступ» позволяет выбрать следующие разрешения: «Везде» или «По объектам». Если выбрать вариант «По объектам», то нужно назначить разрешения на каждый объект, созданный в системе.

Варианты доступа:

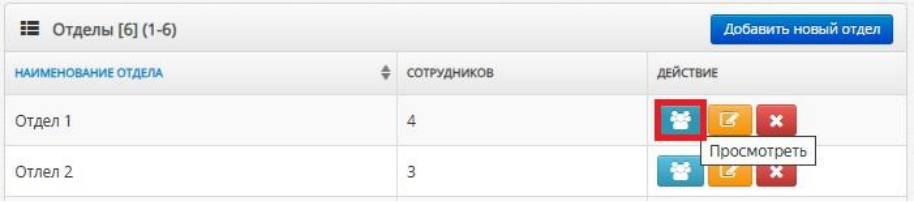
- Никогда;
- Всегда (по умолчанию);
- По расписанию.

Опция «**Рабочая зона**» используется для учета рабочего времени.

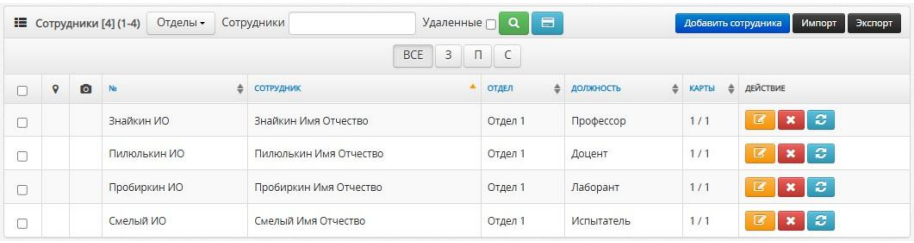
Чтобы сохранить изменения, нажмите кнопку «Сохранить».

Кнопка «Посмотреть»

Для просмотра информации по сотрудникам отдела есть кнопка «Посмотреть».

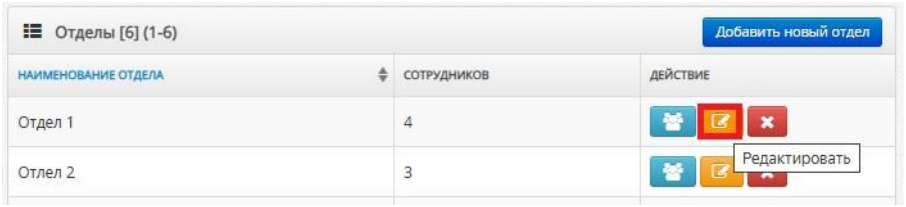


После нажатия на кнопку «Посмотреть» открывается окно «Сотрудники» со списком сотрудников этого отдела.

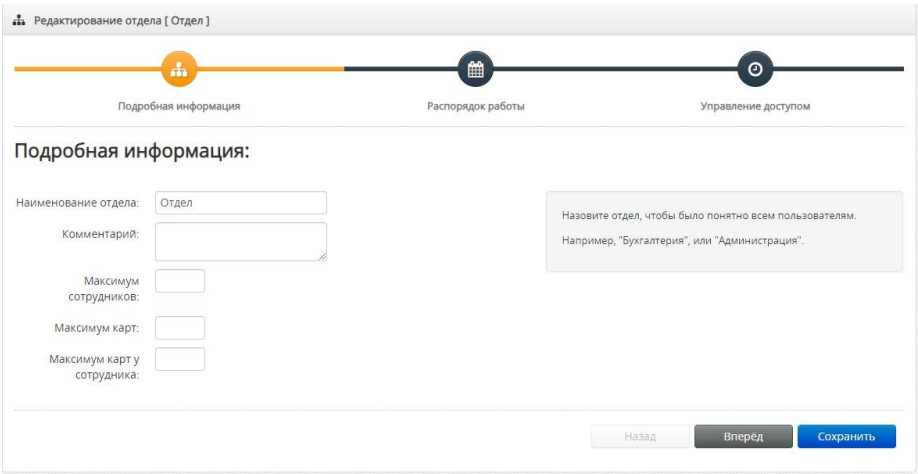


Кнопка «Редактировать»

Кнопка «Редактировать» позволяет редактировать настройки отдела.



После нажатия на кнопку «Редактировать» открывается окно «Редактирование отдела» с подразделами «Подробная информация», «Распорядок работы», «Управление доступом».



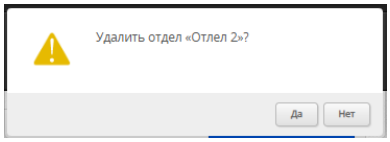
В подразделе «Подробная информация» переименуйте отдел при необходимости или измените другую информацию об отделе.
В подразделе «Распорядок работы» отредактируйте данные для контроля рабочего времени.
В подразделе «Управление доступом» откорректируйте параметры доступа всех сотрудников отдела в каждое помещение.

Кнопка «Удалить»

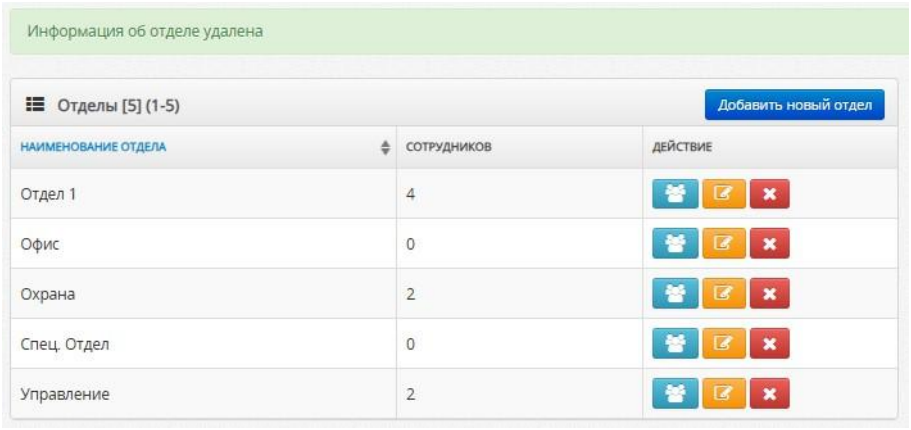
Кнопка «Удалить» позволяет удалить выбранный отдел.



После нажатия на кнопку «Удалить» появится окно предупреждения «Удалить отдел «Отдел 2»?», в котором нужно выбрать «Да».



Затем на экране отобразится строка «Информация об отделе удалена».



Вместе с отделом удалятся все сотрудники отдела.

Почему некоторые отделы в списке отмечены красным цветом?

В списке отделов некоторые записи помечены красным цветом.

Система контролирует настройку правил доступа и помечает отделы, у которых правила доступа не настроены, красным цветом.

Это может быть если:

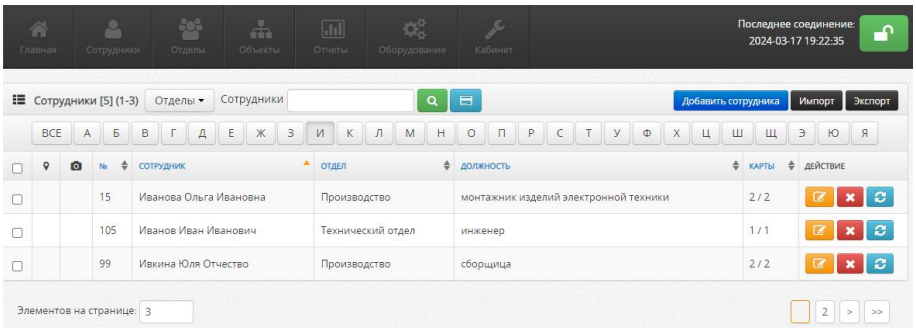
- Добавлено новое оборудование.
- У отдела нет действующих правил доступа к одному или нескольким объектам. Последнее может произойти, если Вы добавили в систему один или более объектов. Система не знает, нужно ли предоставлять доступ к новым объектам существующим отделам. Вам следует открыть карточку такого отдела, проверить все настройки доступа по всем объектам и сохранить карточку отдела.

После этого, индикация красным цветом этого отдела прекратится.

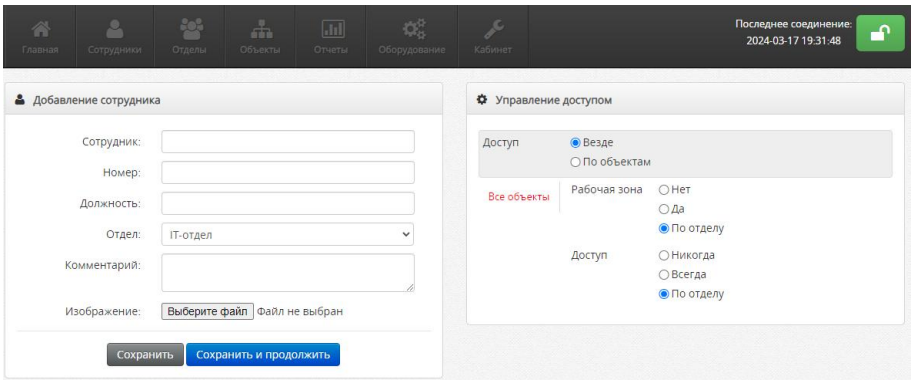
Вкладка «Сотрудники»

Добавление сотрудников

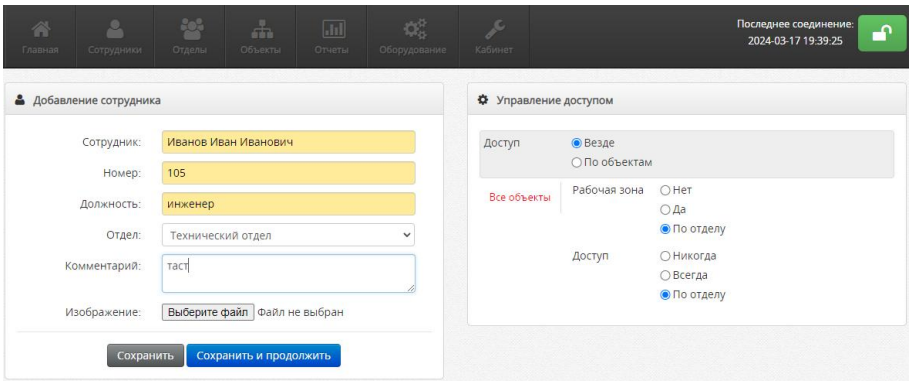
Для управления Сотрудниками, перейдите на вкладку «Сотрудники». На этой вкладке Вы можете создавать, удалять или редактировать сотрудников.



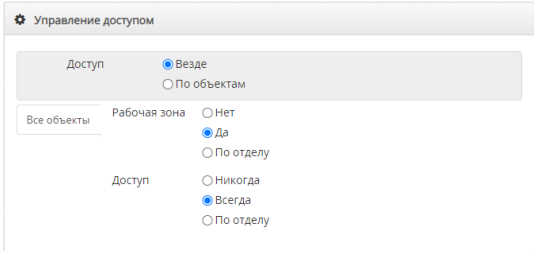
Для добавления нового сотрудника, кликните «Добавить сотрудника».



В окне «Добавление сотрудника» введите личные данные сотрудника, назначьте права доступа.



Доступ назначается либо «Везде», либо отдельно для каждого помещения и может быть выбран из списка:



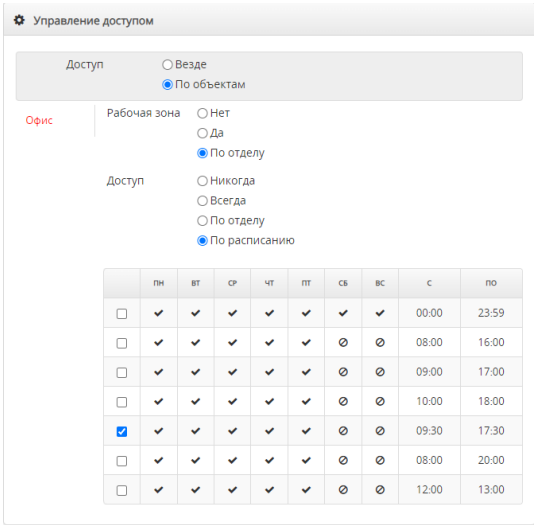
- Никогда – доступ запрещен;
- Всегда – доступ разрешен всегда;
- По расписанию – выберите необходимые временные зоны;
- По расписанию отдела – будет использоваться расписание отдела.

Опция «**Рабочая зона**» используется для учета рабочего времени:

- **По отделу** – время нахождения на объекте/объектах сотрудников **учитывается согласно настройкам отдела**;
- **Нет** – время нахождения на объекте/объектах **не учитывается** как рабочее;
- **Да** – время нахождения на объекте/объектах **учитывается** как рабочее.

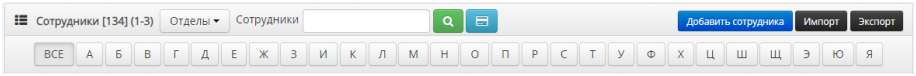
Если назначен доступ по «По объектам» и «По расписанию», нужно назначить временные зоны, во время которых доступ сотрудника в указанное помещение разрешен. Например,

сотрудник имеет право на доступ по 5-й временной зоне с 09:30 по 17:30. Для этого устанавливается флаг на 5-й зоне.



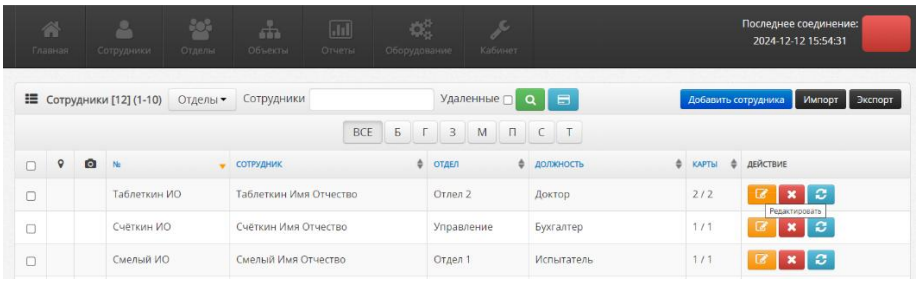
Для завершения процедуры добавления нового сотрудника нажмите кнопку «Сохранить». Если Вы хотите еще назначить карточку для сотрудника, нажмите кнопку «Сохранить и продолжить».

Для удобного поиска сотрудников, можно использовать специальные фильтры: «Отделы», «Сотрудники», «Удаленные», «Поиск по номеру карты».

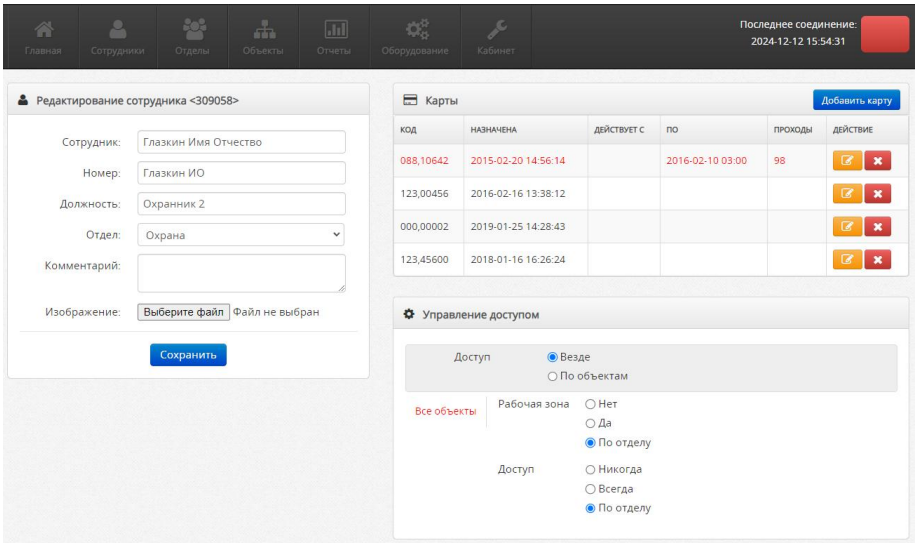


Редактирование сотрудников

Для редактирования сотрудника, перейдите на вкладку «Сотрудники».



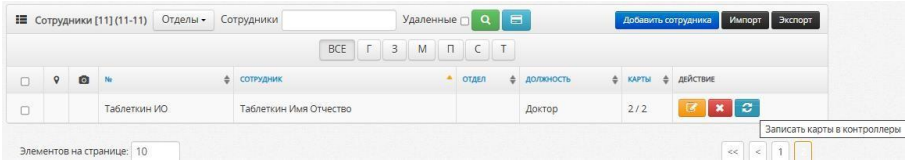
Кликните по кнопке «Редактировать». Откроется окно «Редактирование сотрудника».



В окне «Редактирование сотрудника» измените личные данные сотрудника, права доступа и назначенные карты. Для завершения процедуры редактирования сотрудника нажмите кнопку «Сохранить».

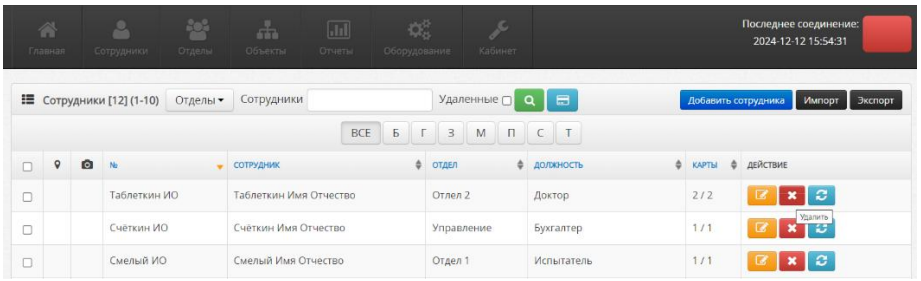
Кнопка «Записать карты в контроллеры»

После добавления или изменения карт при редактировании сотрудника нужно нажать на кнопку «Записать карты в контроллеры», чтобы измененные или добавленные карты выбранного сотрудника добавились в контроллеры согласно правам доступа.

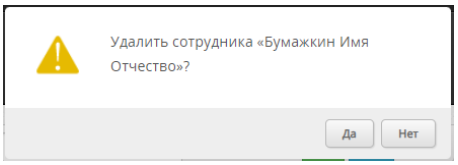


Удаление сотрудников

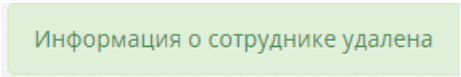
Для удаления сотрудника, перейдите на вкладку «Сотрудники».



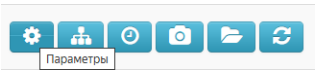
Кликните по кнопке «Удалить» напротив выбранного сотрудника. Откроется окно «Удалить сотрудника …?».



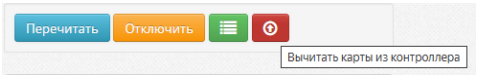
В этом окне кликните по кнопке «Да». Вверху появится строка информации «Информация о сотруднике удалена».



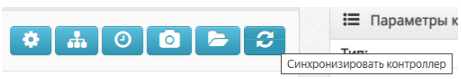
Следует помнить, что вместе с удалением сотрудника из аккаунта удаляются все его карты. Желательно эти карты не занимать в течение года, если планируется восстановить данного сотрудника или сделать по нему отчет.
Однако, после удаления сотрудника его карты остаются в контроллере, их нужно удалить из контроллера.
На вкладке «Оборудование/Контроллеры» напротив нужного контроллера нужно нажать кнопку «Параметры».



Затем в «Параметрах» кликнуть по кнопке «Вычитать карты из контроллера» и вычитать все карты из контроллера.



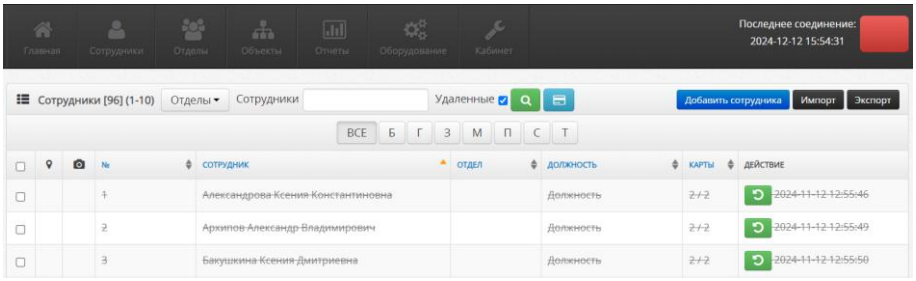
После вычитки карт нужно синхронизировать контроллер, кликнув по кнопке «Синхронизировать контроллер».



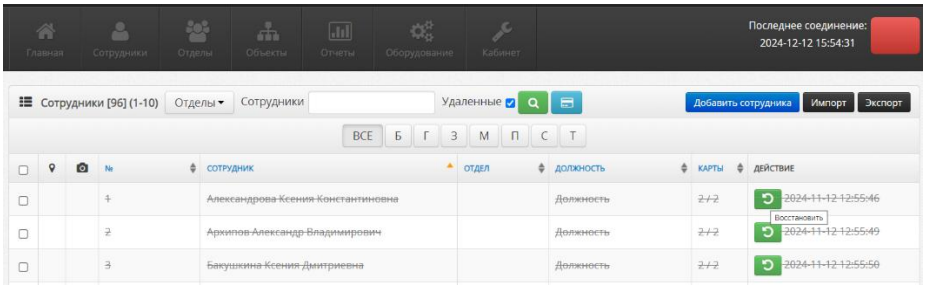
После завершения проделанных операций карты сотрудника удалены из контроллера.

Восстановление удаленных сотрудников

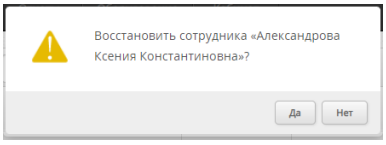
Для восстановления удалённого сотрудника, перейдите на вкладку «Сотрудники». Установите флаг «Удаленные» и кликните по кнопке «Искать».



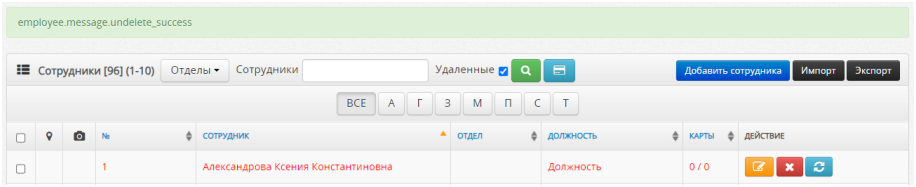
При сортировке по сотрудникам все удаленные сотрудники появятся в начале списка в перечеркнутом виде.



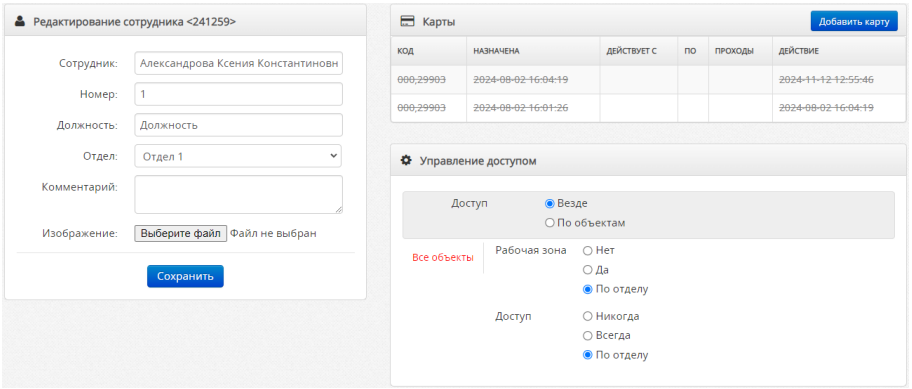
Для восстановления нужного сотрудника нужно кликнуть по кнопке «Восстановить».



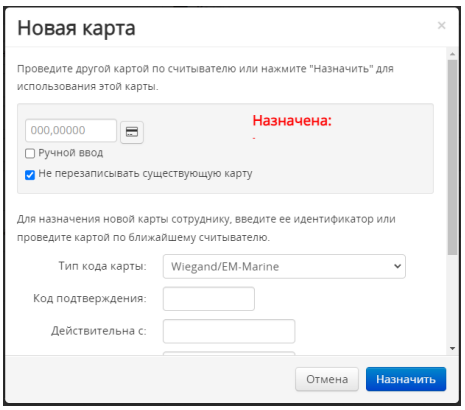
В окне «Восстановить сотрудника…» кликнуть по кнопке «Да».

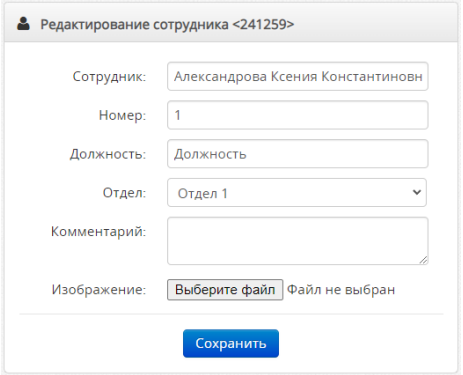


У восстановленного сотрудника нужно вручную добавить удаленные вместе с ним карты.



После добавления карты кликнуть по кнопке «Назначить».

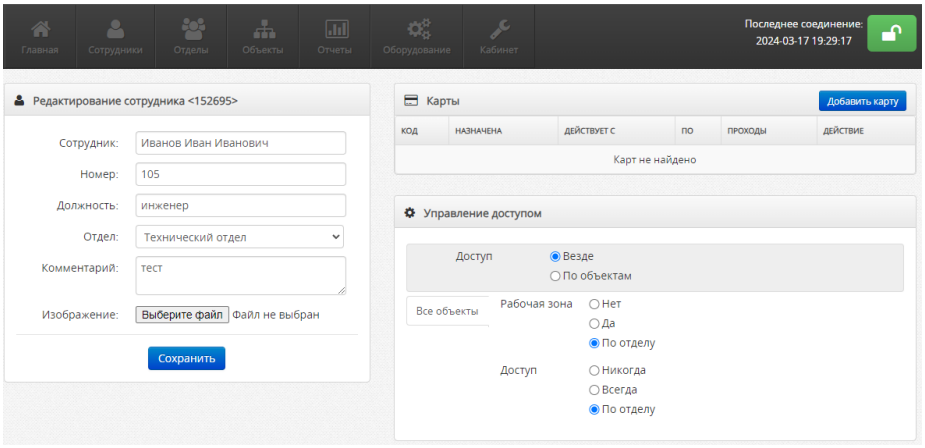




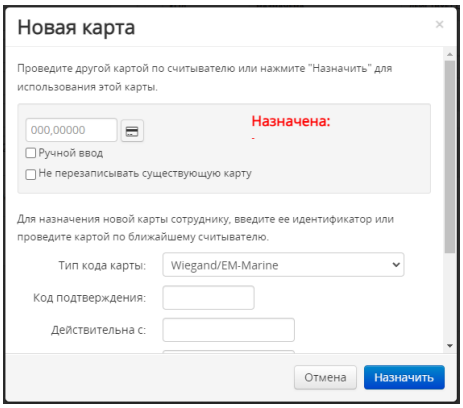
Для завершения процедуры восстановления в окне «Редактирование сотрудника» нажмите кнопку «Сохранить».

Назначение карты

Для добавления карты, нажмите кнопку «Добавить карту».

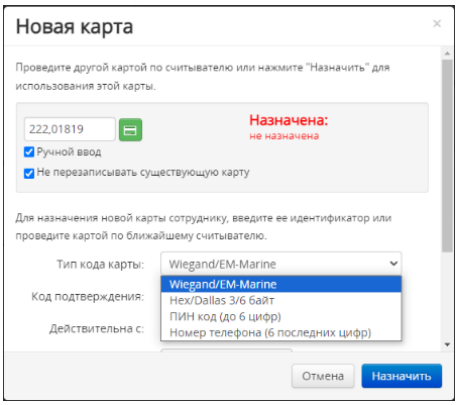


В данном окне также доступно «Управление доступом». Если на предыдущем шаге была допущена ошибка при назначении прав доступа, то здесь можно это исправить.
Появиться окно «Новая карта» для ввода номера карты. При создании сотрудника номер карты ещё можно исправить, после сохранения (кнопка «Назначить») номер карты изменить нельзя.

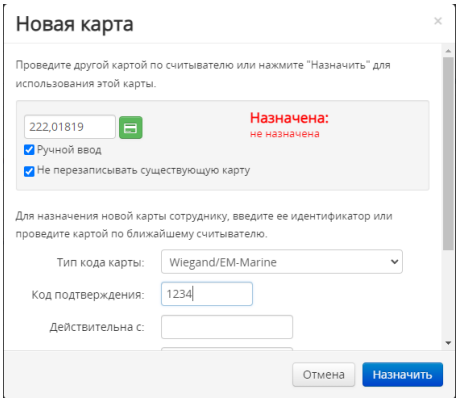


При вводе карты можно выбрать:

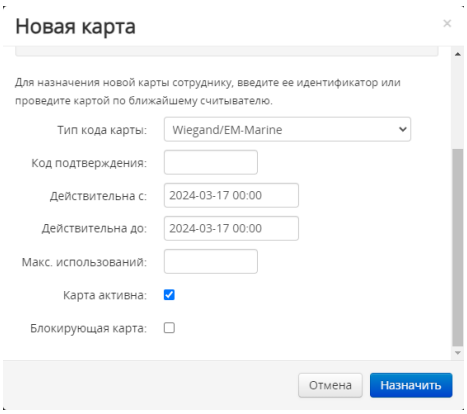
- Тип кода карты – Ввод номера карты в форматах: Wiegand/EM-Marine, Hex/Dallas 3/6 байт, пин-код (до 6 цифр), номер телефона (6 последних цифр).



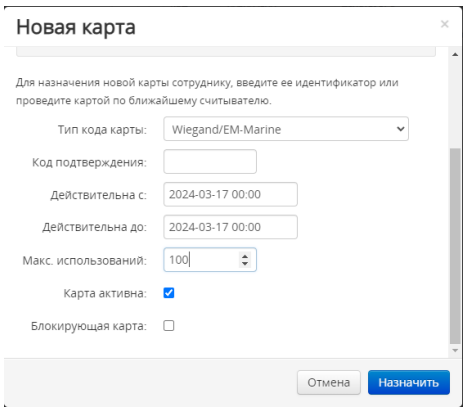
- Код подтверждения – Ввести код подтверждения для прохода по карте и коду. Например, 222,01819+1234.

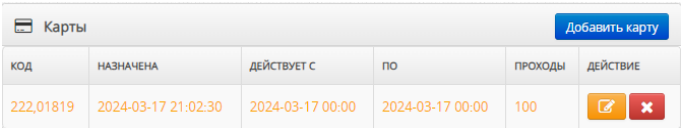


- Период действия карты. («Действительна с:» и «Действительна до:»)



- Макс. использований – Максимальное количество использований карты для прохода. Счетчик в графе «Проходы» после каждого прохода будет уменьшаться на единицу.

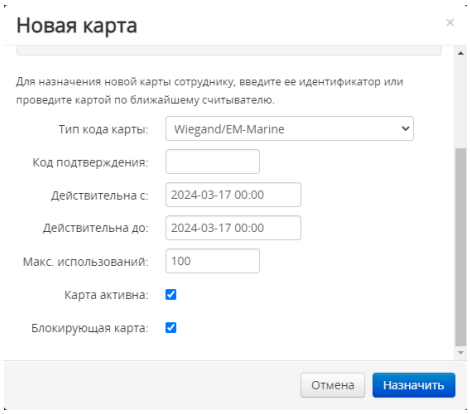




- Флаг «Карты активна» - устанавливается, если карту нужно активировать сразу после ввода.



- Флаг «Блокирующая карта» – устанавливается если нужно создать блокирующую карту.

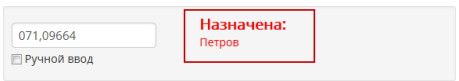


Возможны следующие 3 способа назначения карты:

- **Ручной ввод номера карты;**
- **Автоматический ввод карты;**
- **Ввод карты через USB считыватель**.

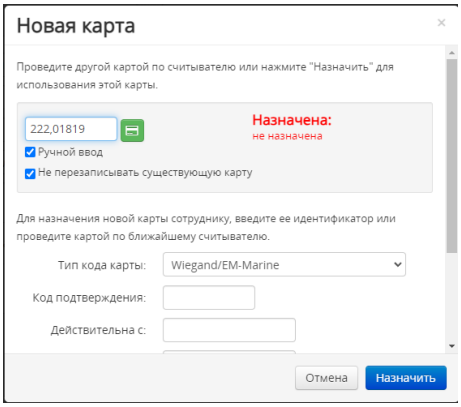
Ручной ввод номера карты

Введите с клавиатуры 8-значный номер идентификатора. Используйте опцию «Ручной ввод», чтобы считывания карт других сотрудников не мешали вводу идентификатора.

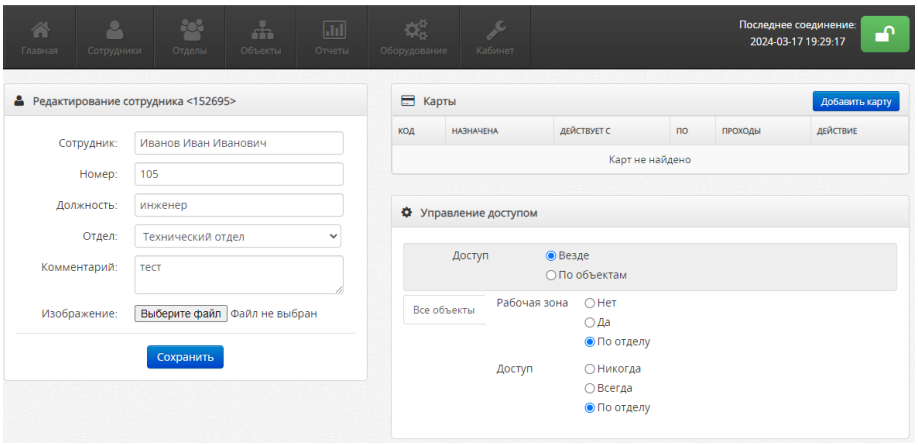


Если введенная карта уже назначена на другого сотрудника, это выводится на экран. Но Вы можете переназначить ее на нового сотрудника.

В поле «Действительна до» введите дату окончания действия карты. В поле «Макс. Использования» введите максимальное количество использования карты.

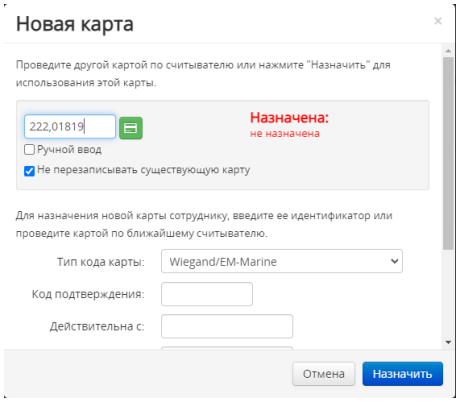


Для сохранения введенной карты нажмите кнопку «Назначить». Карта появится в списке. Чтобы сохранить изменения, нажмите кнопку «Сохранить».

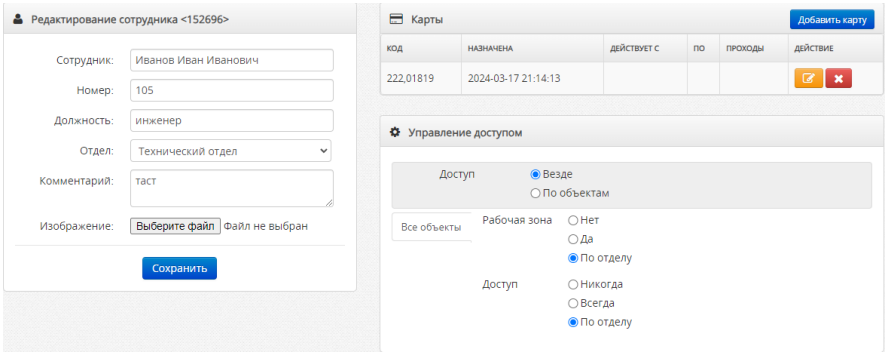


Автоматический ввод карты

Автоматический ввод карты – проведите картой по ближайшему считывателю, подключенному к контроллеру. Номер карты сразу отобразится.



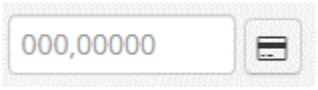
Система опрашивает только те контроллеры, которые имеют настройку «Использовать для ввода карт» в настройке оборудования.
Для сохранения введенной карты нажмите кнопку «Назначить». Карта появится в списке. Чтобы сохранить изменения, нажмите кнопку «Сохранить».



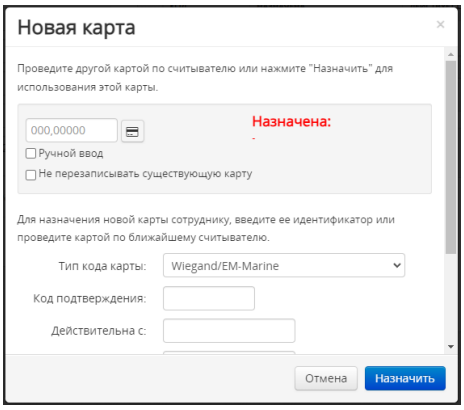
Ввод карты через USB считыватель

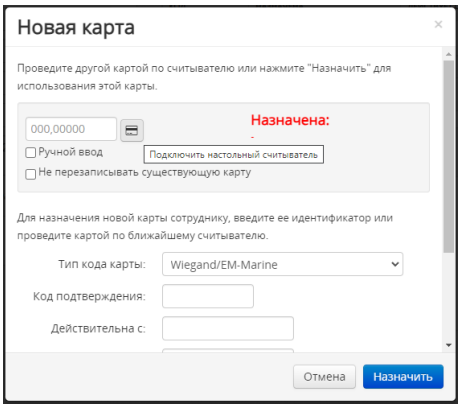
Настольный считыватель позволяет вводить идентификаторы (карты, брелоки и т.д.) сотрудникам в аккаунте.

На сервере добавлена поддержка настольных считывателей. Работает на форме добавления карты сотруднику и в поиске по картам. Добавлена кнопка справа от окна ввода карты, которая позволяет выбрать настольный считыватель.

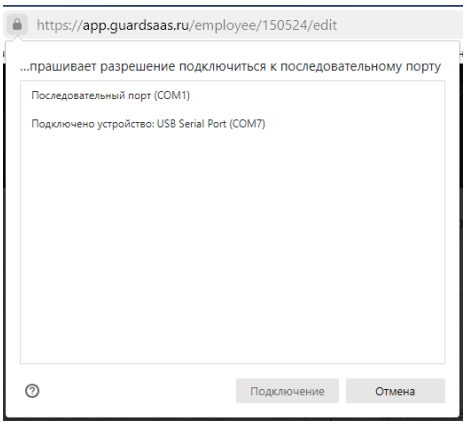


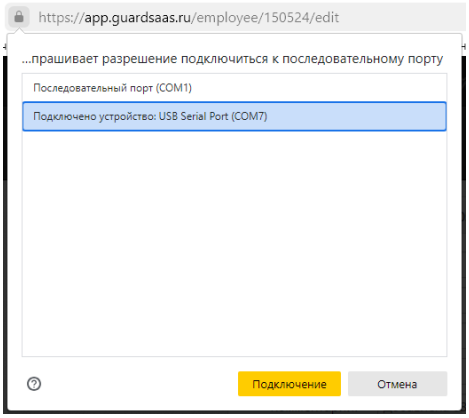
Кликаем по кнопке справа от поля ввода карты «Подключить настольный считыватель».



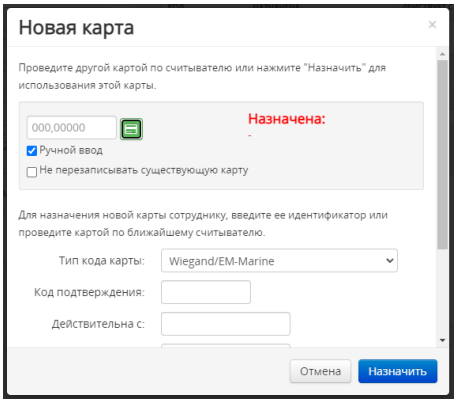


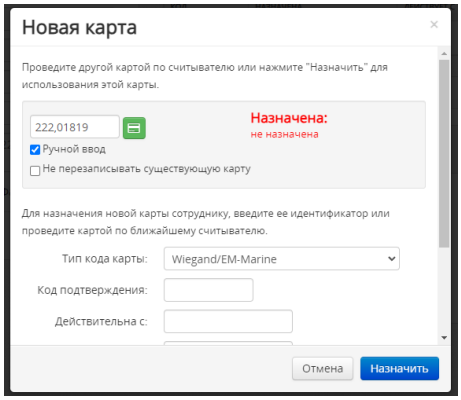
На экране появится запрос браузера на подключение к последовательному порту. Выбираем порт, на котором установлен настольный считыватель и нажимаем кнопку «Подключение».



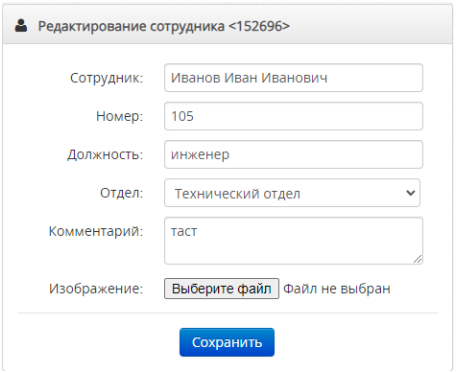


Кнопка «Подключить настольный считыватель» подсветится зеленым цветом. Прикладываем карту к настольному считывателю, номер карты отобразится в окне добавления. Далее нужно назначить карту, кликнув по кнопке «Назначить».

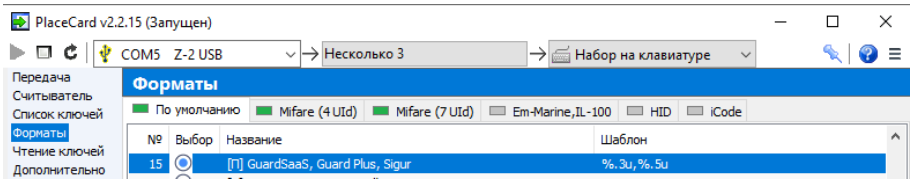




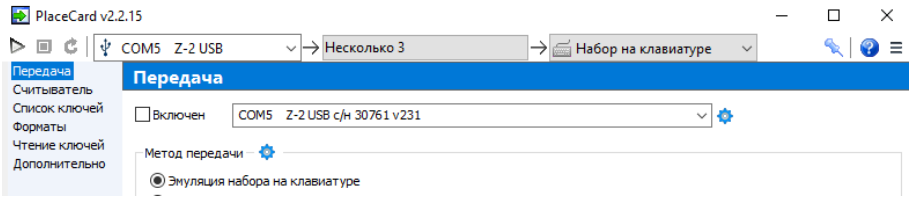
Для сохранения введенной карты нажмите кнопку «Назначить». Карта появится в списке. Чтобы сохранить изменения, нажмите кнопку «Сохранить».



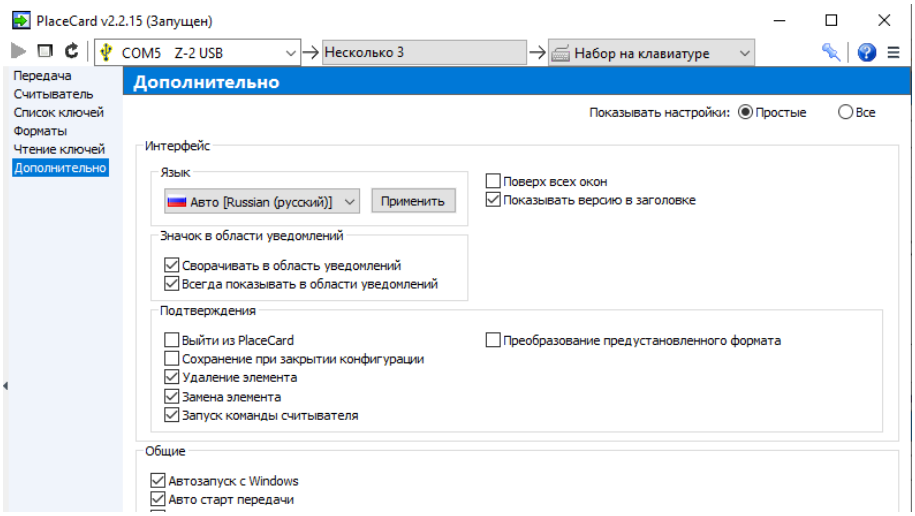
Этот метод работает только в Chromium браузерах (Chrome, Edge, Opera и т.д.), и не работает в Firefox и Safari. Для использования настольного считывателя в других браузерах нужно скачать и установить ПО PlaceCard по Руководству к ПО. Далее нужно настроить ПО согласно Руководству. Обязательно на вкладке «Формат» выбирается формат «Guardsaas».



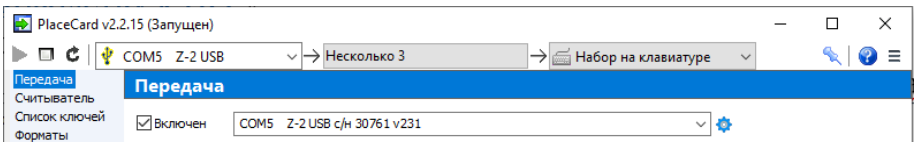
Затем на вкладке «Передача» нужно выбрать режим «Эмуляция набора на клавиатуре.



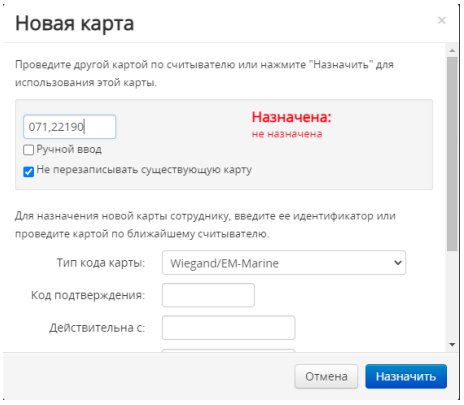
На вкладке «Дополнительно» должны быть установлены флаги: «Сворачивать в область уведомлений», «Автозапуск с Windows», «Автостарт передачи».



После окончания настройки нужно установить флаг «Включен».

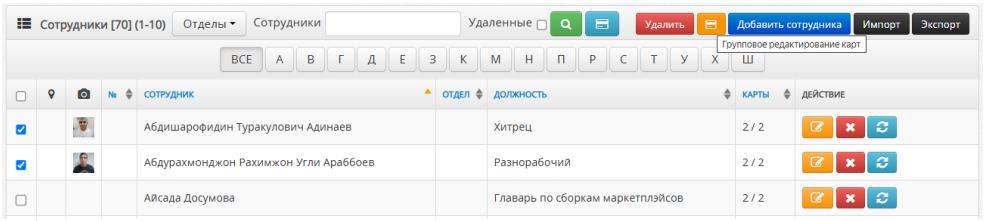


ПО PlaceCard будет передавать номер карты в активное окно (там должен мигать курсор) добавления карты сотруднику.



Групповое редактирование карт

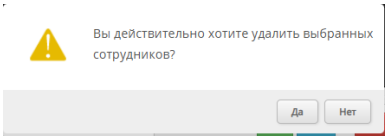
Для группового изменения карт нужно поставить флаги в первой графе перед нужными сотрудниками на вкладке «Сотрудники».



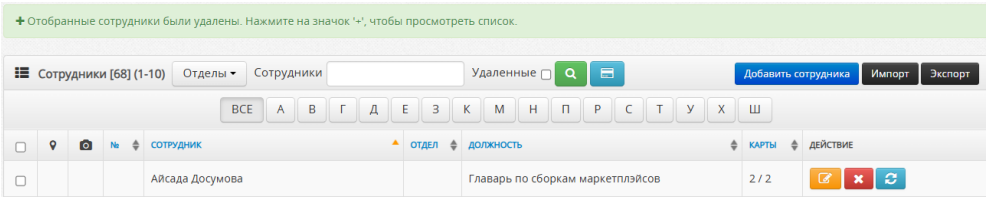
В панели инструментов появятся две кнопки: «Удалить» и «Групповое редактирование карт».

Групповое удаление выбранных сотрудников с картами

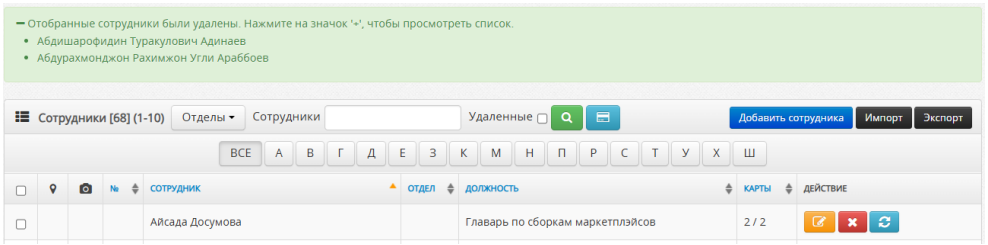
При нажатии на кнопку «Удалить», появится окно предупреждения «Вы действительно хотите удалить выбранных сотрудников?». Нужно кликнуть по кнопке «Да».



Выбранные сотрудники удалятся из списка. Сверху появится информация «Отобранные сотрудники были удалены. Нажмите на значок «+», чтобы просмотреть список.»

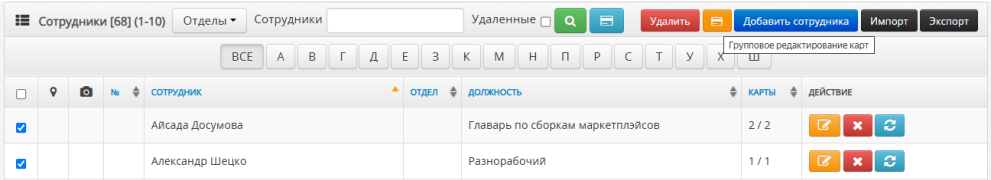


После нажатия на значок «+» развернется список удаленных сотрудников.

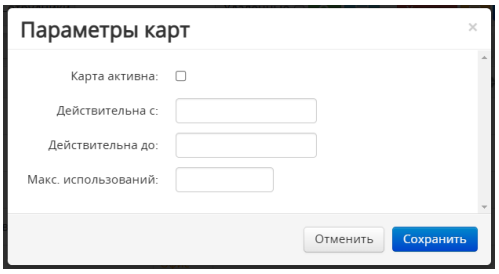


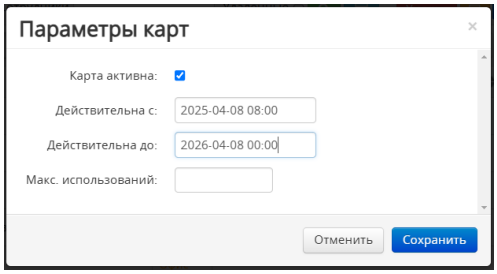
Групповое редактирование карт у выбранных сотрудников

Для группового редактирования карт нужно выбрать сотрудников, поставив флаги в первой графе перед нужными сотрудниками на вкладке «Сотрудники».

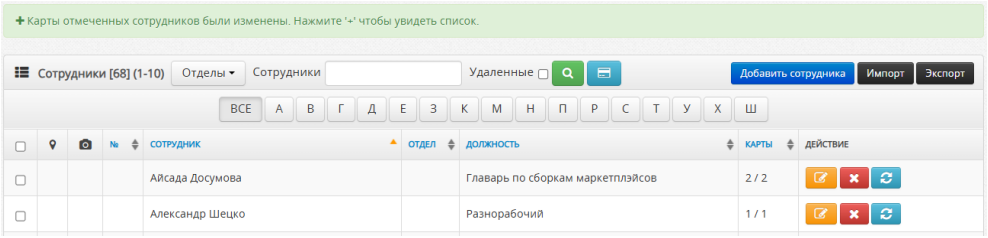


При нажатии на кнопку «Групповое редактирование карт» появится окно «Параметры карт». В этом окне можно активировать или деактивировать карты, указать период действия карт, максимальное количество использований.

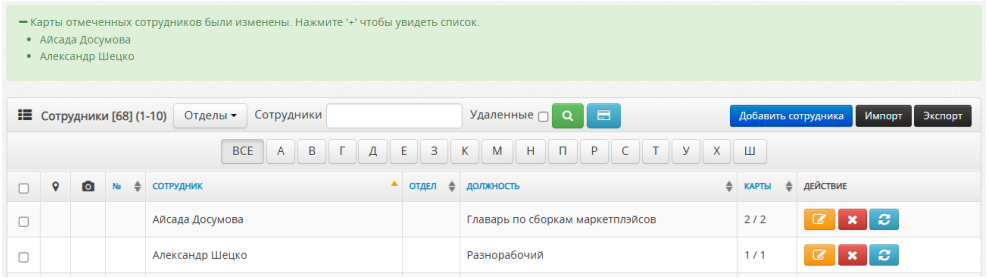




Для применения всех изменений нужно кликнуть по кнопке «Сохранить». После сохранения вверху появится информация «Карты отмеченных сотрудников были изменены. Нажмите «+», чтобы увидеть список.»

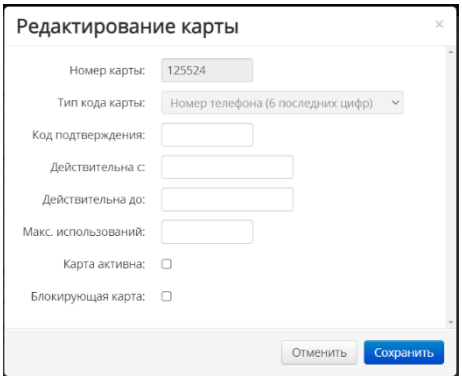


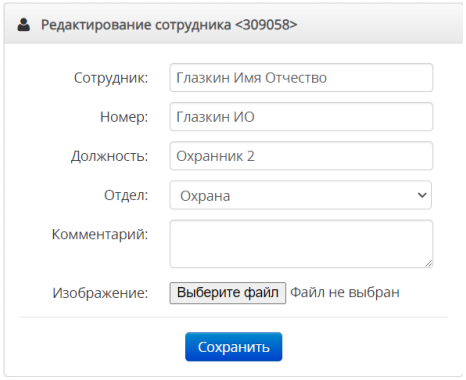
После нажатия на значок «+» развернется список измененных сотрудников.



Деактивация карты

Для деактивации карты, нужно открыть окно «Редактирование карты» и строке «Карта активна» снять флаг и кликнуть по кнопке «Сохранить».

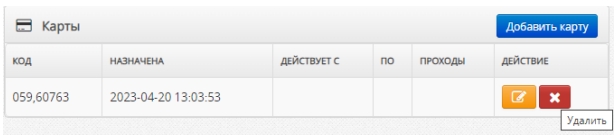




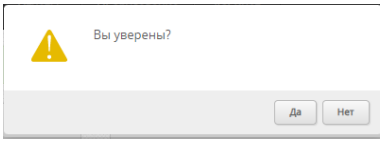
Затем для завершения процедуры редактирования в окне «Редактирование сотрудника» нажмите кнопку «Сохранить».

Удаление карты

Для удаления карты, нужно кликнуть по красной кнопке с крестом «Удалить» в списке назначенных карт.

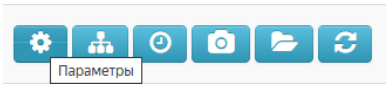


Появится окно предупреждения «Вы уверены?», в котором нужно нажать кнопку «Да». После подтверждения карта будет удалена из системы.

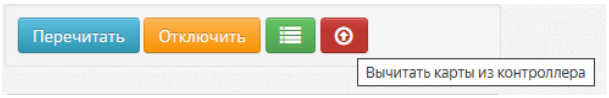


Однако, после удаления карты из аккаунта она остаётся в контроллере, её нужно удалить из контроллера.

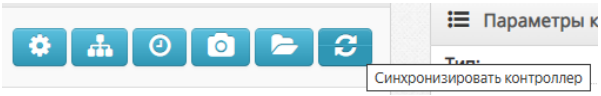
На вкладке «Оборудование/Контроллеры» напротив нужного контроллера нужно нажать кнопку «Параметры».



Затем в «Параметрах» кликнуть по кнопке «Вычитать карты из контроллера» и вычитать все карты из контроллера.



После вычитки карт нужно синхронизировать контроллер, кликнув по кнопке «Синхронизировать контроллер».



После завершения проделанных операций карта будет удалена из контроллера.

Возможные проблемы при назначении карт и работе с ними

Проблемы с синхронизацией карт

При появлении проблем синхронизации карт нужно вычитать все карты из контроллера принудительно и потом заново его синхронизировать.

Для надежности надо повторить эту процедуру для всех контроллеров (по одному и по очереди):

1) Вычитать все карты;
2) Синхронизировать контроллер.

Не получается зарегистрировать новую карту

При поднесении новой карты к считывателю ее код не появляется в поле номера карты.

Нужно проверить:

1) Наличие связи с оборудованием – индикатор связи в правом верхнем углу экрана. Если он красный, то с ним нет связи;
2) Если связь есть и индикатор зеленый, то обновите прошивки контроллеров на актуальные.

Не отображается код карты при поднесении к считывателю

При поднесении карты к считывателю и в списке событий не отображается код карты. Считыватель издает сигнал, но в поле кода карты пусто. В списке событий указано «Ключ не найден» и пустое поле кода.

Считыватель может быть неправильно подключен к контроллеру. Также такая проблема проявляется при использовании устаревших прошивок контроллеров. Рекомендуем обновить прошивки контроллеров до версий:

- Z-5R (мод. Net) – 2.21 +
- Z-5R (мод. Net 8000) – 2.25 +
- Z-5R (мод. Net 16000) – 3.4 +
- Matrix-II (мод. E K Net) – 2.25 +
- Z-5R (мод. Web) – 3.48
- Z-5R (мод. Web BT) – 2.38
- Matrix-II (мод. E K Wi-Fi) – 2.55
- Z-5R (мод. Wi-Fi) – 2.55

После регистрации новой карты она не открывает дверь

Если после регистрации новой карты она не открывает дверь, нужно:

1) Проверить состояние конвертера. Если иконка конвертера выглядит как красный замок в закрытом состоянии, то конвертер находится в режиме LOCK и не позволяет серверу

записывать в него информацию. Переключите конвертер в режим UNLOCK с помощью переключателя на корпусе.

2) Проверить какое событие создается – «Отчет» – «События».

- Если события нет, то скорее всего есть проблемы связи с оборудованием. Нужно проверить индикатор связи в правом верхнем углу.

- Если индикатор связи красный, то нет связи с оборудованием.
- Если индикатор зеленый, а события нет, то скорее всего тип карты несовместим со считывателем. Нужно использовать совместимые типы карты.
- Если событие есть, но номер карты отсутствует, то нужно обновить прошивку контроллера.
- Если событие есть, и его тип «Доступ Запрещен», то необходимо сделать синхронизацию контроллера. Если это не помогает, то проверить правильность настройки прав доступа и прошивку контроллера.

Почему некоторые сотрудники в списке отмечены красным цветом?

В списке сотрудников некоторые записи помечены красным цветом.

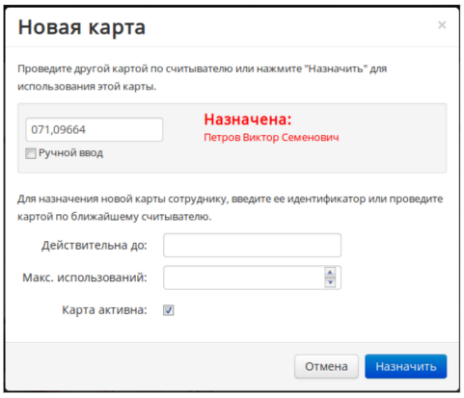
Система контролирует настройку правил доступа и помечает сотрудников, у которых правила доступа не настроены, красным цветом. Это может быть если:

- У сотрудника нет ни одной назначенной карты.
- У сотрудника нет действующих правил доступа к одному или нескольким объектам. Последнее может произойти, если Вы добавили в систему один или более объектов. Система не знает, нужно ли предоставлять доступ к новым объектам существующим сотрудникам. Вам следует открыть карточку такого сотрудника, проверить все настройки доступа по всем объектам и сохранить карточку сотрудника.

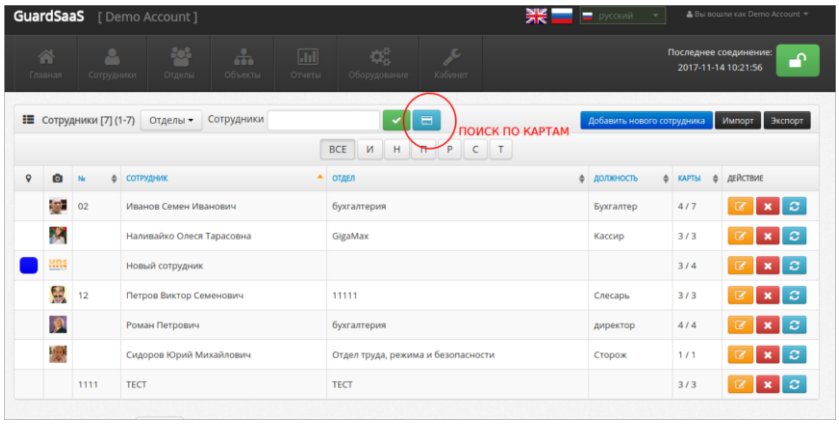
После этого, индикация красным цветом этого сотрудника прекратится.

Как узнать, какому сотруднику принадлежит карточка?

Откройте список карт любого сотрудника, затем нажмите кнопку «Добавить карту». Появится окно ожидания ввода номера карты. Поднесите карту к любому считывателю, назначенному регистрировать новые карты. Также можно использовать считыватель Z-2 USB. После определения номера карты появится имя сотрудника, которому назначена карта на данный момент.

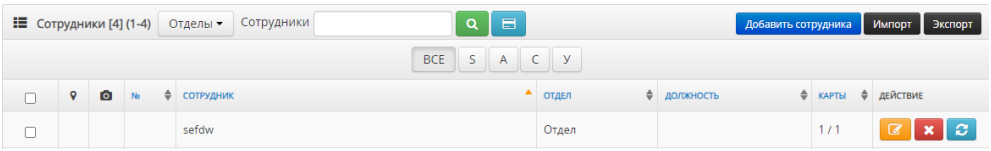


В сервисе также добавлена возможность поиска по картам в списке сотрудников.



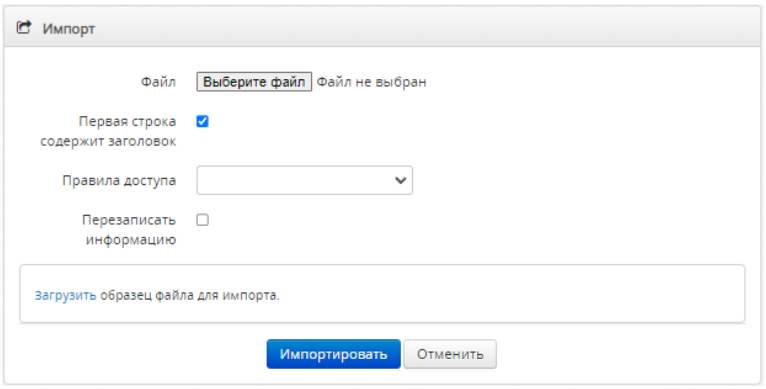
Импорт/ Экспорт сотрудников

В система GuardSaaS предусмотрен также **импорт** и **экспорт** сотрудников.

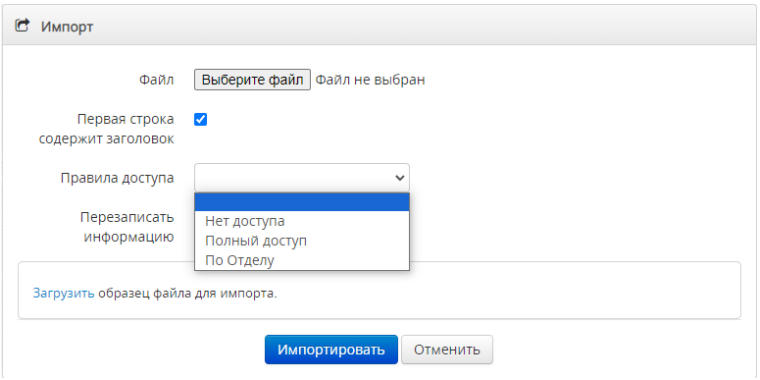


Импорт

Для импорта нажмите кнопку «Импорт». Далее кликните по кнопке «Выберите файл» и вставьте из проводника файл с сотрудниками. Поддерживаемый формат – **XLS**, **XML**, **ZIP.** Затем нажмите кнопку «Импортировать».

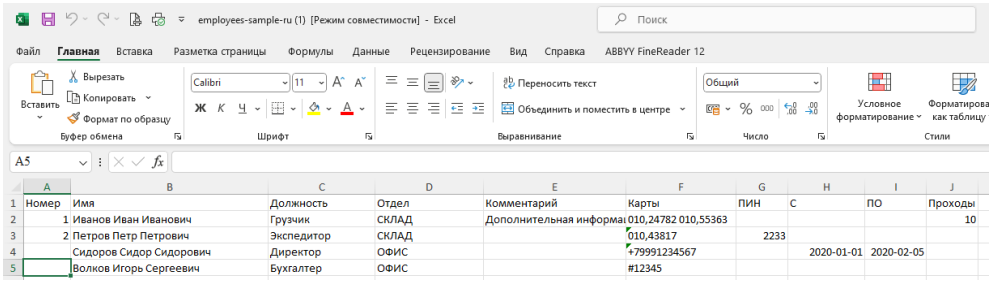


До импорта в окне «Правила доступа» можно указать права доступа для загружаемого списка сотрудников (Нет доступа, Полный доступ, По Отделу).



Если уже была загружена база, её можно перезаписать, установив флаг «Перезаписать информацию».
Для примера можно скачать образец файла для импорта, кликнув по ссылке «Загрузить».

В папку с загрузками скачается файл «employees-sample-ru.xls».

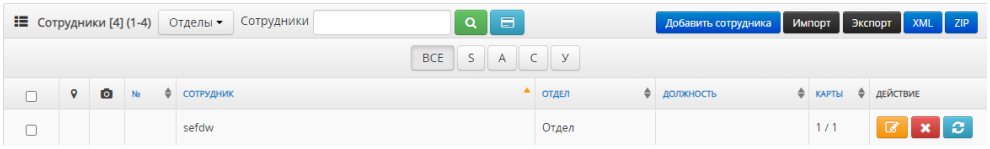


Нужно заполнить этот файл, не изменяя формата столбцов. Затем заполненный файл можно вставить при импорте.

В систему GuardSaaS можно, например, импортировать **XML** файл сотрудников из Guard Light. Этот функционал облегчит Вам переход с Guard Light на облачную систему GuardSaaS.

Экспорт

Для экспорта нажмите кнопку «Экспорт». Появятся дополнительные кнопки «XML» и «ZIP».



Для сохранения списка сотрудников в формате **XML** кликните по кнопке «XML». В «Загрузки» браузера скачается файл вида «employees-20240315143737.xml»

This XML file does not appear to have any style information associated with it. The document tree is shown below.


```
<Export>
  <Base>
    <Group Name="отдел 4" ID="6605" Comment="">
      <User Name="Укапр" Pos="" ID="126269" Number="" Comment="" Picture="">
        <Card Name="(123,04522)" Num="AA 11 7B" Comment="Добавлена 01.31.24" Type="0" Assigned="2024-01-31 16:20:25"/>
      </User>
    </Group>
    <Group Name="Отдел" ID="6606" Comment="">
      <User Name="sefdw" Pos="" ID="126267" Number="" Comment="" Picture="">
        <Card Name="(123,04567)" Num="D7 11 7B" Comment="Добавлена 01.31.24" Type="0" Assigned="2024-01-31 15:06:18"/>
      </User>
    </Group>
    <Group Name="отдел3" ID="6607" Comment="">
      <User Name="аааа" Pos="" ID="126268" Number="" Comment="" Picture="">
        <Card Name="(234,05678)" Num="2E 16 EA" Comment="Добавлена 01.31.24" Type="0" Assigned="2024-01-31 15:06:57"/>
        <Card Name="(255,03434)" Num="6A 0D FF" Comment="Добавлена 01.31.24" Type="0" Assigned="2024-01-31 16:29:45"/>
      </User>
    </Group>
    <Group Name="ОФИС" ID="6609" Comment="">
      <User Name="Сидоров Сидор Сидорович" Pos="Директор" ID="126272" Number="" Comment="" Picture="aa90e67d5fc41662173525b8d4e02ba9b3f5fccf.jpeg">
        <Card Name="(234567)" Num="67 45 23" Comment="Добавлена 01.31.24" Type="4" Assigned="2024-01-31 16:25:42" ValidFrom="2020-01-01 00:00:00" ValidTo="2020-02-05 00:00:00"/>
      </User>
    </Group>
  </Base>
</Export>
```


Для сохранения списка сотрудников с фотографиями в формате **ZIP** кликните по кнопке «ZIP». В «Загрузки» браузера скачается архив вида «employees-20250326142902.zip» В этом архиве находятся папка с фотографиями «img» и файл с базой «employees.xml».

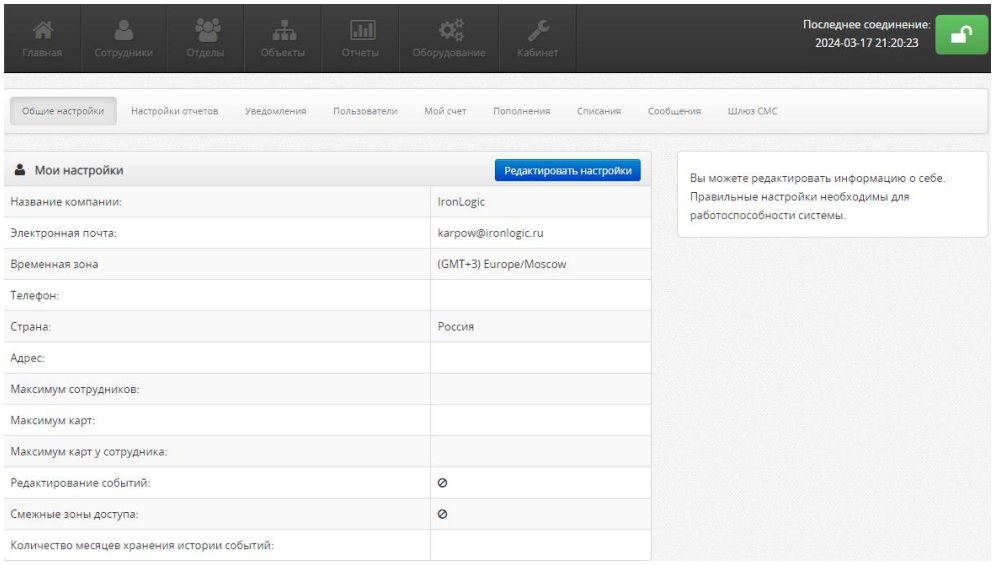


Вкладка «Кабинет»

Для управления своим счетом, аккаунтом, оплатой и другими настройками, используется раздел «Кабинет». Для управления Профилем, перейдите на вкладку «Кабинет».

Общие настройки

В подразделе «Общие настройки» можно изменить текущие настройки профиля: название компании, адрес электронной почты, временную зону, телефон, страну, адрес.



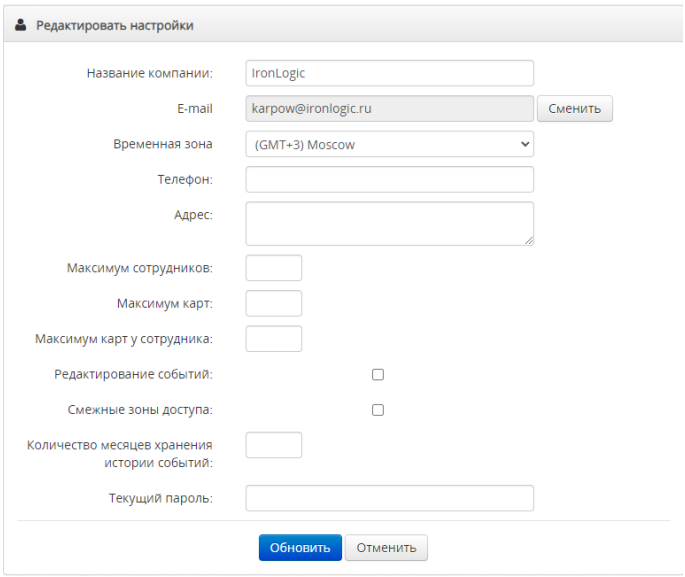
Для доступа к этому разделу, у Вашего пользователя должны быть установлены соответствующие права.

Для редактирования профиля нажмите кнопку «Редактировать настройки».

Обязательными для профиля являются следующие настройки:

- **Электронная почта** – для входа в систему (задается при регистрации);
- **Временная зона** – для правильности отображения времени в системе;
- **Страна** – тариф и валюта оплаты зависят от страны (задается при регистрации).

Окно редактирования настроек профиля представлено ниже:



Доступны для изменения следующие настройки:

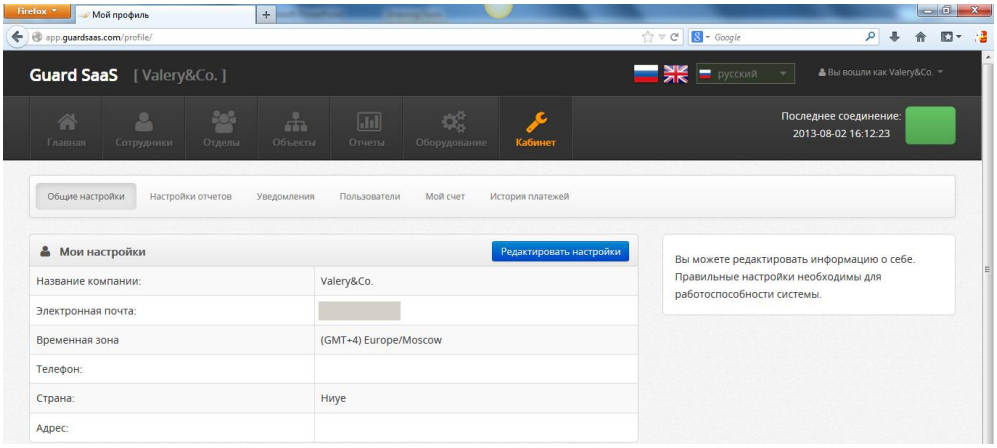
- **Название компании:** – Введите название Вашей компании.
- **E-mail** – Нажмите кнопку «Сменить» и введите новый адрес электронной почты. На указанный адрес придет письмо. Подтвердите смену e-mail, кликнув по ссылке в этом письме.
- **Временная зона** – Выберите Вашу временную зону.
- **Телефон:** – Укажите по Вашему желанию телефон для контакта.

- **Адрес:** – Укажите по Вашему желанию адрес для контакта.
- **Максимум сотрудников:** – Максимальное количество сотрудников в системе.
- **Максимум карт:** – Максимальное количество карт в системе.
- **Максимум карт у сотрудника:** – Максимальное количество карт у одного сотрудника.
- **Редактирование событий:** – Возможность редактировать события в отчете «События».
- **Смежные зоны доступа:** – Флаг устанавливается для смежных помещений и для показа кнопки «Объекты» на вкладке «Оборудование/Контроллеры».
- **Количество месяцев хранения истории событий:** – Задается период хранения всех событий в системе.
- **Текущий пароль:** – введите текущий пароль для разрешения внесенных изменений.

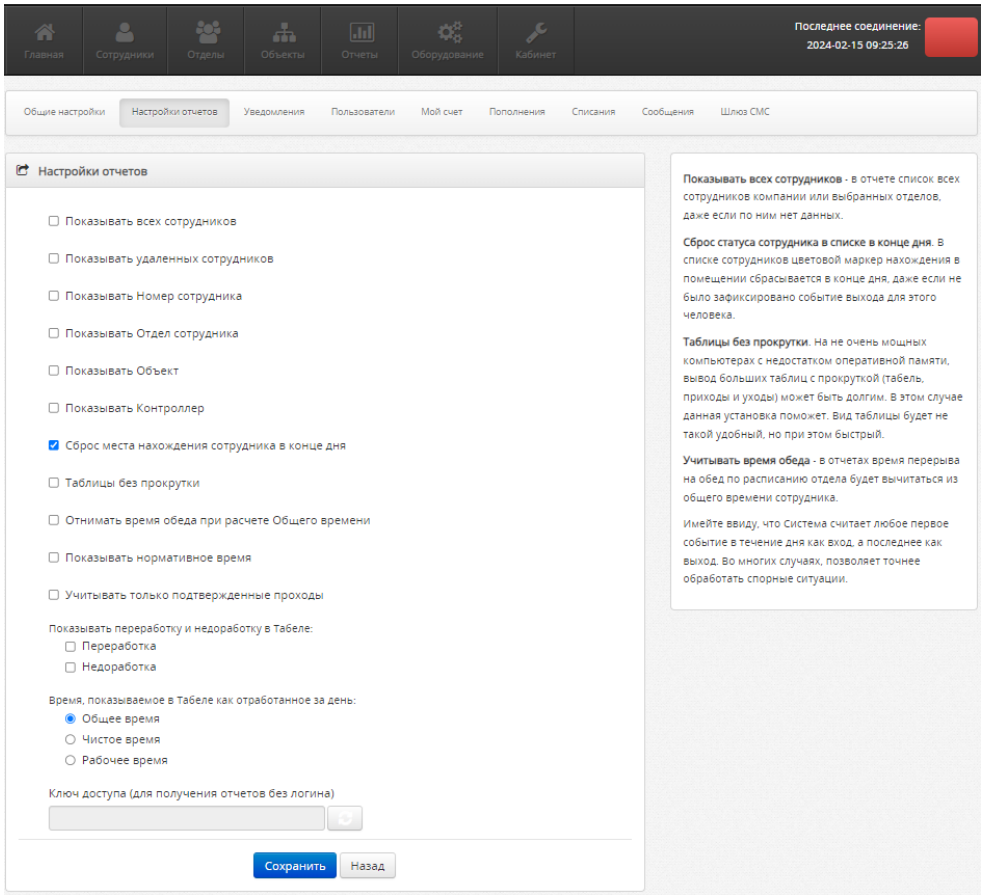
Для вступления изменений в силу нажмите кнопку «Обновить».

Настройки отчетов

Управление общими параметрами вывода отчетов осуществляется в разделе «Настройки отчетов». Для управления Отчетами, перейдите на вкладку «Кабинет».



Далее кликните на разделе «Настройка отчетов». Измените необходимые настройки вывода отчетов.



Представлены следующие настройки:

Показывать всех сотрудников - если у сотрудника нет данных по фактическим проходам за выбранный период, то он все равно показывается в списке отчета.
Показывать удаленных сотрудников – показывать удаленных ранее сотрудников.
Показывать Номер сотрудника - показывать колонку с номером сотрудника
Показывать Отдел сотрудника - показывать колонку с отделом сотрудника
Показывать Объект - показывать колонку с названием объекта
Показывать Контроллер - показывать колонку с названием контроллера
Сброс места нахождения сотрудника в конце дня - в списке сотрудников показывать индикатор положения сотрудника только за текущий день, если сотрудник не входил ни на один объект в текущие сутки, то индикатор ничего не показывает. Если галочка не установлена, то показывается положение сотрудника по последнему входу без ограничения срока (например, он мог войти на объект 2 дня назад).
Таблицы без прокрутки - при выводе табеля и отчета о приходах и уходах используется «широкий» формат отчета. Такой отчет выводится существенно быстрее и более удобен для больших отчетов.
Отнимать время обеда при расчете Общего времени - если для вывода табеля используется настройка «Общее Время», то от него будет отниматься время обеда сотрудника согласно расписанию его отдела.
Показывать нормативное время – показывать время, которое должен отработать сотрудник по норме.
Учитывать только подтвержденные проходы – показывать только проходы, подтвержденные датчиком двери или датчиком турникета.
Показывать переработку и недоработку в Табеле - в табеле кроме отработанного времени будет показываться сколько времени сотрудник переработал или недоработал согласно расписанию его отдела.
Время, показываемое в Табеле как отработанное за день - установить тип времени, показываемый в Табеле:

- **Общее время** - время между первым и последним проходом за день;
- **Чистое время** - сумма времени каждого посещения объектов (от входа до выхода на объект);
- **Рабочее время** - сумма времени посещения рабочих объектов (отмеченных как Рабочий объект в настройках доступа. Например, Офис может быть отмечен как Рабочий объект, а Коридор не отмечен как Рабочий объект).

Ключ доступа (для получения отчетов без логина) - автоматически генерируемый ключ, используемый при автоматическом получении отчетов по ссылке без логина.

Рекомендации по настойке отчетов

В зависимости от настройки отчеты могут показывать:

Чистое время. Это сумма всех промежутков времени присутствия сотрудника в помещении.

Присутствие сотрудника в помещении считается от события ВХОД до события ВЫХОД из помещения, при этом неважно, какую из карт или кодов сотрудник использует.
Не учитывается время, если сначала было событие ВЫХОД, а затем ВХОД.
Не учитывается время, если ВХОД был в одно помещение, а ВЫХОД из другого.
Не учитывается время, если вход был по карте, а выход по КНОПКЕ.
Для учета чистого времени нужно организовать четкое использование сотрудниками карт при каждом входе и выходе.
Если используются контроллеры с одним считывателем, направление прохода определить нельзя, и нужно устанавливать настройку контроллера «ОДИН СЧИТЫВАТЕЛЬ», чтобы система автоматически меняла направление прохода при каждом последующем проходе сотрудника.
Если такое четкое использование карт невозможно организовать, то можно считать ОБЩЕЕ ВРЕМЯ.
Если нужно учитывать время нахождения не во всех помещениях, то те помещения, в которых нужно учитывать время нужно указать как «РАБОЧЕЕ ПОМЕЩЕНИЕ», и установить расчет РАБОЧЕГО ВРЕМЕНИ.

Общее время. Это время между ПЕРВЫМ ВХОДОМ и ПОСЛЕДНИМ ВЫХОДОМ сотрудника в ЛЮБОЕ помещение за смену.

В случае, если направление прохода неважно, то можно использовать настройку «Общее время от любого первого события до любого последнего события». В этом случае будет считаться время между ПЕРВЫМ и ПОСЛЕДНИМ ПРОХОДАМИ (независимо от направления) сотрудника в ЛЮБОЕ помещение за смену.

Нормативное время. Это время, которое должен отработать сотрудник согласно графику работы отдела. Если расчетное время превышает нормативное, то показывается нормативное время, иначе - расчетное.

Для того, чтобы иметь некоторую гибкость в расчете нормативного времени, применяется установка «Считать ранний/поздний приход/уход нормой». Тогда если приход и уход сотрудника попадает в интервал ранний/поздний, то указывается нормативное время.

По умолчанию в табеле указываются только сотрудники, у которых есть хоть какие-то данные за месяц. Чтобы выводить ВСЕХ сотрудников, даже тех, кто не посещал помещения в течение месяца, применяется настройка «Показывать всех сотрудников».

По умолчанию данные удаленных сотрудников НЕ ПОКАЗЫВАЮТСЯ. Чтобы их увидеть, используется настройка «Показывать удаленных сотрудников».

Ключ доступа (для получения отчетов без логина)

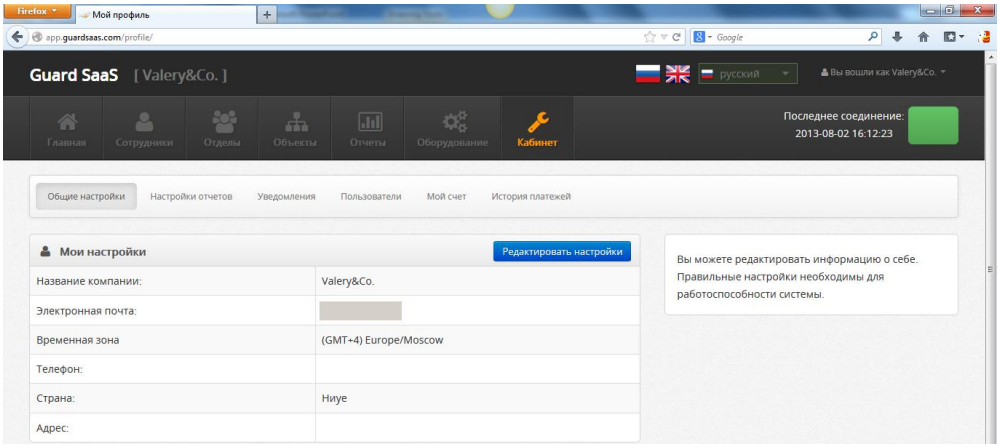
Для получения ключа доступа нужно перейти на вкладку «Кабинет» в раздел «Настройка отчетов». В разделе перейти к пункту «Ключ доступа (для получения отчетов без логина)» и кликнуть по кнопке «Сгенерировать новый ключ».



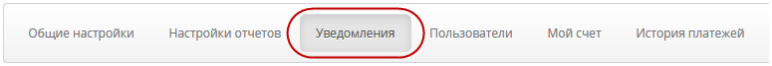
В окне появится сгенерированный ключ. Для сохранения настроек нужно кликнуть по кнопке «Сохранить».

Настройка уведомлений

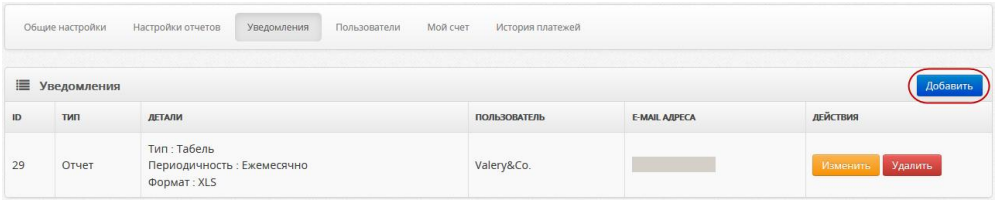
Уведомления - автоматические сообщения на электронную почту или по СМС на телефон о случившихся событиях. В уведомлении можно указать несколько адресов электронной почты или телефонов, разделив их запятой.
Уведомления настраиваются в подразделе «Уведомления». Для управления Уведомлениями, перейдите на вкладку «Кабинет».



Далее кликните раздел «Уведомления».

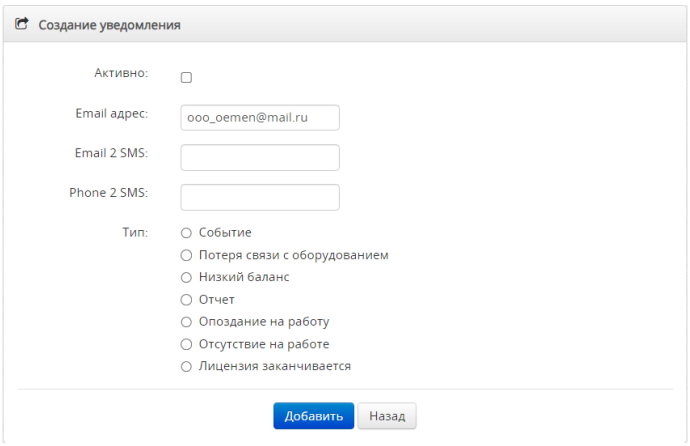


Вы можете создавать, удалять или редактировать уведомления.
Для добавления нового уведомления, кликните «Добавить».



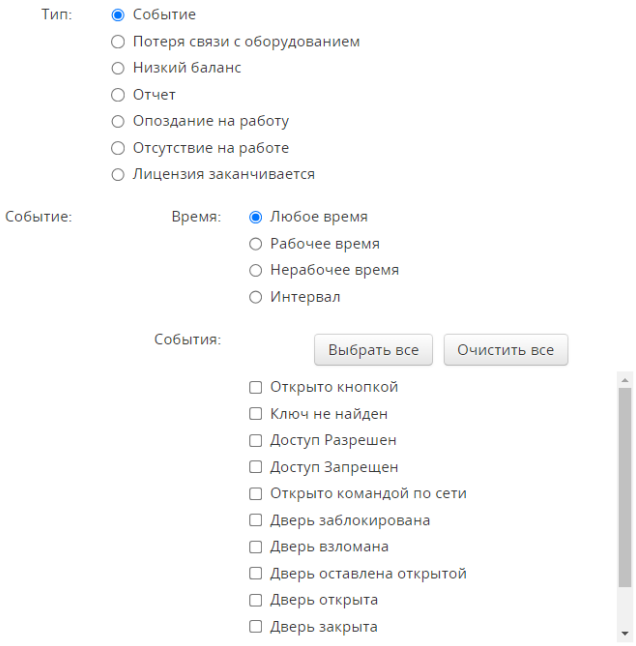
События для уведомлений можно выбирать по разным критериям.
Выберите тип уведомления:

- Событие;
- Потеря связи с оборудованием;
- Низкий баланс;
- Отчет;
- Опоздание на работу;
- Отсутствие на работе;
- Лицензия заканчивается.

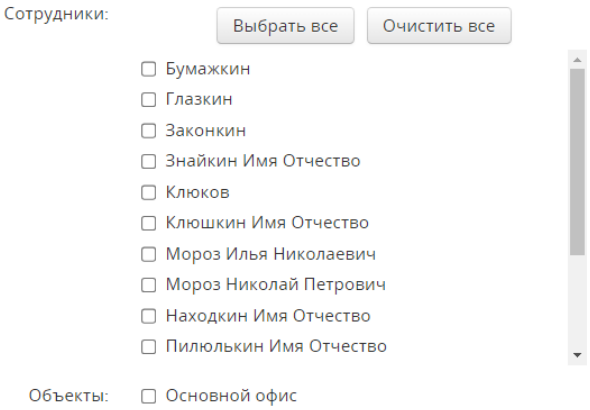


Тип «Событие» – используется для уведомления о конкретном совершенном событии. Выберите одно или несколько событий, конкретных сотрудников, объекты. Если не выбраны

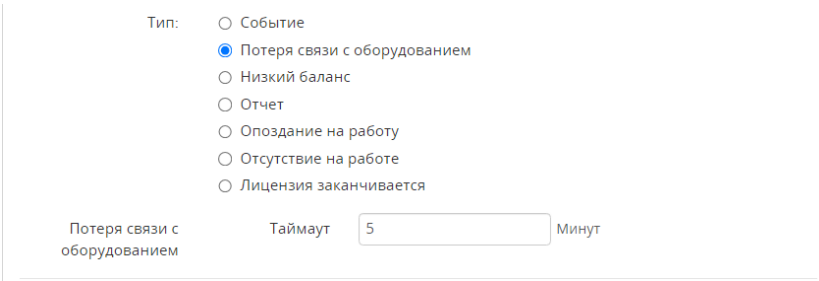
никакие опции, придет полный отчет: по всем событиям, сотрудникам, объектам. События могут отфильтровываться по времени, сотруднику, объекту.



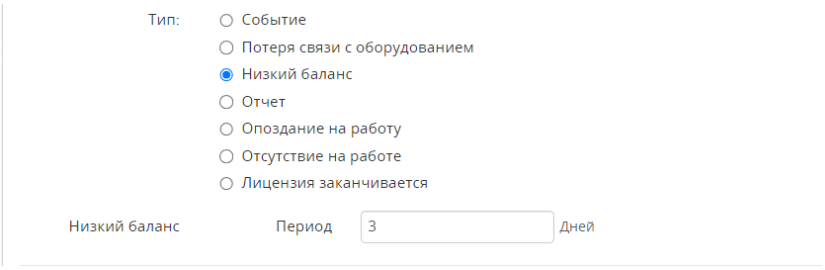
События можно фильтровать по сотрудникам и объектам.



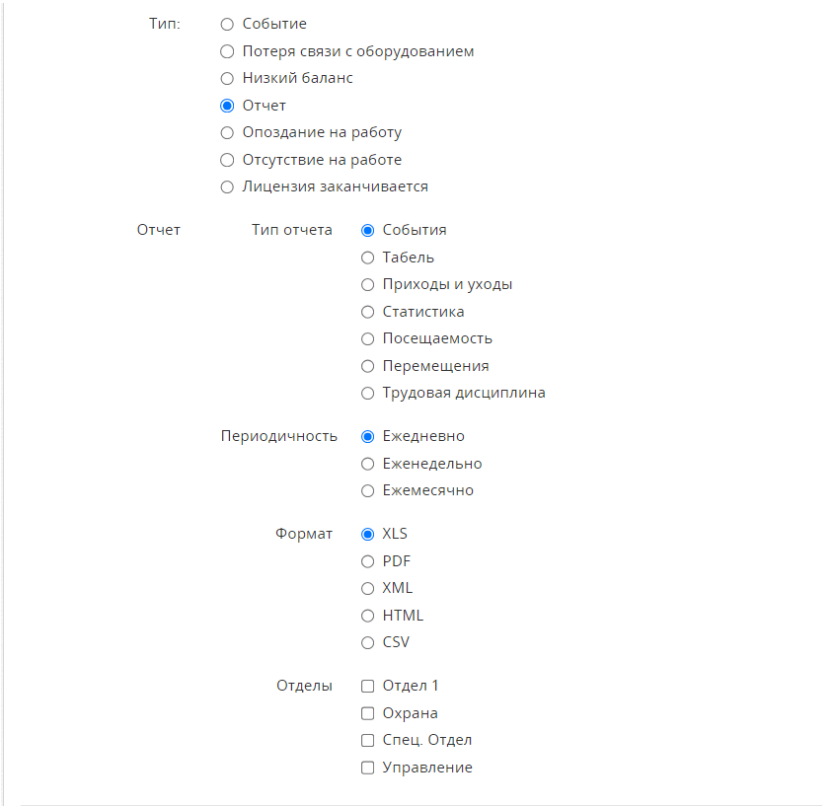
Тип «Потеря связи с оборудованием» – используется для уведомления о том, что связь с оборудованием потеряна. Через определенные промежутки времени осуществляется обмен информацией с оборудованием. Если ответ не получен, связь с оборудованием считается потерянной. В поле «Таймаут» укажите количество минут, после истечения которых связь считается потерянной. Если Таймаут=0, то придет уведомление сразу после того, как с оборудованием была потеряна связь. Значение по умолчанию – 5 минут.



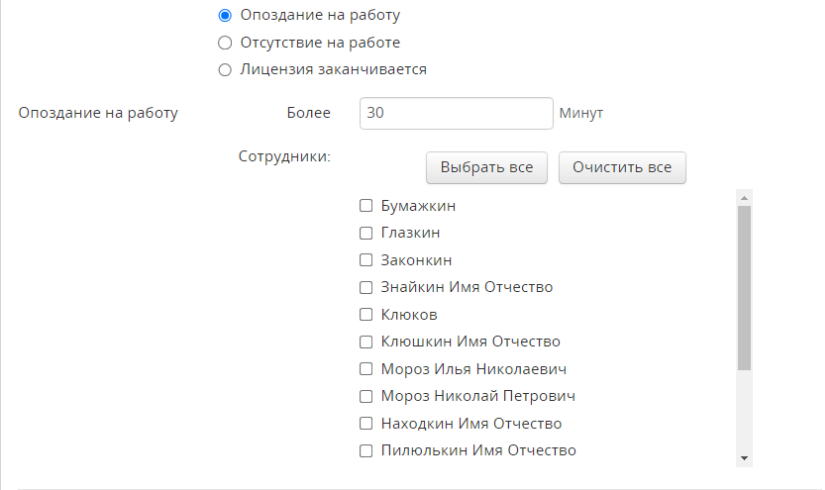
Тип «Низкий баланс» – используется для уведомления о том, что скоро закончатся средства на Вашем счете, и после этого функциональность будет ограничена. Средства списываются со счета в конце каждого дня равными частями. В поле «Период» укажите, за сколько дней предупреждать Вас об окончании средств. Если Период=0, то уведомление придет сразу на следующий день. Значение по умолчанию - 3 дня.



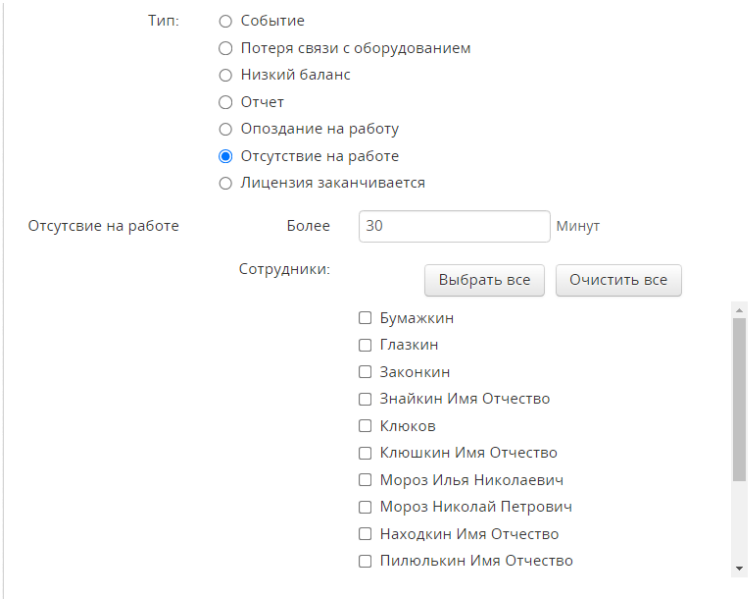
Тип «Отчет» – используется для отсылки определенного отчета. Выберите тип отчета, периодичность, формат отчета.



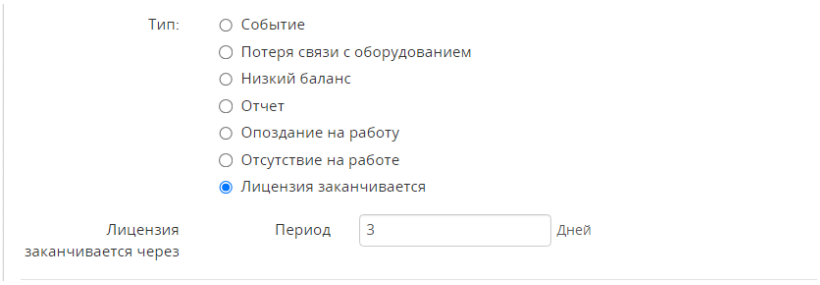
Тип «Опоздание на работу» – используется для уведомления об опоздании сотрудника на работу.



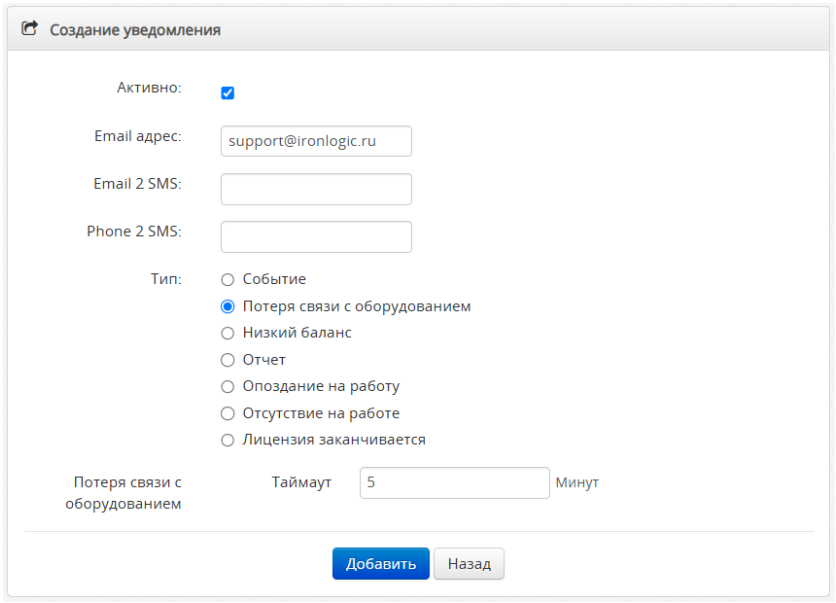
Тип «Отсутствие на работе» – используется для уведомления об отсутствии сотрудника на работе свыше трех часов.



Тип «Лицензия заканчивается» – используется для уведомления о приближении окончания времени действия лицензии.



После всех настроек уведомления его нужно активировать, поставив флаг в чекбоксе «Активно».



После того, как вы настроили и активировали уведомление, нажмите кнопку «Добавить».



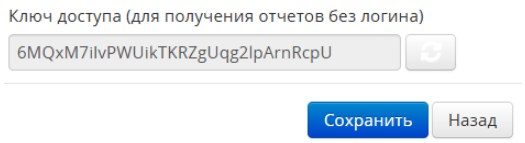
Получение отчета по http запросу

Иногда удобно автоматизировать получение отчетов из командной строки или из браузера по http запросу. Такая возможность реализована в GuardSaaS.

Формат запроса такой:
CODE: SELECT ALL

```
https://app.guardsaas.ru/reports/export/{REPORT}/{FORMAT}?{PARAMETERS}&appkey=utPZHIuIv4WO4ia3K5s0VpglO9ityDwA
```

appkey – Автоматически генерируемый ключ, используемый при автоматическом получении отчетов по ссылке без логина. Ключ доступа генерируется на вкладке «Кабинет» в разделе «Настройка отчетов». В разделе перейти к пункту «Ключ доступа (для получения отчетов без логина)» и скопировать сгенерированный ключ.



Далее это ключ вставляется в http-запрос как appkey.

Возможные значения:
{REPORT}
- events – События
- timesheet – Табель
- inout – Входы и Выходы
- discipline – Дисциплина
- statistics – Статистика
- attendance – Посещаемость
- movement – Перемещения

{FORMAT}
- csv – текстовый, через запятую
- xls – Excel
- html – HTML
- xml – XML
- pdf – PDF

{PARAMETERS}
dateFrom=YYYY-MM-DD – дата начала отчета, месяц отчета
dateTo=YYYY-MM-DD – дата конца отчета (если нужна)

Примеры:

CODE: SELECT ALL

```
Список событий
http://app.guardsaas.ru/reports/export/events/xls?dateFrom=2016-12-05&dateTo=2016-12-06&appkey=utPZHIuIv4WO4ia3K2u0VpglO9ityDwA

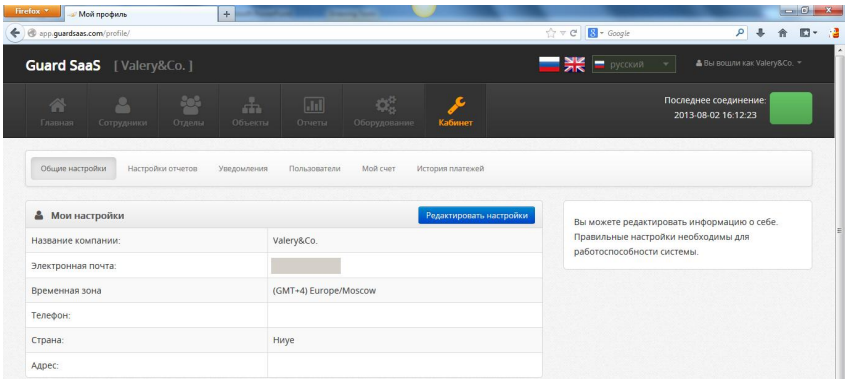
Табель
http://app.guardsaas.ru/reports/export/timesheet/html?dateFrom=2016-09-01&appkey=utPZHIuIv4WO4ia3K2u0VpglO9ityDwA

Дисциплина
http://app.guardsaas.ru/reports/export/discipline/pdf?appkey=utPZHIuIv4WO4ia3K2u0VpglO9ityDwA
```

Пользователи

Добавление пользователей системы

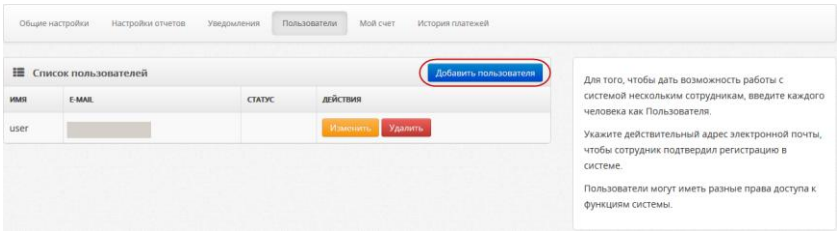
Для управления Пользователями, перейдите на вкладку «Кабинет». Управление пользователями и их правами осуществляется в разделе «Пользователи».



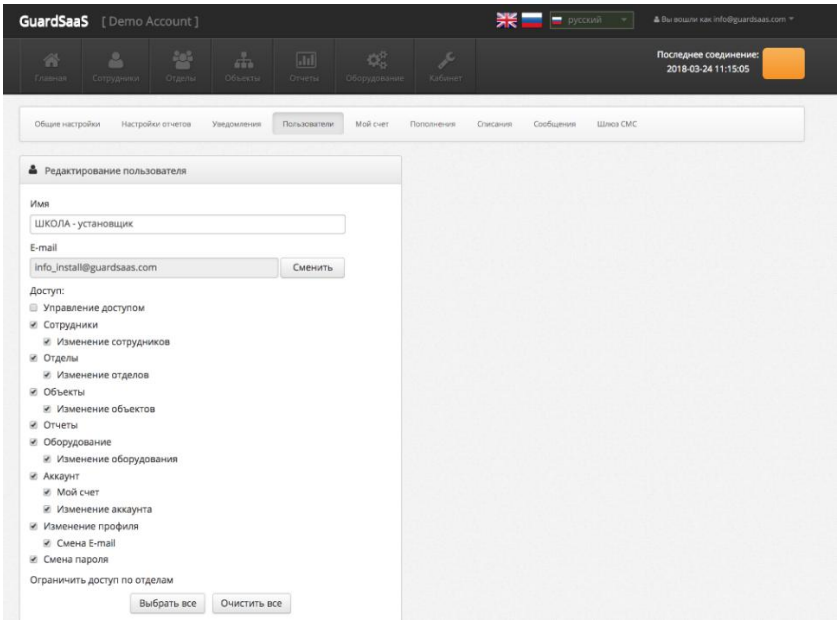
Далее кликните «Пользователи».



Для того, чтобы дать возможность работы с системой нескольким сотрудникам, добавьте каждого человека как Пользователя.
Вы можете создавать, удалять или редактировать пользователей.
Для добавления нового пользователя, кликните «Добавить пользователя».

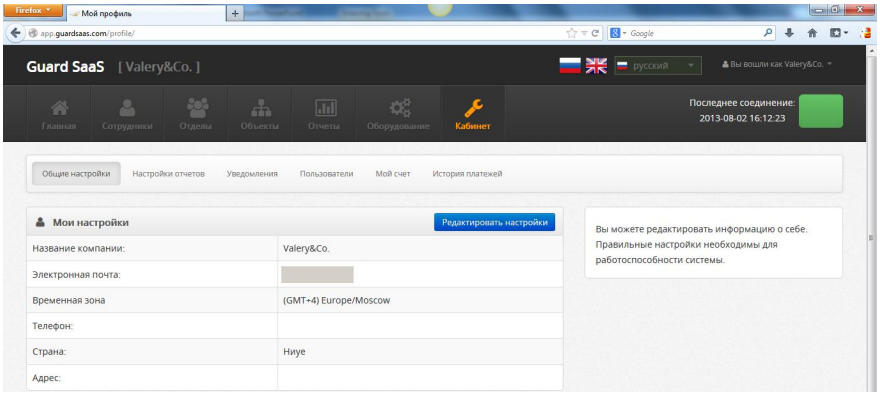


Укажите имя пользователя, действительный адрес электронной почты, пароль для входа. Нажмите «Добавить».
Для регистрации в системе на указанный адрес электронной почты придет письмо со ссылкой. Нажав на нее, пользователь подтвердит свою регистрацию и автоматически войдет в систему.
После создания пользователя, нажав на кнопку «Изменить» в списке пользователей, задайте права на доступ и изменение. Нажмите «Сохранить».
Каждому пользователю можно задать права доступа к функциональным областям GuardSaaS.

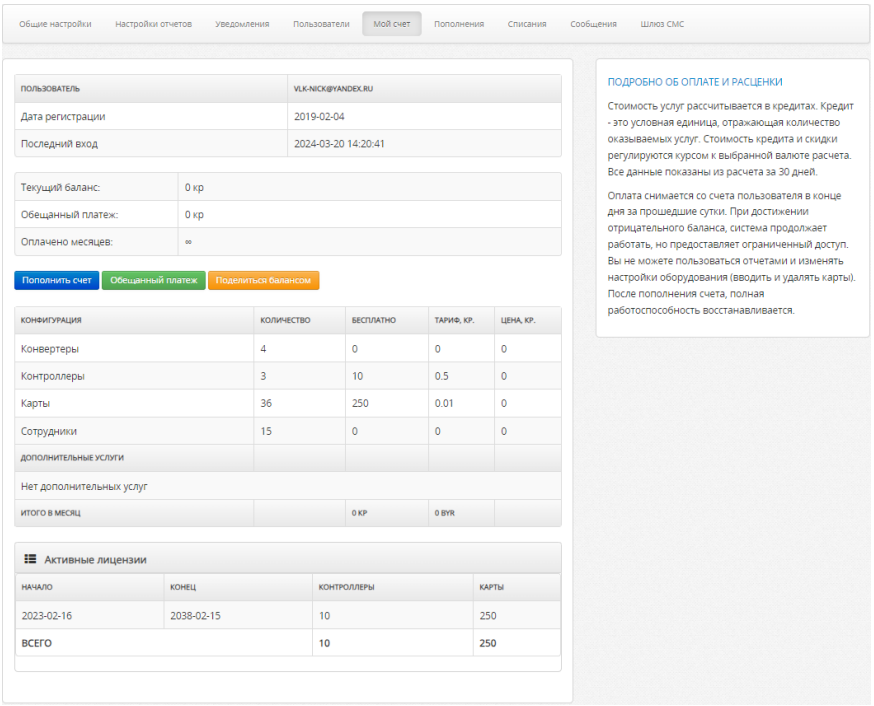


Мой счёт

В подразделе «Мой Счет» можно видеть текущее состояние аккаунта, его размер, текущий баланс. Чтобы пополнить счет или узнать его состояние, перейдите на вкладку «Кабинет».



Далее кликните на разделе «Мой счет».



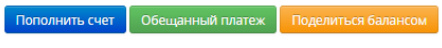
Здесь представлена следующая информация:

- **Информация о пользователе** – дата регистрации, время последнего входа;
- **Текущий баланс** – обещанный платеж, оплачено месяцев;
- **Конфигурация** – количество оборудования, тарифы, рассчитанная стоимость;
- **Дополнительные услуги** – количество зарегистрированных пользователей, стоимость;
- **Итого в месяц** – общая рассчитанная стоимость в месяц;
- **Активные лицензии** – действующие лицензии.

Стоимость услуг рассчитывается в кредитах. Кредит — это условная единица, отражающая количество оказываемых услуг. Стоимость кредита и скидки регулируются количеством выбранных для покупки кредитов. Все данные показаны из расчета за месяц.

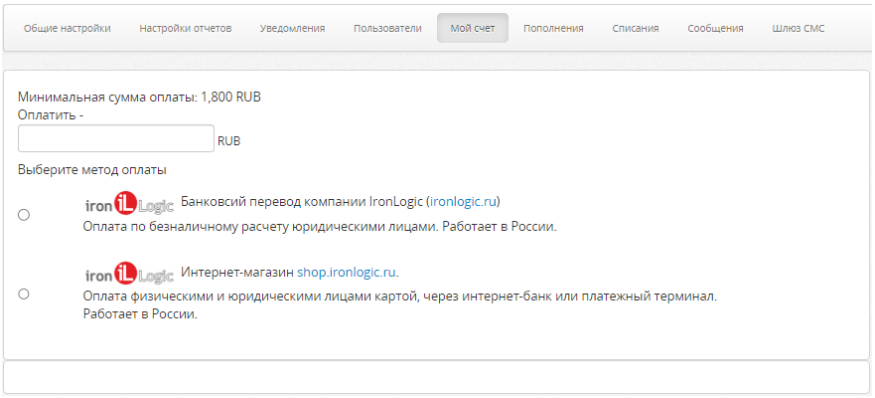
Оплата снимается со счета пользователя в конце дня за прошедшие сутки. При достижении отрицательного баланса, система продолжает работать, но предоставляет ограниченный доступ. Вы не можете пользоваться отчетами и изменять настройки оборудования (вводить и удалять карты). После пополнения счета, полная работоспособность восстанавливается.

Для пополнения счета можно перейти по кнопкам «Пополнить счет» или «Обещанный платеж». Для того, чтобы поделиться балансом нужно перейти по кнопке «Поделиться балансом».

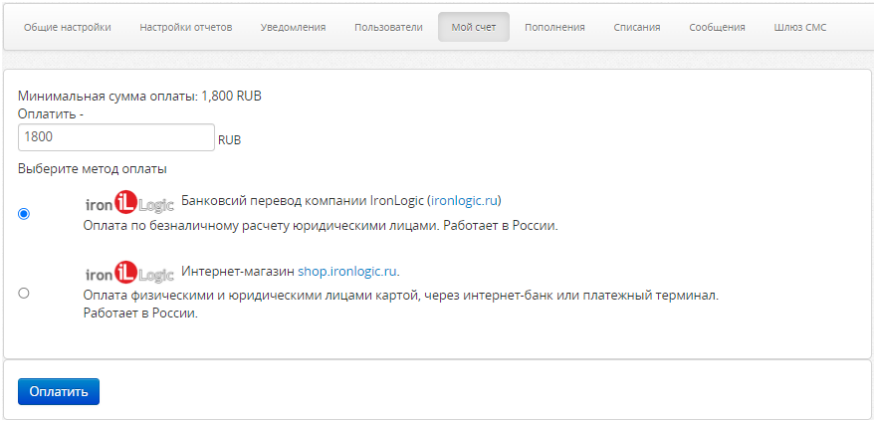


Пополнить счёт

Чтобы пополнить счет, нажмите кнопку «Пополнить счет».



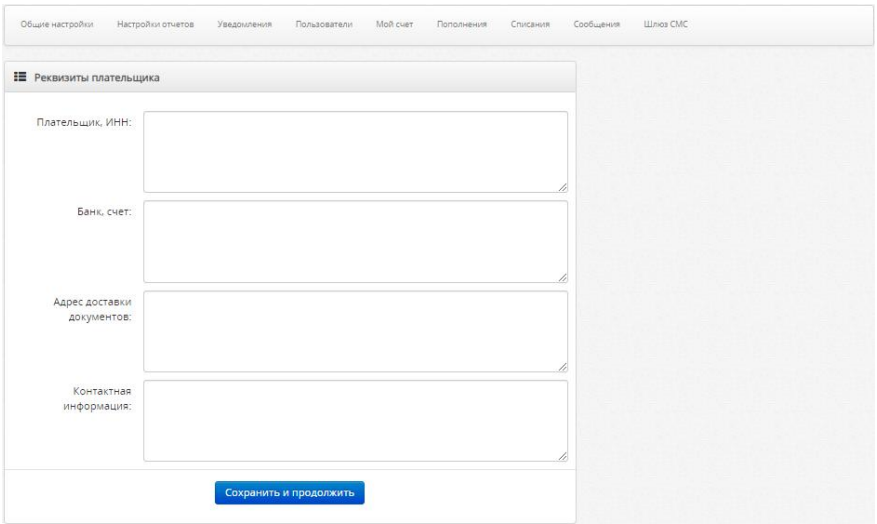
Если Вы юридическое лицо, выберите метод оплаты для юридического лица и укажите сумму. Нажмите кнопку «Оплатить».



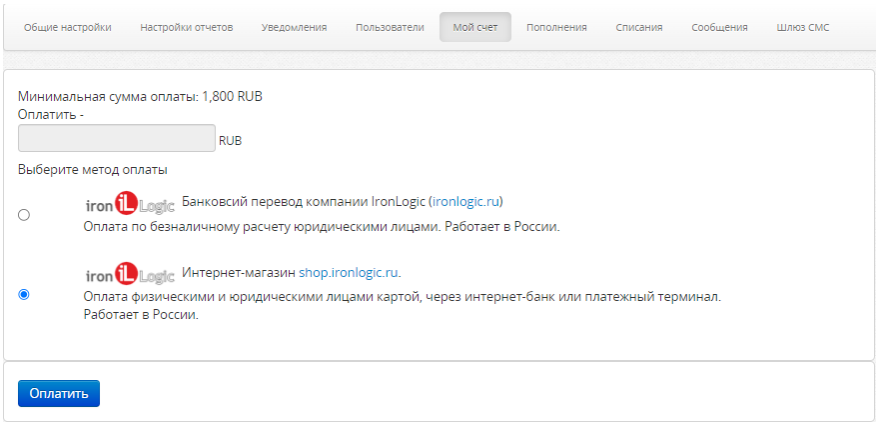
Откроется окно «Реквизиты плательщика». Заполните свои реквизиты.
Юридическому лицу необходимо заполнить:

- **Плательщик –** название компании, ИНН;
- **Банк –** название банка, БИК, кор. счет, расчетный счет;
- **Адрес доставки документов**;
- **Контактная информация –** электронная почта, телефон.

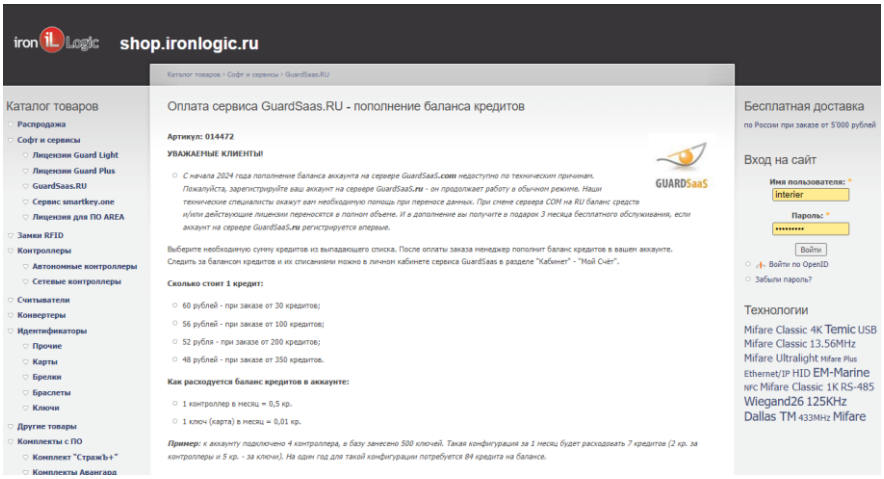
Затем нажмите кнопку «Сохранить и продолжить».



Если Вы физическое или юридическое лицо, и оплата будет производиться картой, выберите метод оплаты «Оплата физическими или юридическими лицами картой…». Нажмите кнопку «Оплатить».

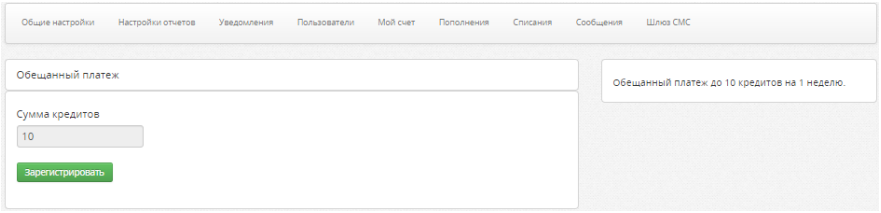


В открывшемся окне Интернет-магазина зайдите в свою учетную запись и выберите нужную лицензию.

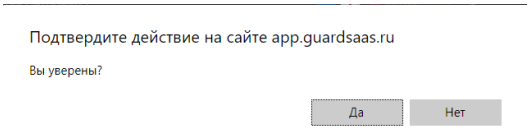


Обещанный платёж

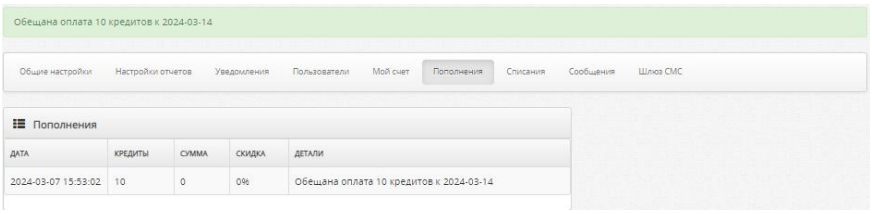
Для запроса обещанного платежа нажмите кнопку «Обещанный платеж».



Появится окно подтверждения, в котором нужно нажать кнопку «Да».

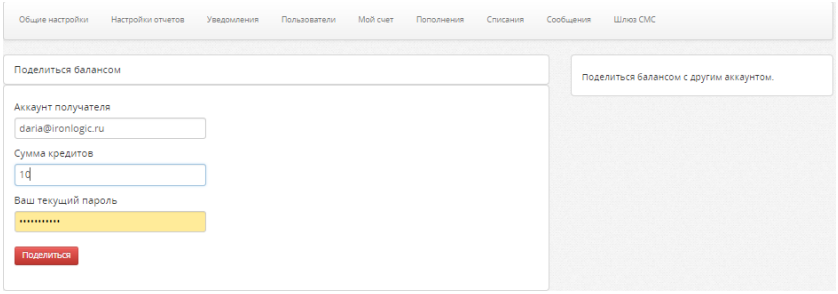


Откроется подраздел «Пополнения» с записью Ваших пополнений.

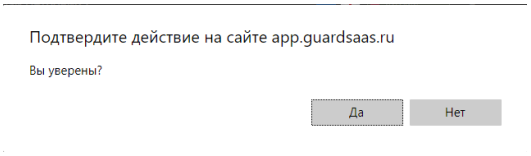


Поделиться балансом

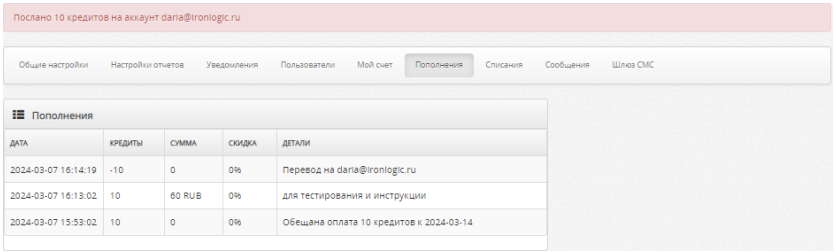
При необходимости поделиться балансом с другим аккаунтом нажмите кнопку «Поделиться балансом». Откроется окно «Поделиться балансом», в котором нужно внести имя аккаунта получателя (электронную почту), сумму кредитов, текущий пароль аккаунта, с которого переводится баланс.



Появится окно подтверждения, в котором нужно нажать кнопку «Да».

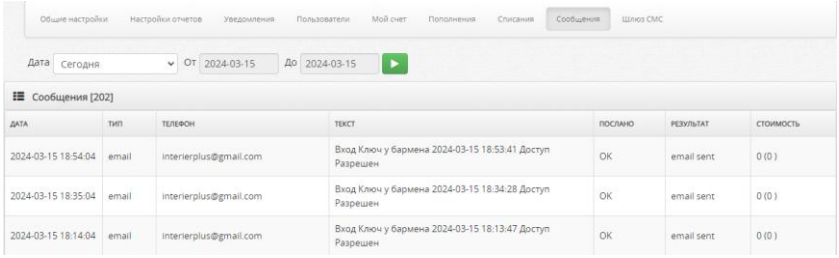


Откроется подраздел «Пополнения» с записью «Перевод на …».



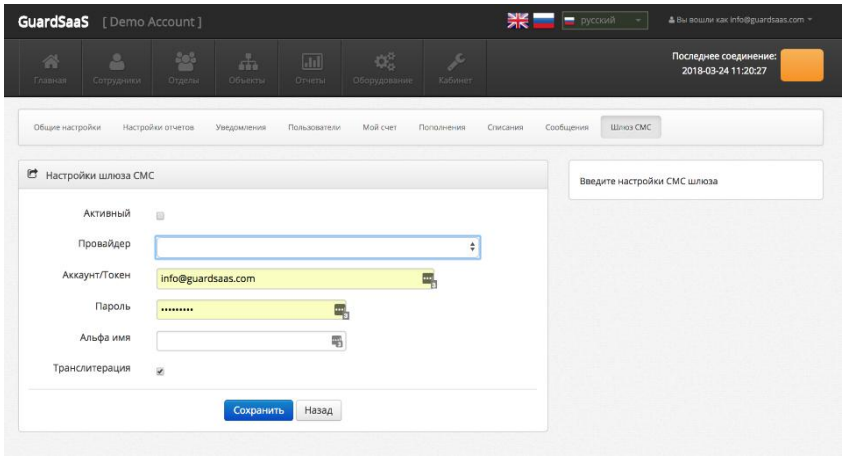
Сообщения

В подразделе «Сообщения» можно видеть список отосланных на email уведомлений.



Шлюз СМС

Для настройки шлюза СМС используется подраздел «Шлюз СМС».



Здесь вводится провайдер, имя аккаунта, пароль и др. Для включения шлюза нужно поставить флаг на чек-боксе «Активный». Пользователь может использовать уведомления по email и попробовать подключить опцию email2sms своего мобильного оператора.
Кроме этого, СМС отправляется не сотруднику, а на email администратора системы.

На данный момент система поддерживает ограниченный список шлюзов для отсылки СМС. GuardSaaS может отсылать уведомления о событиях также в виде СМС прямо на Ваш телефон. Настроить это можно двумя способами:
1) Используя СМС шлюз Вашего мобильного оператора.
2) Через шлюзы провайдеров, к которым подключен GuardSaaS, при этом есть шлюзы, которые могут использовать Ваш мобильный телефон для отправки сообщений.

СМС через шлюз Вашего мобильного оператора

Многие мобильные операторы во всем мире предоставляют своим клиентам услугу СМС шлюза с использованием адреса электронной почты. При подключении этой услуги (примерное название «email на SMS») Вашему телефону присваивается адрес электронной почты. Сообщения, которые посланы на этот адрес приходят на Ваш телефон в виде СМС. Вы указываете этот адрес в поле «Email 2 SMS» GuardSaaS, и наша система будет посылать на него специально отформатированные уведомления.
При этом Вы оплачиваете эту услугу только Вашему мобильному оператору.

Использование СМС шлюза с собственным логином

Если Вы уже имеете регистрацию на одном из распространенных СМС шлюзов (sms.ru, smsc.ru, sms-fly.com, htmlweb.ru) и желаете использовать его для рассылки своих СМС из GuardSaaS, Вы оплачиваете услуги по рассылке СМС непосредственно шлюзу. GuarSaaS не берет оплату за такие СМС.
Чтобы подключить свой аккаунт для использования собственного СМС шлюза, пришлите запрос на электронную почту support@ironlogic.ru

Шлюз htmlweb.ru может использовать ВАШ смартфон для отсылки СМС сообщений.

Прямые СМС

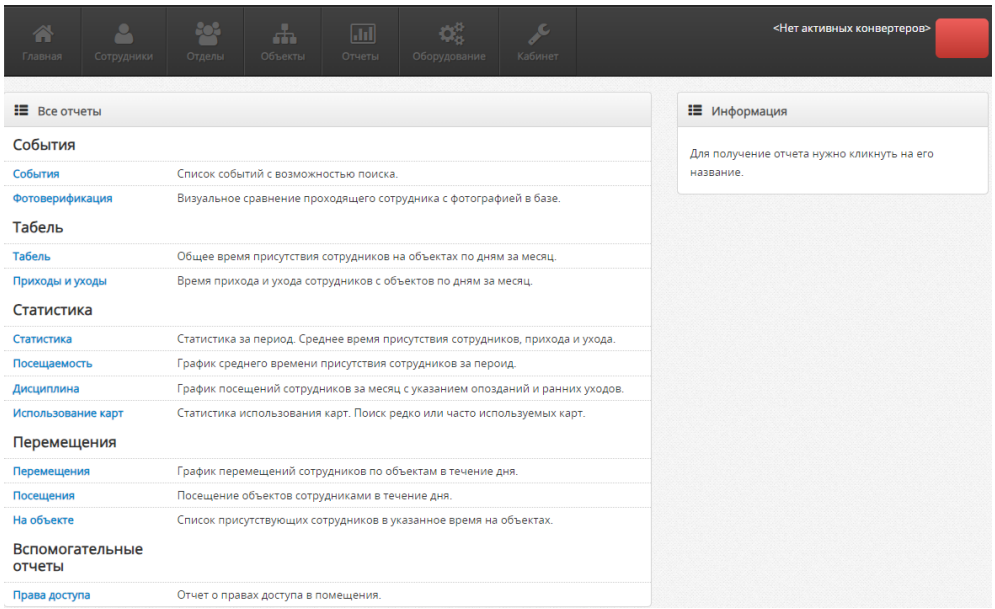
Этот вариант больше не поддерживается.

Списание оплаты за СМС и возврат денег

Технология доставки СМС не является гарантированной, поэтому сообщение в некоторых случаях может не дойти, хотя деньги списаны. GuardSaaS НЕ ВОЗВРАЩАЕТ денег на баланс аккаунта, кроме случаев, связанных с ошибкой работы самого GuardSaaS.
Если СМС шлюз списал деньги за отсылку сообщения, то GuardSaaS не будет принимать претензии по их возврату. Учитывайте это, пожалуйста, при использовании данной услуги.

Вкладка «Отчёты»

Для получения полезной информации в отчетах GuardSaaS необходимо их настроить в соответствии со спецификой используемой конфигурации оборудования и правил посещения. Для работы с отчетами перейдите на вкладку «Отчеты».



Доступны следующие виды отчетов:

- **События** – Список событий с возможностью поиска.
- **Фотоверификация** – Визуальное сравнение проходящего сотрудника с фотографией в базе.
- **Табель** – Общее время присутствия сотрудников на объектах по дням за месяц.
- **Приходы и уходы** – Время прихода и ухода сотрудников с объектов по дням за месяц.
- **Статистика** – Статистика за период. Среднее время присутствия сотрудников, прихода и ухода.
- **Посещаемость** – График среднего времени присутствия сотрудников за период.
- **Дисциплина** – График посещений сотрудников за месяц с указанием опозданий и ранних уходов.
- **Использование карт** – Статистика использования карт. Поиск редко или часто используемых карт.
- **Перемещения** – График перемещений сотрудников по объектам в течение дня.
- **Посещения** – Посещение объектов сотрудниками в течение дня.
- **На объекте** – Список присутствующих сотрудников в указанное время на объектах.
- **Права доступа** – Отчет о правах доступа в помещения.

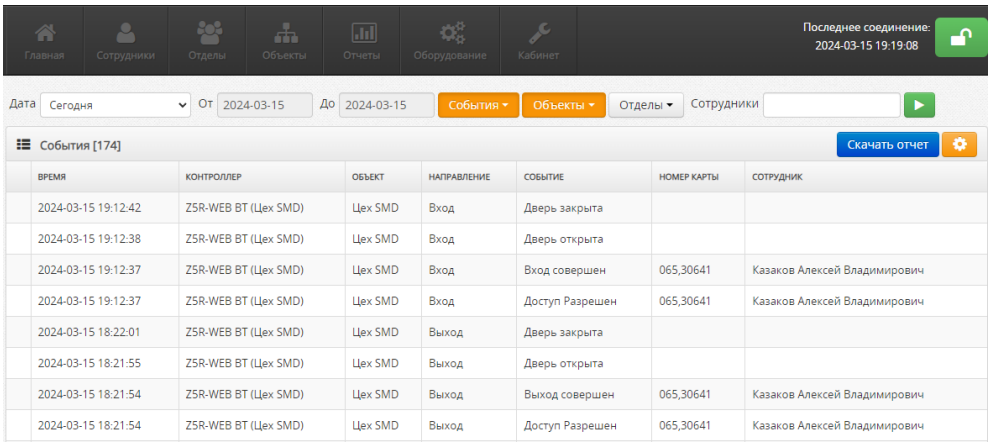
Для всех отчетов возможно:

- Устанавливать конкретную дату, период для фильтрации;
- Скачивать файл в форматах **xls, xml, html, pdf, csv;**
- Выслать системой по электронной почте.

События

Отчёт «События»

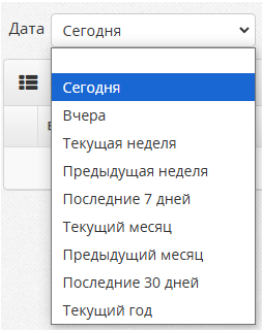
Отчёт «События» представляет следующие данные: время, контроллер, объект, направление, событие, номер карты, сотрудник.



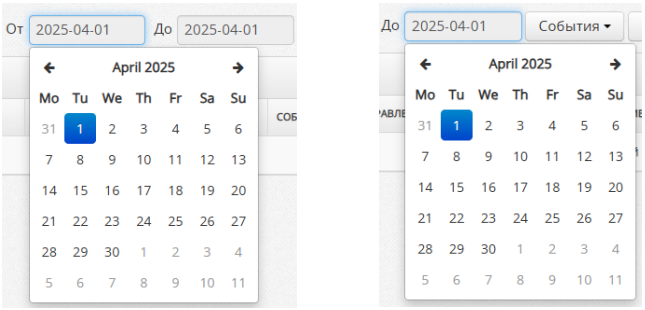
ВРЕМЯ	КОНТРОЛЛЕР	ОБЪЕКТ	НАПРАВЛЕНИЕ	СОБЫТИЕ	НОМЕР КАРТЫ	СОТРУДНИК
2024-03-15 19:12:42	Z5R-WEB BT (Цех SMD)	Цех SMD	Вход	Дверь закрыта		
2024-03-15 19:12:38	Z5R-WEB BT (Цех SMD)	Цех SMD	Вход	Дверь открыта		
2024-03-15 19:12:37	Z5R-WEB BT (Цех SMD)	Цех SMD	Вход	Вход совершен	065,30641	Казаков Алексей Владимирович
2024-03-15 19:12:37	Z5R-WEB BT (Цех SMD)	Цех SMD	Вход	Доступ Разрешен	065,30641	Казаков Алексей Владимирович
2024-03-15 18:22:01	Z5R-WEB BT (Цех SMD)	Цех SMD	Выход	Дверь закрыта		
2024-03-15 18:21:55	Z5R-WEB BT (Цех SMD)	Цех SMD	Выход	Дверь открыта		
2024-03-15 18:21:54	Z5R-WEB BT (Цех SMD)	Цех SMD	Выход	Выход совершен	065,30641	Казаков Алексей Владимирович
2024-03-15 18:21:54	Z5R-WEB BT (Цех SMD)	Цех SMD	Выход	Доступ Разрешен	065,30641	Казаков Алексей Владимирович

Используйте фильтрацию событий следующим образом:

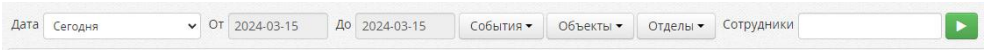
1) выберите дату из выпадающего меню;



2) выберите любую дату в календаре, кликнув левой кнопкой мыши на окне календаря (внешне окно серое и видится, как неактивное);



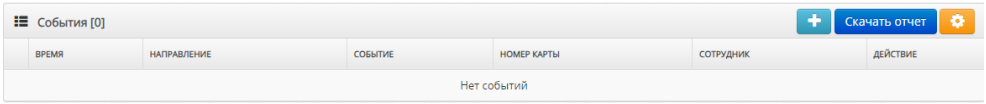
3) выберите конкретное событие.



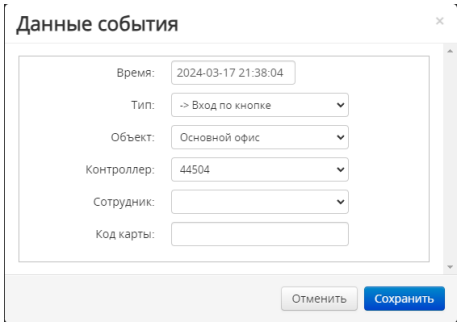
Нажмите кнопку «Применить».

Добавление события вручную

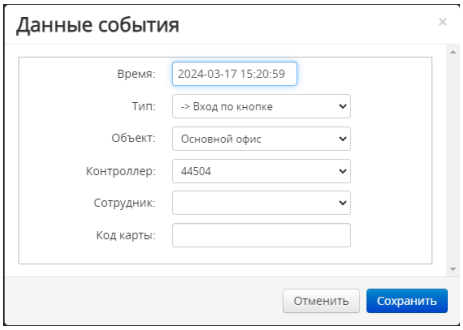
В систему добавлена возможность редактирования и добавления события в отчете «События». После установки флага «Редактирование событий:» в «Кабинете»/«Общие настройки» на панели дополнительно появится кнопка «Добавить событие», слева от кнопки «Скачать отчет».



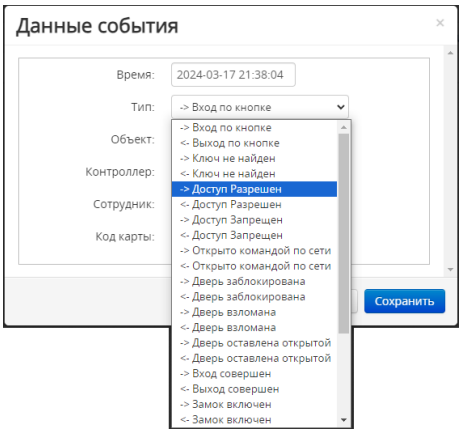
Кликните по кнопке «Добавить событие» и откроется окно «Данные события».

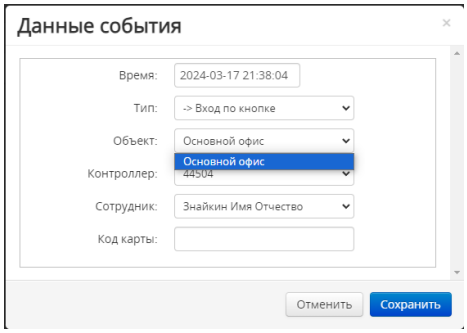


В этом окне можно указать: время события, тип, объект, контроллер, сотрудник, код карты.

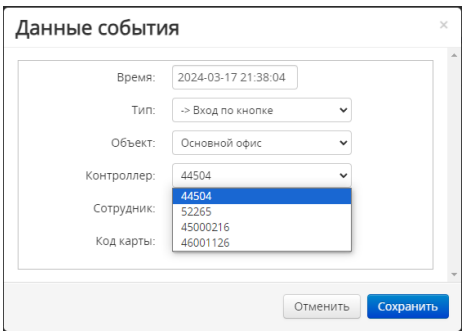


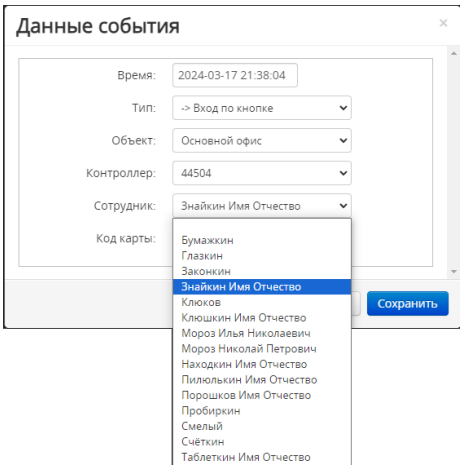
Выберите тип события из разворачивающегося списка.



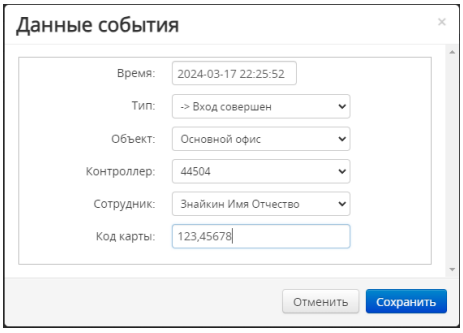


Укажите объект и контроллер для прохода.

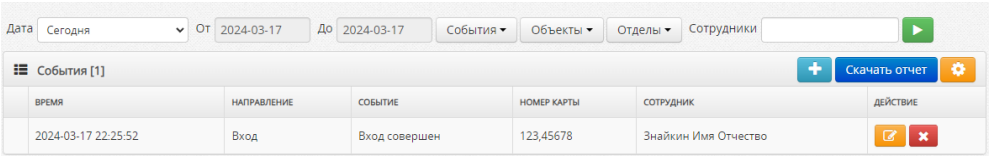




Укажите сотрудника и его карту.

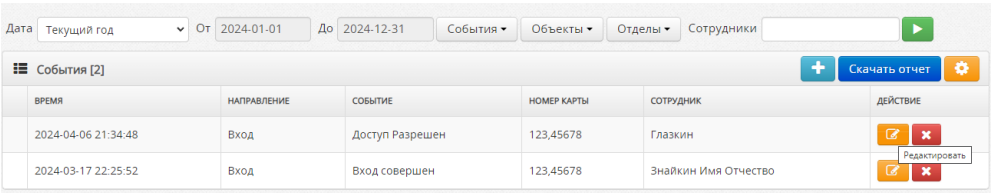


После ввода всех данных кликните по кнопке «Сохранить». В окне «События» появится введенное вручную событие.

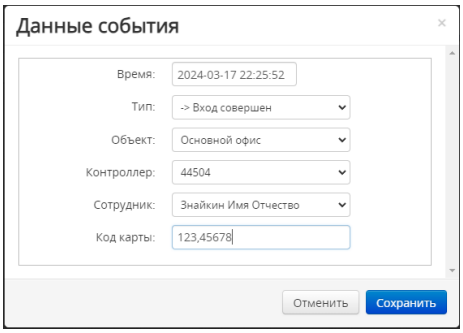


Редактирование событий

Добавленное или любое другое событие можно отредактировать, кликнув по кнопке «Редактировать» в строке выбранного события. Эта опция включается на вкладке «Кабинет» в «Общих настройках».



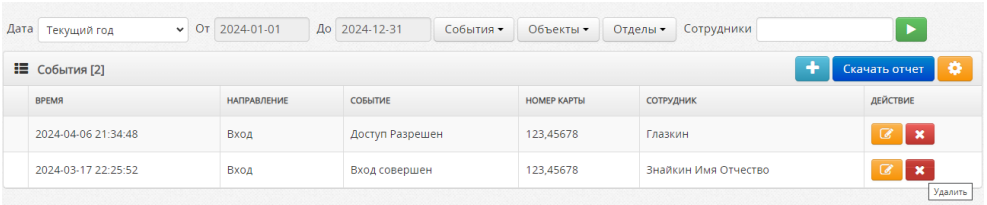
Откроется окно ввода «Данные события», в котором можно ввести откорректированные данные по событию.



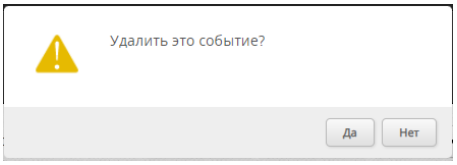
Введите корректировки и сохраните их, кликнув по кнопке «Сохранить».

Удаление событий

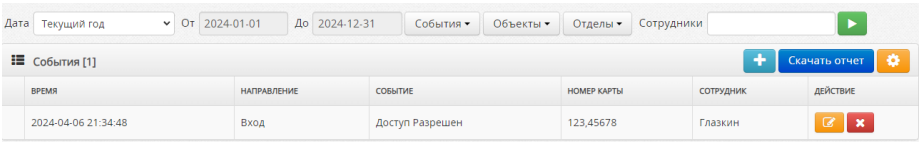
Любое событие можно удалить из отчета «События», кликнув по кнопке «Удалить» в строке выбранного события.



Появится окно предупреждения с вопросом «Удалить это событие?». Кликните по кнопке «Да» для подтверждения удаления события.

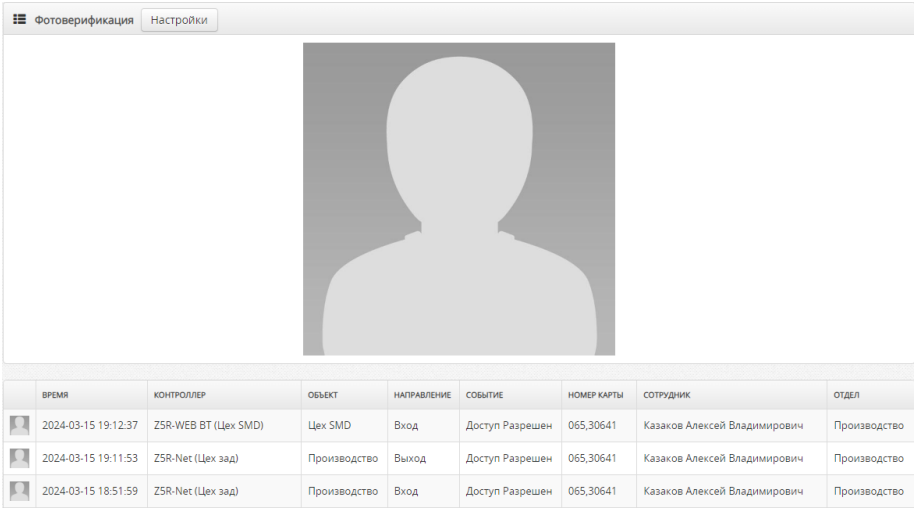


Выбранное событие будет удалено из отчета.

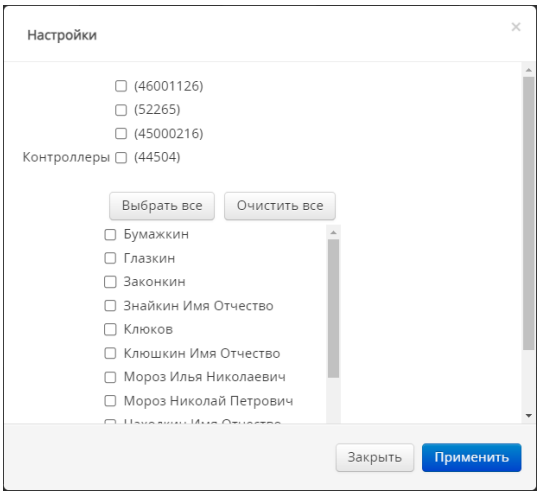


Отчёт «Фотоверификация»

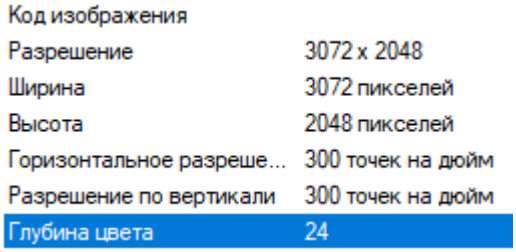
Фотоверификация – это визуальное сравнение проходящего сотрудника с фотографией в базе.



Если кликнуть по кнопке «Настройки» откроется окно, в котором выбираются контроллеры и сотрудники из списка.



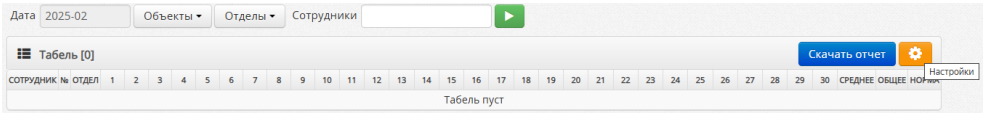
Размер фото не должен быть более 1,5 Мб, и параметры не выше, чем рекомендовано:

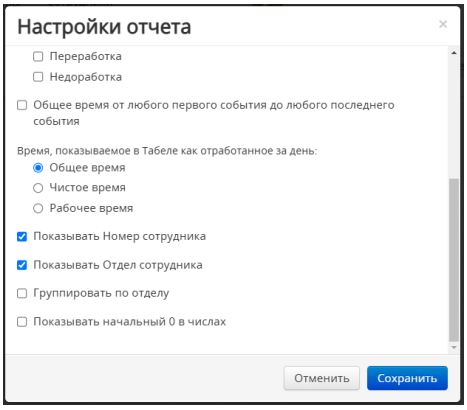


Табель

Отчёт «Табель»

Отчет «Табель» показывает общее время нахождения сотрудников в помещениях.





В зависимости от настройки отчеты могут показывать:

- **Чистое время.**

Это сумма всех промежутков времени присутствия сотрудника в помещении. Присутствие сотрудника в помещении считается от события ВХОД до события ВЫХОД в помещение, при этом неважно, какую из карт или кодов сотрудник использует.

- ***Не учитывается время, если сначала было событие ВЫХОД, а затем ВХОД***
- ***Не учитывается время, если ВХОД был в одно помещение, а ВЫХОД из другого***
- ***Не учитывается время, если вход был по карте, а выход по КНОПКЕ.***

Для учета чистого времени нужно организовать четкое использование сотрудниками карт при каждом входе и выходе.

Если используются контроллеры с одним считывателем, направление прохода определить нельзя, и нужно устанавливать настройку контроллера «ОДИН СЧИТЫВАТЕЛЬ», чтобы система автоматически меняла направление прохода при каждом последующем проходе сотрудника.

Если такое четкое использование карт невозможно организовать, то можно считать ОБЩЕЕ ВРЕМЯ.

Если нужно учитывать время нахождения не во всех помещениях, то те помещения, в которых нужно учитывать время нужно указать как «РАБОЧЕЕ ПОМЕЩЕНИЕ», и установить расчет РАБОЧЕГО ВРЕМЕНИ.

Для учёта сменной работы и перехода ночной смены на другие сутки, нужно установить расчет «Чистого времени». При этом смена, попадающая на разрыв месяца (дня) относится к суткам начала смены.

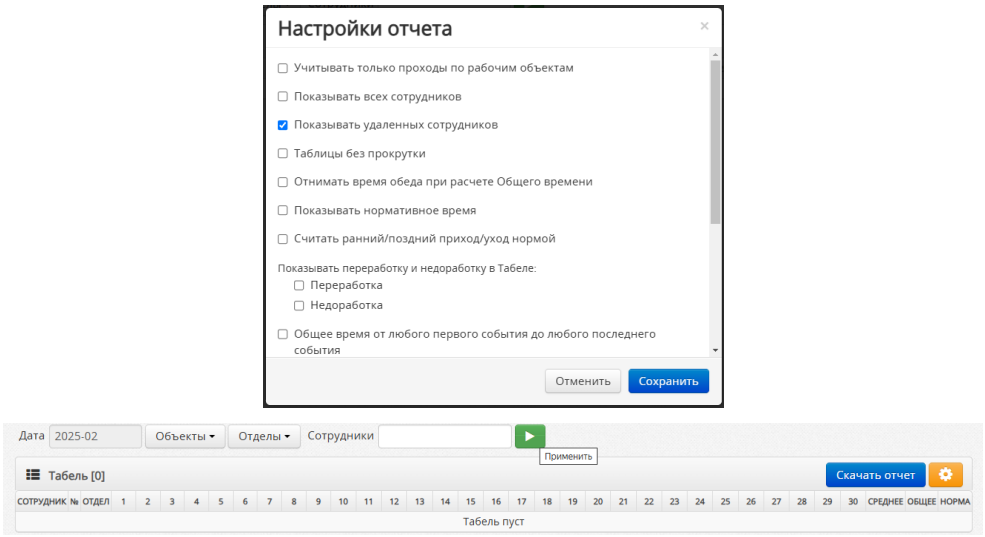
- **Общее время.**

Это время между ПЕРВЫМ ВХОДОМ и ПОСЛЕДНИМ ВЫХОДОМ сотрудника в ЛЮБОЕ помещение за смену. В случае, если направление прохода неважно, то можно использовать настройку «Общее время от любого первого события до любого последнего события». В этом случае будет считаться время между ПЕРВЫМ и ПОСЛЕДНИМ ПРОХОДАМИ (независимо от направления) сотрудника в ЛЮБОЕ помещение за смену.

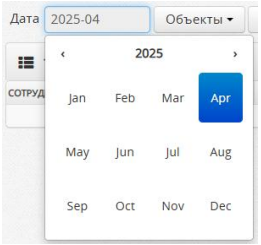
- **Нормативное время.**

Это время, которое должен отработать сотрудник согласно графику работы отдела. Если расчетное время превышает нормативное, то показывается нормативное время, иначе - расчетное. Для того, чтобы иметь некоторую гибкость в расчете нормативного времени,

применяется установка «Считать ранний/поздний приход/уход нормой». Тогда если приход и уход сотрудника попадает в интервал ранний/поздний, то указывается нормативное время.
По умолчанию в табеле указываются только сотрудники, у которых есть хоть какие-то данные за месяц. Чтобы выводить ВСЕХ сотрудников, даже тех, кто не посещал помещения в течение месяца, применяется настройка «Показывать всех сотрудников».
По умолчанию данные удаленных сотрудников НЕ ПОКАЗЫВАЮТСЯ. Чтобы их увидеть, используется настройка «Показывать удаленных сотрудников».

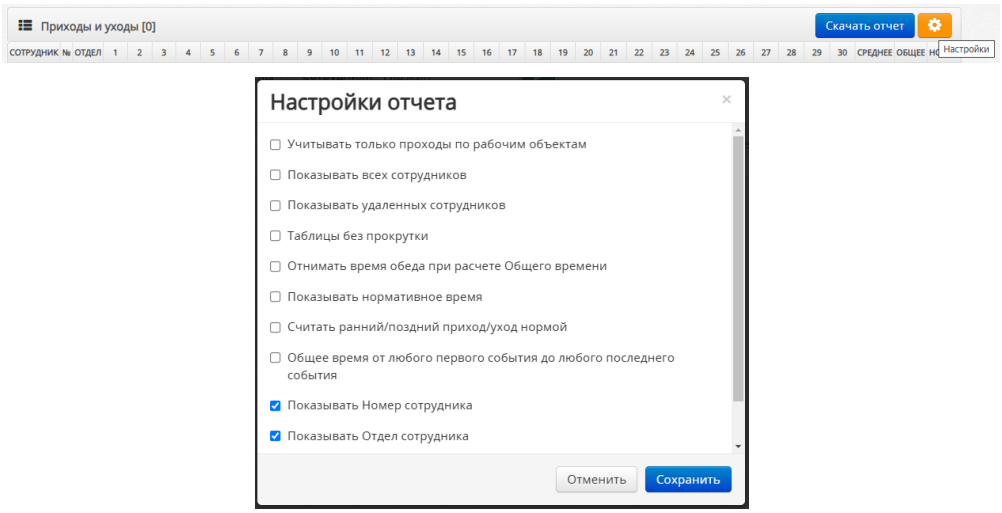


Для фильтрации табеля по дате выберите дату, кликнув левой кнопкой мыши на окне календаря (внешне окно серое и видится, как неактивное) и нажмите «Применить».

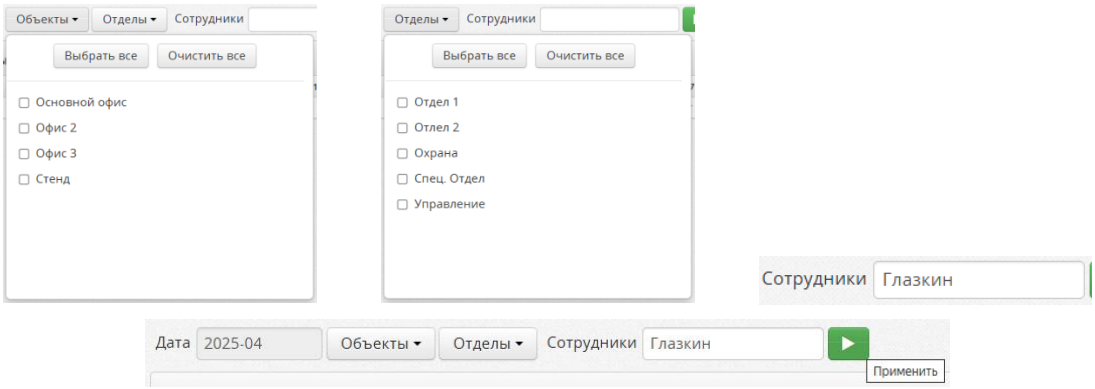


Отчёт «Приходы и уходы»

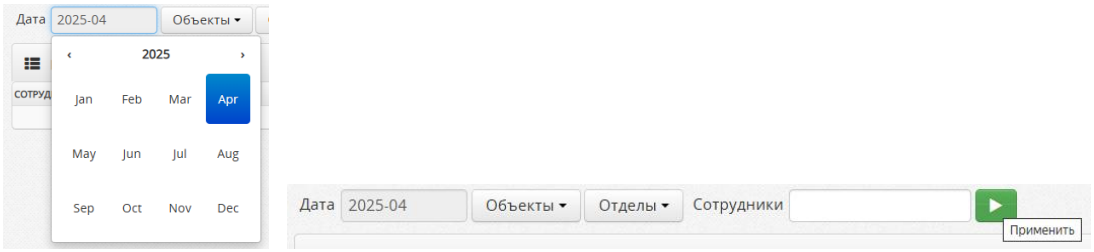
Отчет «Приходы и Уходы» – показывает время прихода и ухода соответственно.
В зависимости от настройки отчеты могут показывать:



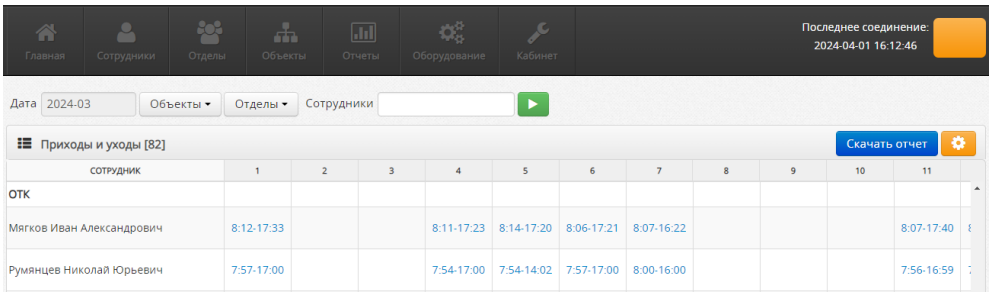
Для фильтрации по объекту, отделу или сотруднику выберите нужный объект, отдел или сотрудника и нажмите «Применить».



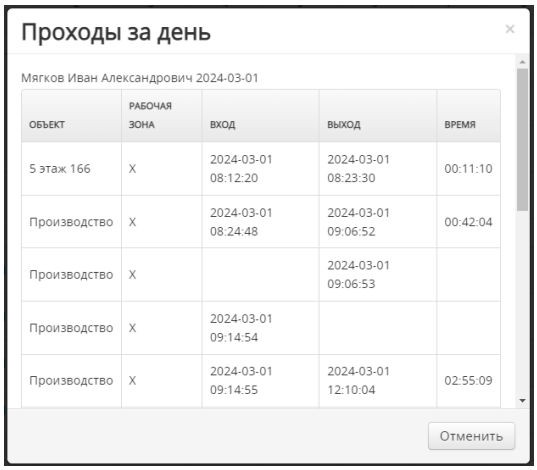
Для фильтрации отчета по дате кликните левой кнопкой мыши на окне календаря (внешне окно серое и видится, как неактивное) и нажмите «Применить».



В открывшемся отчете показано время прихода и ухода сотрудника за каждый день в течение месяца.



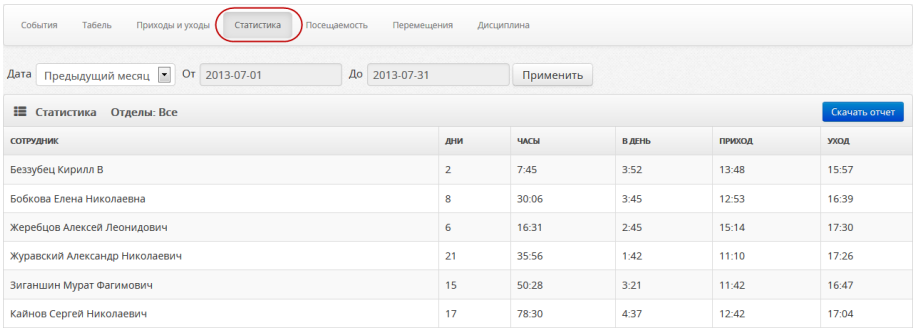
При необходимости просмотра всех приходов и уходов за день у конкретного сотрудника, нужно кликнуть по времени проходов за выбранный день. Откроется окно «Проходы за день», в котором подробно расписаны все перемещения сотрудника в течение дня.



Статистика

Отчёт «Статистика»

В отчете «Статистика» показывается Статистика за период. Среднее время присутствия сотрудников, прихода и ухода.

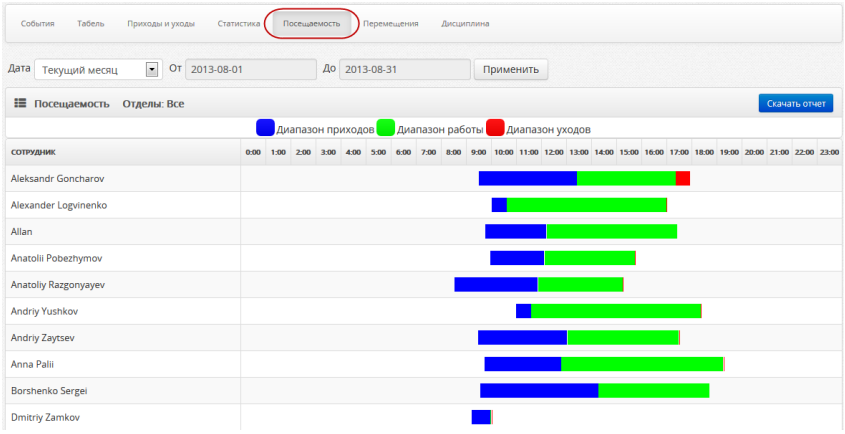


Для фильтрации выберите дату или период и нажмите «Применить».



Отчёт «Посещаемость»

В отчете «Посещаемость» показывается график среднего времени присутствия сотрудников за период.

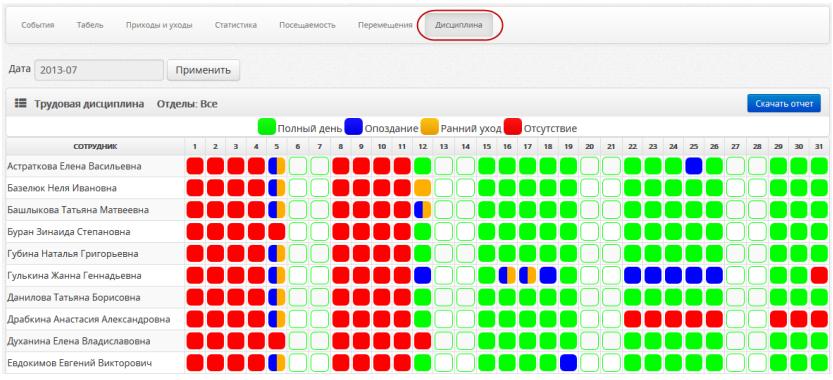


Для фильтрации выберите дату или период и нажмите «Применить».

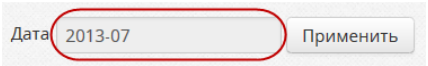


Отчёт «Дисциплина»

В отчете «Дисциплина» показывается график посещений сотрудников за месяц с указанием опозданий и ранних уходов.

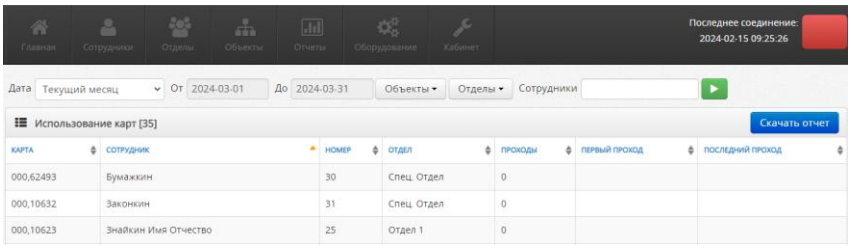


Для фильтрации выберите дату и нажмите «Применить».



Отчёт «Использование карт»

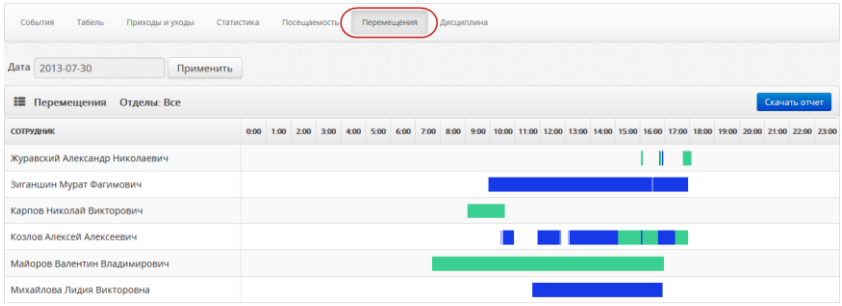
В отчете «Использование карт» показывается статистика использования карт. Поиск редко или часто используемых карт.



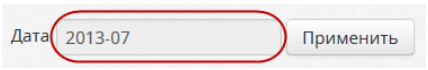
Перемещения

Отчёт «Перемещения»

В отчете «Перемещения» показывается график перемещений сотрудников по объектам в течение дня.

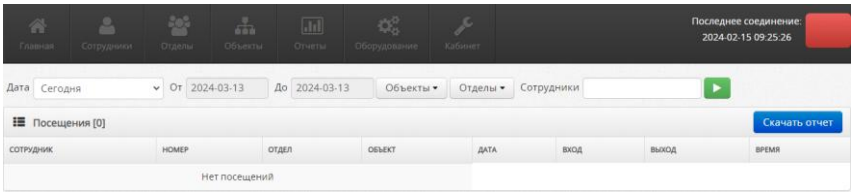


Для фильтрации выберите дату и нажмите «Применить».



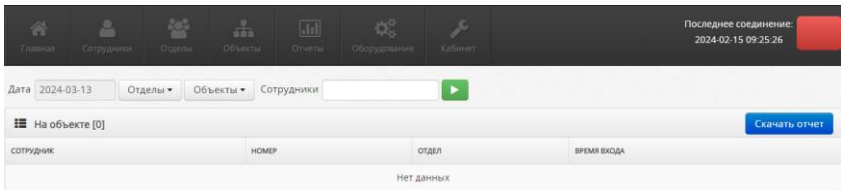
Отчёт «Посещения»

В отчете «Посещения» показывается посещение объектов сотрудниками в течение дня.



Отчёт «На объекте»

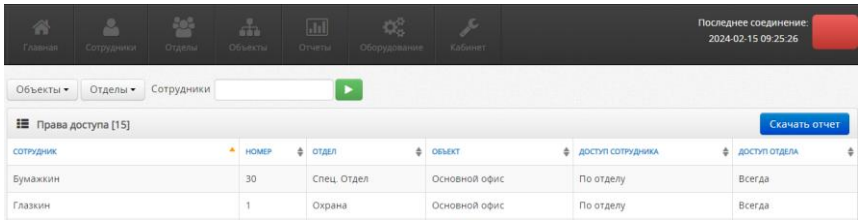
В отчете «На объекте» показывается список присутствующих сотрудников в указанное время на объектах.



Вспомогательные отчеты

Отчёт «Права доступа»

В отчете «Права доступа» показывается отчет о правах доступа в помещения.



Наиболее частые проблемы с отчетами

Дата и время событий указаны наперёд (из будущего)

При снятии напряжения с контроллера в нем сбивается время. Год в контроллере не хранится.

Если контроллер после подачи напряжения работал (совершались проходы) без синхронизации с сервисом, время событий в нем некорректное. После подключения к сервису контроллер синхронизируется с ним и все прошлогодние события и некорректные записывает как события текущего года.

Вывод: после подачи напряжения, до начала совершения проходов, контроллер нужно синхронизировать с сервисом. Тогда события проходов будут верные и не будет событий из будущего. Из контроллера события не удаляются, а только затираются свежими. Для того, чтобы ситуация не повторялась, контроллеры должны питаться от бесперебойников (ББП, ИБП, БРП). Если напряжение всё же сбрасывалось, нужно до начала совершения проходов синхронизировать контроллер с сервисом (без синхронизации время событий в нем некорректное).

Внимание! ***В сервисе добавлена автоматическая корректировка событий из контроллера со сбитым временем. При получении таких событий из будущего, сервис автоматически назначает им прошлый год. В отчетах такие события будут показываться как прошлогодние.***

Смещение времени событий

Время событий может отображаться со смещением в 1 (2,3) часа.

В информации о контроллере время отображается корректное, а в отчетах о прибытии/убытии время прихода сотрудников сдвинуто, например на 3 часа назад.

Время событий задается контроллером согласно состоянию внутренних часов. Часы контроллера синхронизируются с сервером периодически при соединении. Так как система позволяет соединять удаленные (иногда очень далеко) объекты, необходимо устанавливать часовой пояс оборудования, который задается в настройках конвертера.

В системе есть также установка часового пояса аккаунта, в личном кабинете. Эти установки разные, так как часовой пояс аккаунта и оборудования может быть разный.

Время последнего соединения оборудования показано в часовом поясе аккаунта. Время событий - в локальном времени часового пояса оборудования.

В списке событий не показывает фамилию сотрудника

В отчете «События» не показывается фамилия сотрудника. При этом номер карты определяется.

Фамилия сотрудника определяется не только кодом карты, но и временем назначения. Если карта еще не назначена сотруднику на время регистрации события, то поле Фамилии будет пустым. Это может произойти, например, при неправильной установке часового пояса конвертера. Время события устанавливается контроллером в локальном часовом поясе, и если он установлен неправильно, то время события не попадет в интервал времени назначения

карты конкретному сотруднику, и система будет считать, что карта на момент прохода никому не назначена.

«Ключ не найден», но Имя сотрудника указано

В списке событий указана Фамилия сотрудника, но тип события «Ключ не найден».
Решение о проходе принимает контроллер по номеру карты. Если ключ не найден - его нет в памяти контроллера. Фамилия показывается сервером по коду карты и не зависит от наличия ключа в контроллере. Ключ попадает в память контроллера не сразу. Некоторое время (обычно до нескольких минут) может быть ситуация, когда карта уже ассоциирована с человеком, но ключ еще не попал в контролер. Также такое может случиться из-за временного обрыва связи контроллера с сервером. Иногда такая ситуация происходит из-за устаревшей или проблемной прошивки контроллера, или даже его сбоя.
Если такое происходит случайно и редко, достаточно повторно сохранить карточку сотрудника, чья карта не попала в контроллер. При постоянных проблемах проверить прошивку и прошить контроллер рекомендуемой прошивкой. Если не помогает, то следует заменить контроллер.

Отчеты пустые, не показывается информация

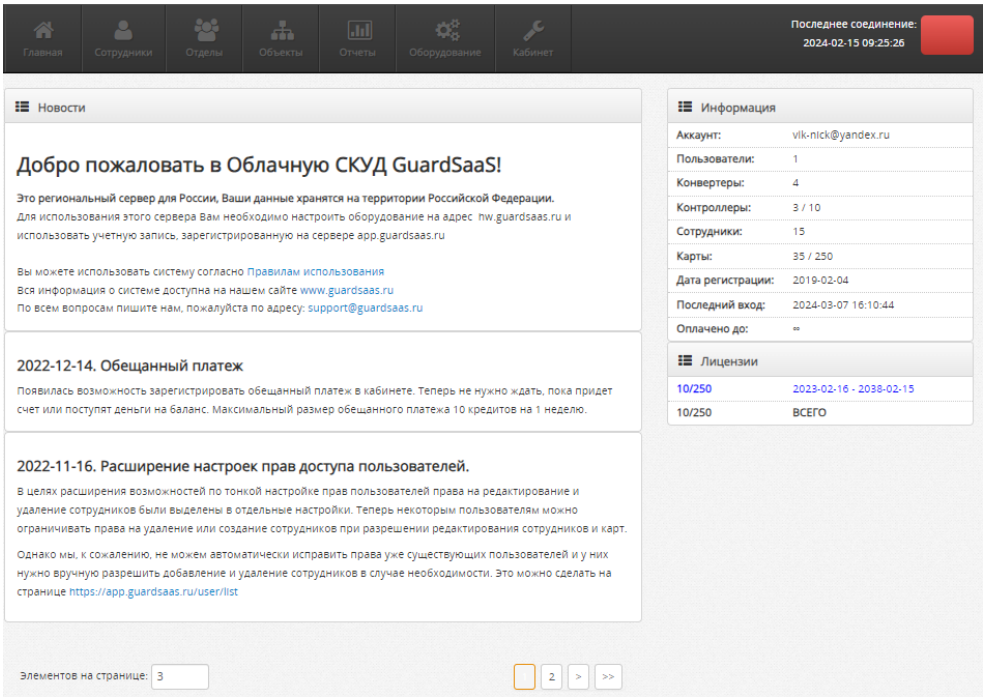
В GuardSaaS контроллеры создают события в системе при получении сигнала от карты через считыватель. Если связи контроллера с сервером нет, то события хранятся в памяти контроллера, пока не будет возможности передать их на сервер. Емкость памяти контроллеров различная и может быть от 2 до 32 тысяч событий. Обычно контроллер связывается с сервером несколько раз в секунду. Но при обрыве связи или неисправности интернета, или сбое контроллера, передача событий прерывается. В этом случае индикатор контроля оборудования в правом верхнем углу экрана становится красным, и время последнего соединения с сервером не обновляется. Вы легко можете понять, когда в последний раз контроллеры передали информацию на сервер. Соответственно отчеты нашего сервера показывают ту информацию, которую они получили от контроллеров, до момента нарушения связи. ***Для устранения проблемы необходимо восстановить связь контроллеров с сервером***.

В отчетах «Табель», «Приходы и уходы» и других нет данных за текущий день, или они неполные.

Статистические отчет (все, кроме отчета «События») формируются несколько раз в день. Окончательно данные пересчитываются в конце дня. Чтобы получить актуальные данные, воспользуйтесь кнопкой «Пересчитать».

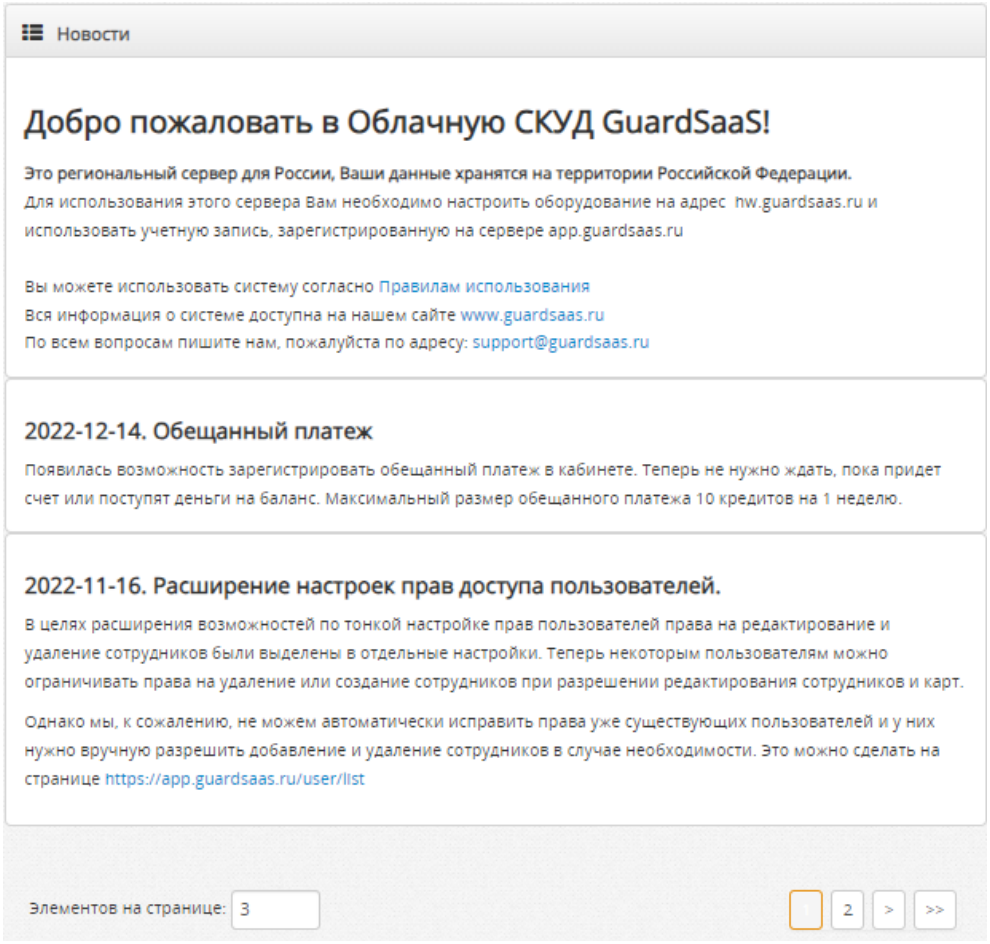
Вкладка «Главная»

На вкладке «Главная» находятся последние новости по сервису и информация по аккаунту.



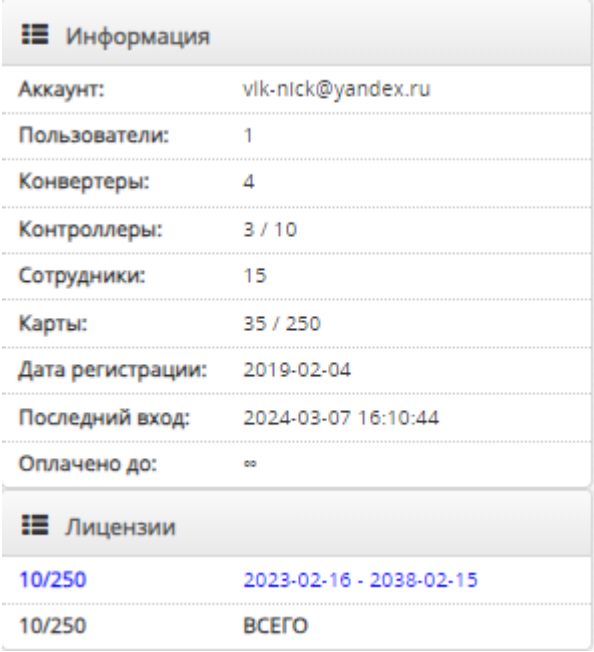
Новости

В разделе «Новости» показываются актуальные новости по работе с облачным сервисом.



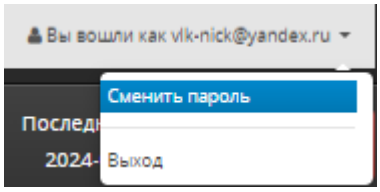
Информация

В разделе «Информация» отображается имя аккаунта, количество пользователей системы, количество подключенного оборудования, количество сотрудников и карт, а также дата регистрации и время последнего входа в систему.
В разделе «Лицензии» показаны актуальные лицензии.

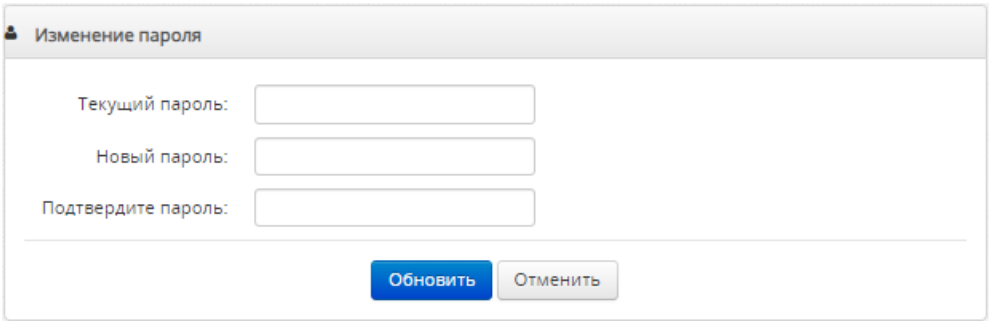


Смена пароля аккаунта

Для смены пароля нужно кликнуть левой кнопкой мыши на «Вы вошли как...» и выбрать «Сменить пароль».



Откроется окно «Изменение пароля». Введите текущий пароль, а затем новый пароль и подтвердите его.



После ввода нового пароля кликните по кнопке «Обновить».

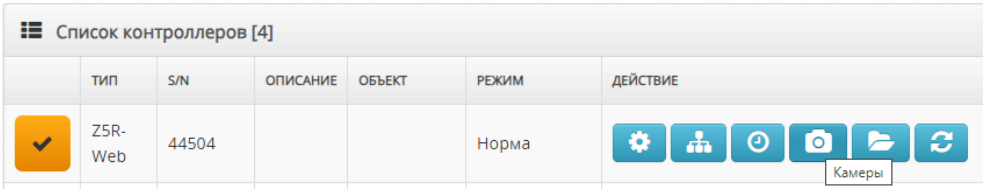
Интеграция GuardSaaS и систем видеонаблюдения

Интеграция предоставляет возможность быстрого просмотра видео, привязанное к событиям по месту и времени прямо из системы GuardSaaS. При этом GuardSaaS **не подключается к камерам напрямую** и **не хранит видео** на своем сервере, а получает видеопоток напрямую из системы видеонаблюдения. Для этого система видеонаблюдения должна уметь транслировать поток в интернет по заданной временной метке.
В настоящее время поддерживаются такие системы видеонаблюдения:

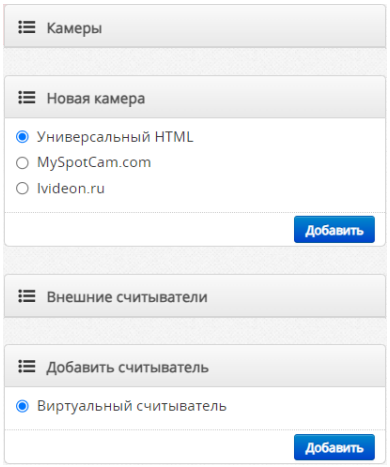
- MySpotCam.com (https://www.myspotcam.com/ru)
- Ivideon.com (https://ru.ivideon.com)
- Любые системы, предоставляющие встраиваемый код HTML для показа потока в Интернете.

Камеры

Для привязки видеокамеры к контроллеру нужно кликнуть по кнопке Камеры».



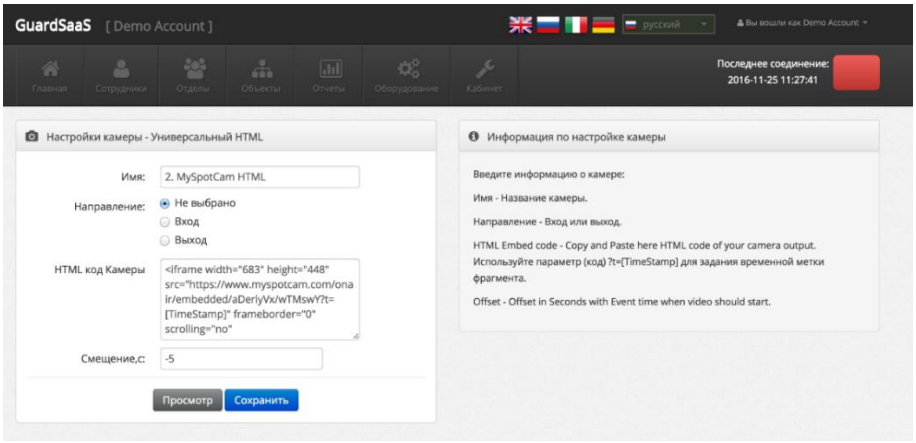
Далее в окне «Новая камера» выбирается тип камеры: «Универсальный HTML», «MySpotCam.com», «Ivideon.ru».



После выбора типа камеры нужно кликнуть по кнопке «Добавить».

Универсальный HTML

Существует большое количество систем и интегрироваться специально с каждой довольно сложно. Если система поддерживает возможность размещения HTML кода камеры на внешних сайтах, то этот код можно использовать в поле «HTML код камеры»:



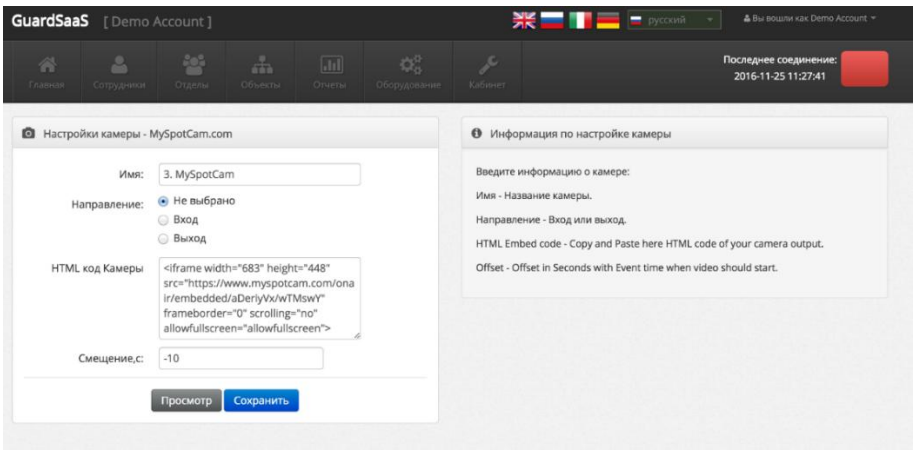
Для позиционирования потока на определенную временную метку используется параметр ?t=[TimeStamp] который размещается в нужном месте HTML кода.
Пример:
<frame width="683" height="448"
src="https://www.myspotcam.com/onair/embedded/aDeriyVx/wTMswY?t=[TimeStamp]"
frameborder="0" scrolling="no" allowfullscreen="allowfullscreen">
Такой параметр должен поддерживаться системой видеонаблюдения.

MySpotCam

https://www.myspotcam.com/ru

Вы должны иметь рабочий аккаунт в системе MySpotCam и подключить как минимум 1 камеру в систему.

Камеры настраиваются таким же образом, как и для других систем. При Выборе типа, нужно указать MySpotCam и задать все требуемые параметры:

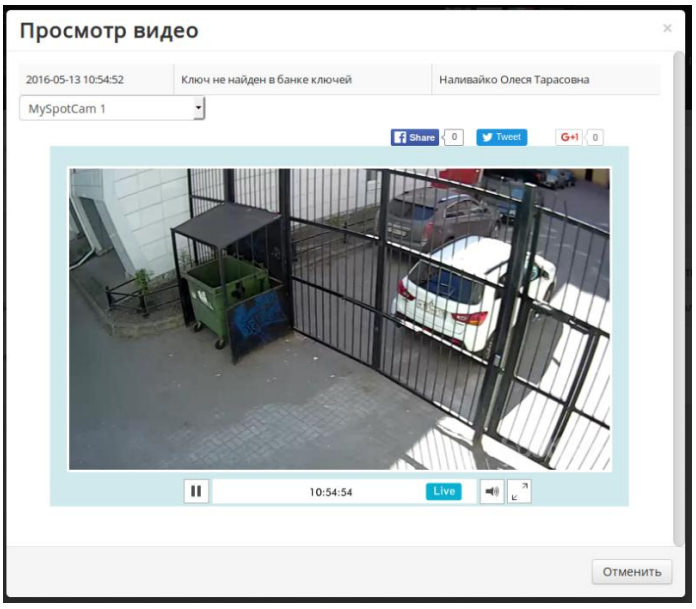


В поле «HTML код камеры» нужно скопировать embedded HTML code из настроек камеры в системе MySpotCam.

Пример: <frame width="683" height="448" src="https://www.myspotcam.com/onair/embedded/aDeriyVx/wTMswY" frameborder="0" scrolling="no" allowfullscreen=" allowfullscreen ">

Больше ничего делать не надо.

Нажмите «Просмотр» для получения текущей картинки:



И далее сохраните настройки.

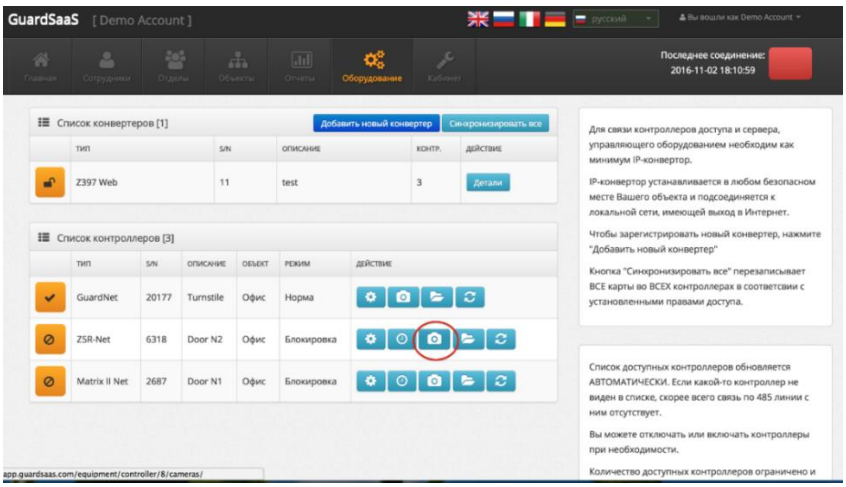
Дальнейшее использование аналогично другим типам систем видеонаблюдения.

Ivideon

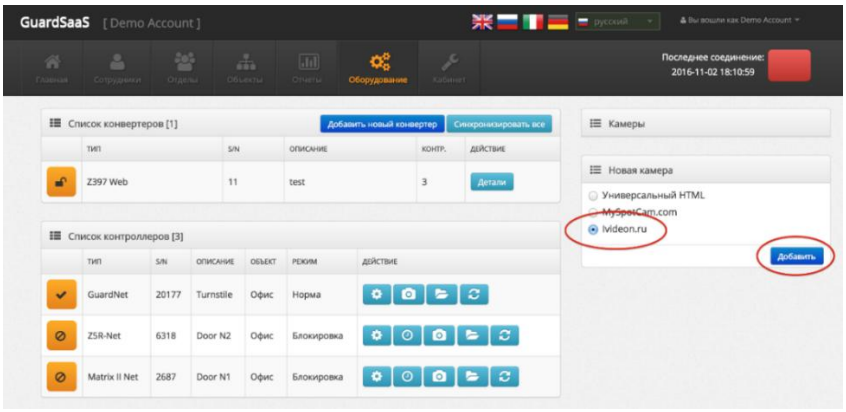
https://ru.ivideon.com/

Вы должны иметь рабочий аккаунт в системе Ivideon и подключить как минимум 1 камеру в систему.

Для привязки камеры к контроллеру нужно открыть список оборудования и нажать на кнопку «Камеры» контроллера.

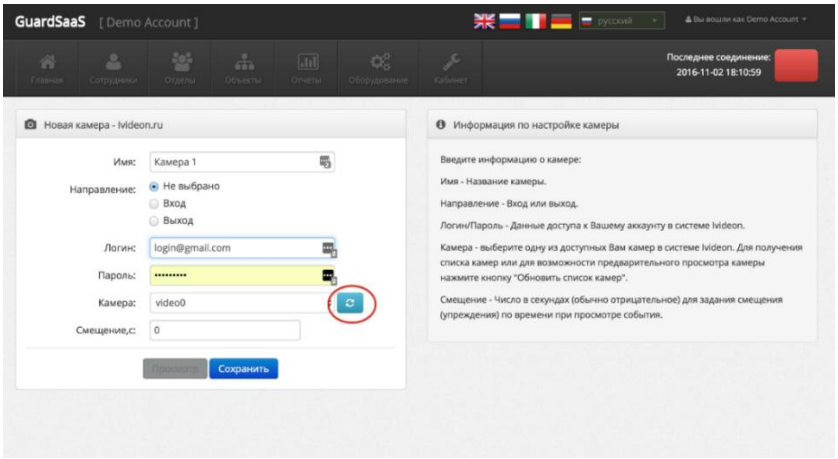


Выберите тип системы Ivideon и нажмите кнопку «Добавить». Введите название камеры, направление прохода, логин и пароль к системе Ivideon. Затем нажмите кнопку «Обновить», чтобы стал доступен список камер Ivideon.

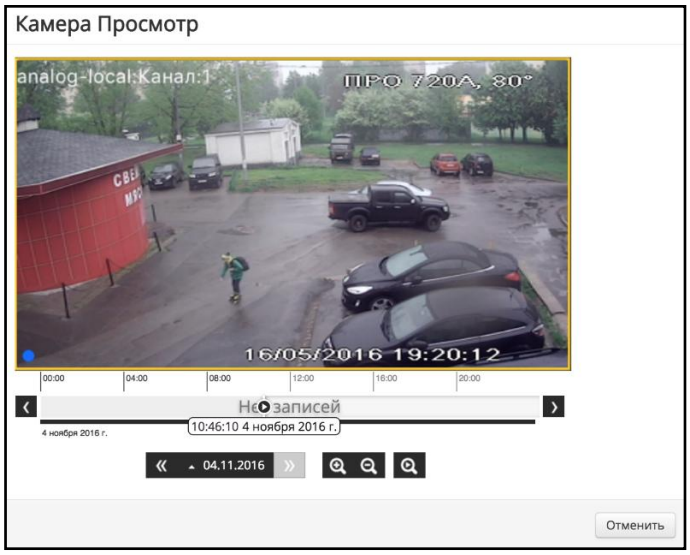


Введите информацию о камере:

- **Имя** – название камеры;
- **Направление** – вход или выход;
- **Логин/Пароль** – данные доступа к Вашему аккаунту в системе Ivideon;
- **Камера** – выберите одну из доступных Вам камер в системе Ivideon;
- **Смещение** – число секунд (обычно отрицательное) для задания смещения (упреждения) по времени при просмотре события.



При правильном вводе данных доступа в Ivideon станет доступной кнопка «Просмотр», и Вы сможете просмотреть изображение с камеры.



Далее нажмите кнопку «Сохранить». После чего можно перейти в список событий. Напротив события контроллера появится иконка просмотра, нажав на которую можно будет посмотреть видеофрагмент события из системы видеонаблюдения.

