SIGUR

Руководство по настройке интеграции с ключницами KeyGuard

Редакция от 15.09.2025.

«Промавтоматика», г. Н. Новгород, 2025 г.

SEC.RU | Короткий путь к информации

Скачано с sec.ru

Оглавление

1. Введение ... 3
2. Версии документа ... 4
3. Используемые определения, обозначения и сокращения ... 5
4. Системные требования ... 6
5. Описание интеграции ... 7
6. Подключение и настройка ... 8
   6.1. Установка IP-параметров ключницы ... 8
   6.2. Добавление ключницы в Sigur ... 9
      6.2.1. Вкладка «Ключницы» ... 11
      6.2.2. Вкладка «Списки ключей» ... 14
      6.2.3. Вкладка «Праздники» ... 15
      6.2.4. Вкладка «Временные зоны» ... 16
      6.2.5. Вкладка «Права доступа» ... 17
   6.3. Редактирование прав по доступу к ключам для объектов доступа ... 19
   6.4. Специальные логики доступа к ключам ... 20
      6.4.1. Выдача ключей с санкции оператора ... 21
      6.4.2. Выдача ключей с верификацией лица ... 22
      6.4.3. Выдача ключей с верификацией лица и санкцией оператора ... 23
   6.5. Логика работы с охранными зонами при выдаче/сдаче ключа ... 24
   6.6. События от ключницы ... 25
   6.7. Возможные сообщения об ошибках ... 25
7. Контакты ... 27

SEC.RU | Короткий путь к информации Скачано с sec.ru

1. Введение

Данный документ содержит инструкцию по настройке взаимодействия программного обеспечения системы контроля и управления доступом (СКУД) Sigur и ключниц KeyGuard.

Руководство по установке и настройке системы Sigur можно найти в отдельных документах: «Руководство администратора ПО Sigur» и «Руководство пользователя ПО Sigur».

Предприятие-изготовитель несёт ответственность за точность предоставляемой документации и при существенных модификациях в программном обеспечении обязуется предоставлять обновлённую редакцию данной документации.

SEC.RU | Короткий путь к информации Скачано с sec.ru

2. Версии документа

Данный документ имеет следующую историю ревизий.

Ревизия	Дата публикации	Что изменилось
0001	2021 г.	Первая версия документации.
0002	11 августа 2023 г.	Обновление внешнего вида документа. Устранение неточностей и опечаток.
0003	2 августа 2024 г.	Актуализация описания процесса настройки интеграции.
0004	15 сентября 2025 г.	Актуализация требований в связи с изменением схемы лицензирования. Добавление информации о возможности сортировки списка прав доступа к ключнице.

SEC.RU | Короткий путь к информации Скачано с sec.ru

3. Используемые определения, обозначения и сокращения

СКУД	Система контроля и управления доступом. Программно-аппаратный комплекс, предназначенный для осуществления функций контроля и управления доступом.
Точка доступа (ТД)	Место, где осуществляется контроль доступа. Например: дверь, турникет, ворота, шлагбаум, оборудованные считывателем, электромеханическим замком и другими необходимыми средствами.
ПО	Программное обеспечение.

SEC.RU | Короткий путь к информации Скачано с sec.ru

4. Системные требования

- Версия ПО Sigur: 1.0.60.1 и выше.
- Операционная система: согласно «Руководству администратора ПО Sigur».
- Лицензирование: необходима лицензия по количеству ключей. В случае использования пакетного лицензирования также требуется пакет лицензий Pro или Enterprise.

SEC.RU | Короткий путь к информации
Скачано с sec.ru

5. Описание интеграции

Настроенная интеграция позволяет:

- Добавлять ключницы KeyGuard в ПО Sigur.
- Управлять списком ключей и правами сдачи/выдачи ключей для конкретных пользователей.
- При наличии подключённого охранного шлейфа к контроллерам Sigur E2, E4, E300H или настроенного взаимодействия с интегрированными в Sigur охранными системами – автоматически ставить на охрану/снимать с охраны зоны при сдаче/выдаче ключей.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6. Подключение и настройка

Настройка взаимодействия с ключницей KeyGuard состоит из следующих этапов:

1. Задание IP-параметров на устройстве.
2. Редактирование и задание списка ключей, прав выдачи/сдачи ключей.
3. Назначение прав выдачи/сдачи ключей пользователям.

6.1. Установка IP-параметров ключницы

Установка IP-параметров ключницы происходит через меню настроек, доступ к которому можно получить путём открытия внешней дверцы (при её наличии) и внутренней (на которой расположены ячейки для брелоков с ключами) при помощи специального ключа аварийной разблокировки.

После открытия дверцы нужно нажать кнопку Settings (на модуле заряда АКБ, расположенном справа внутри основного блока).

На вкладке «IP настройки» необходимо заполнить параметры:

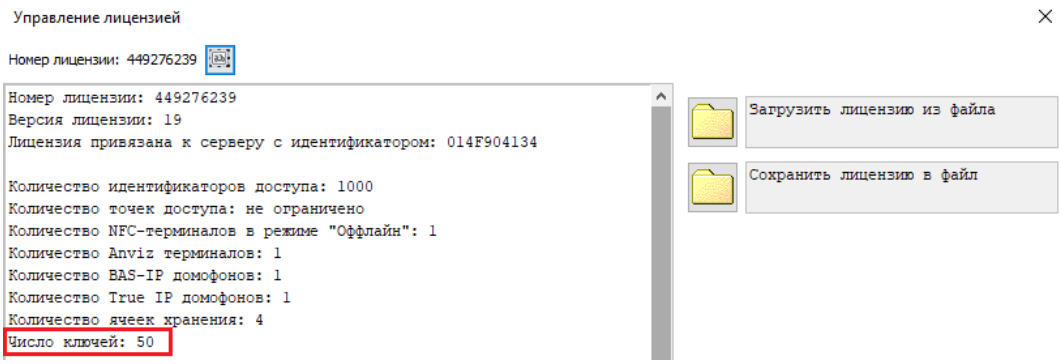
- «IP Адрес». Поле для установки IP-адреса устройства.
- «IP Сервер». IP-адрес ПК, на котором расположен сервер Sigur.
- «Маска подсети», «Осн. Шлюз». Поля заполняются в соответствии с настройками подсети, в которой устанавливается устройство.
- «Порт Серв.». Номер TCP-порта, используемого на стороне устройств и сервера для обмена данными. Рекомендуется оставить значение по умолчанию (8000).

После указания всех параметров необходимо последовательно нажать кнопки «Сохранить» и «Перезагрузка». После этого внесённые изменения вступят в силу.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2. Добавление ключницы в Sigur

Первоначально требуется проверить, что присутствует лицензия на необходимое количество ключей (через меню ПО «Клиент» – «Файл» – «Управление модулями»).



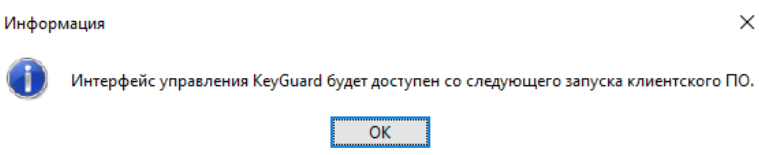
Отображение информации о лицензии на подключение ключниц KeyGuard.

Далее необходимо установить галочку «Включить интеграцию с KeyGuard» в меню «Файл» – «Настройки» – «Устройства хранения» и нажать кнопку «ОК».



Включение интеграции с KeyGuard.

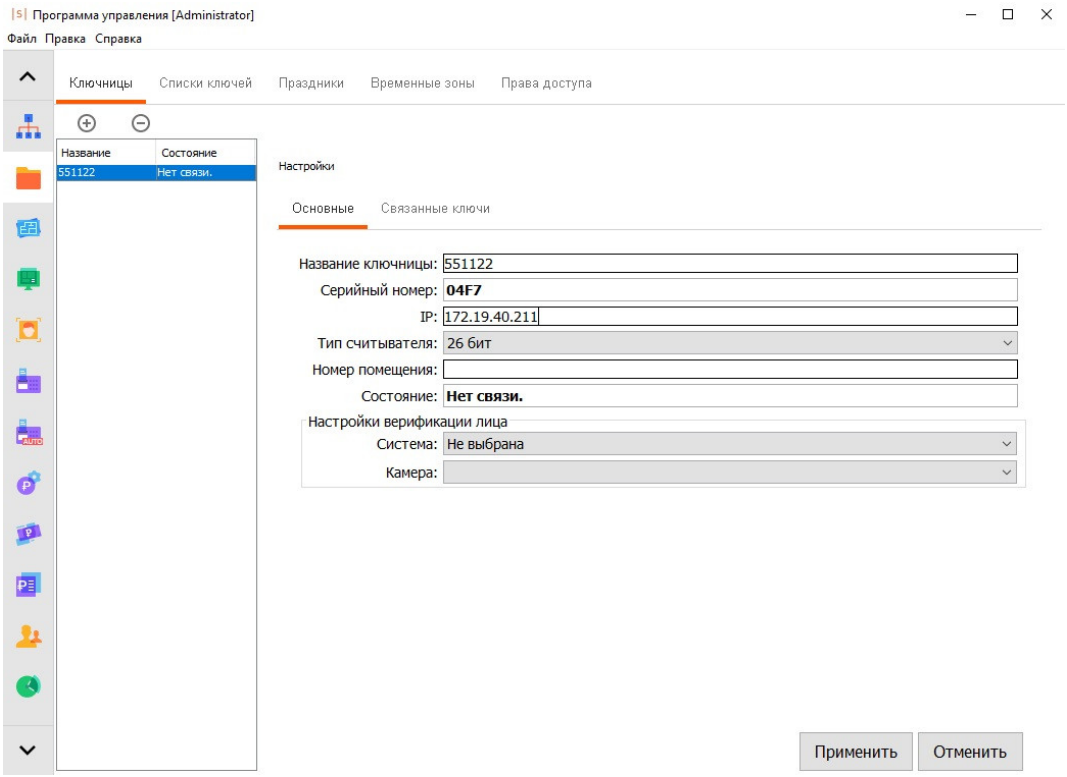
Функциональность интеграции будет доступна после перезапуска программы «Клиент», о чём будет выведено соответствующее предупреждение.



Информационное сообщение.

SEC.RU | Короткий путь к информации Скачано с sec.ru

После перезагрузки ПО «Клиент» становится доступна вкладка KeyGuard. На данной вкладке можно добавить необходимое количество ключниц, а также сформировать настройки для каждой из них (управление списками ключей и временных интервалов на сдачу/выдачу ключей).



Вкладка KeyGuard.

Вкладка KeyGuard имеет пять подвкладок: «Ключницы», «Списки ключей», «Праздники», «Временные зоны» и «Права доступа». Функциональность каждой подвкладки описана в соответствующих разделах ниже.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.2.1. Вкладка «Ключницы»

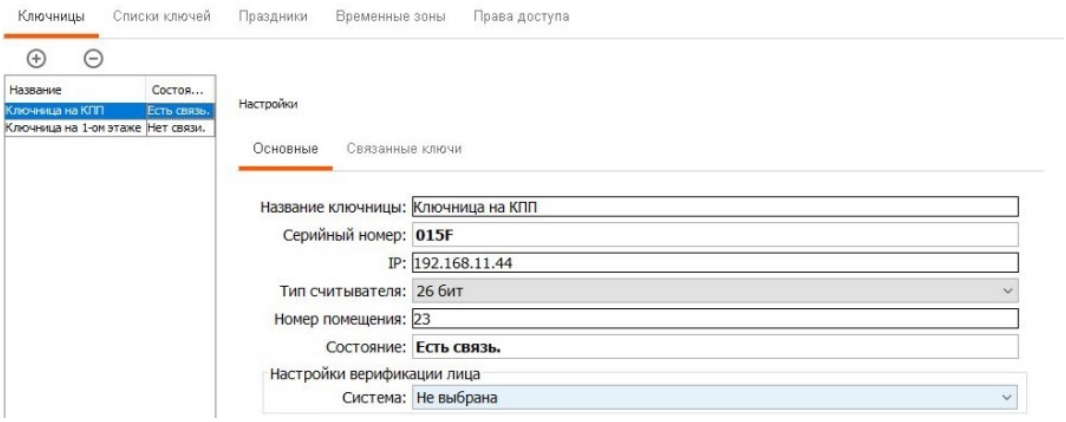
Нажатием на кнопки «+» и «-» можно добавить в список устройств новую ключницу или удалить из списка имеющуюся. При нажатии на кнопку «+» откроется окно для указания параметров нового устройства:



Окно добавления ключницы.

- «Название ключницы». Строка для указания названия ключницы. Длина строки – от 1 до 23 символов.
- «IP-адрес». Поле, в котором необходимо указать IP-адрес ключницы KeyGuard, уже заданный через её меню настроек или планируемый.
- «Производитель».

После указания всех параметров нажмите кнопку «OK». В случае необходимости прерывания операции добавления нового устройства нажмите кнопку «Отмена». После успешного добавления новое устройство появится в списке ключниц.



Основные настройки ключницы.

Для каждой ключницы доступны следующие параметры настройки:

- «Название ключницы». Строка для указания названия ключницы. Длина строки – от 1 до 23 символов.
- «Серийный номер». Нередактируемое поле, в котором отображается заводской номер устройства, автоматически считанный с ключницы, как только с ней появилась связь.
- «IP». Поле для указания IP-адреса ключницы.

SEC.RU | Короткий путь к информации Скачано с sec.ru

- «Тип считывателя». Выпадающий список с выбором формата Wiegand для встроенного в контрольную панель ключницы считывателя карт. Возможен выбор «26 бит» и «44 бит».
- «Номер помещения». Строка для указания номера помещения, в котором установлена ключница. Номер помещения должен быть в формате от 1 до 3 цифр и, при необходимости, 1 буквы (Примеры: «1А», «154Б» или «27»).
- «Состояние». Поле с отображением текущего статуса связи с устройством. Возможные состояния:

  - «Нет связи». По указанному адресу не удаётся связаться с ключницей KeyGuard.
  - «Есть связь». С устройством есть связь, идёт работа в штатном режиме.
  - «Загрузка БД...». С устройством есть связь, идёт чтение информации из ключницы. Происходит при первичном добавлении устройства, а также при перезапуске серверного модуля Sigur.
  - «Синхронизация». В БД Sigur были изменены связанные с ключницей данные, идёт запись обновлённых данных в устройство.

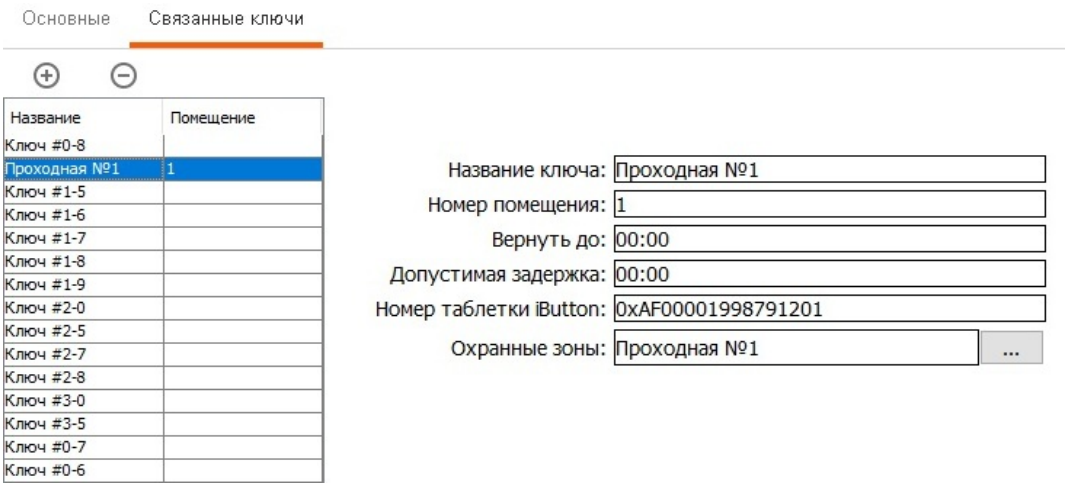
- «Система». Выпадающий список с выбором камеры, привязанной к ключнице. Используется при реализации специальной логики «Доступ с верификацией лица». Подробнее – в разделе «Выдача ключей с верификацией лица».



В зависимости от ключницы, загрузка базы данных может занимать продолжительное время (вплоть до нескольких часов).

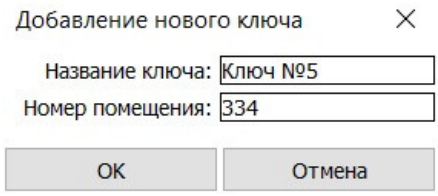
Для каждой из добавленных в систему ключниц в разделе «Настройки» – «Связанные ключи» отображаются ключи, которые должны быть известны ключнице. Перечень ключей автоматически загружается из ключницы в момент первого установления с ней связи. Также перечень можно редактировать вручную, добавляя новые ключи и удаляя более ненужные из имеющихся – для этого предназначены кнопки «+» и «-» соответственно на подвкладке «Связанные ключи».

SEC.RU | Короткий путь к информации Скачано с sec.ru



Окно связанных с ключницей ключей.

При добавлении ключа необходимо указать для него название и, если нужно, номер связанного с ним помещения. По нажатию на кнопку «ОК» новый ключ будет добавлен к ключнице.



Окно добавления ключа.

Для каждого добавленного ключа доступны следующие параметры:

- «Название ключа». Строка для указания названия ключа. Длина строки – от 1 до 23 символов.
- «Номер помещения». Поле для указания связанного с ключом помещения в формате «1-3 цифры + 0-1 буква». На стороне СКУД никак не интерпретируется, прописывается в ключницу для дополнительного отображения на экране ключницы KeyGuard при операциях с ключом.
- «Вернуть до». Указание в формате «ЧЧ:ММ» времени суток, к которому ключ должен быть возвращён в ключницу.
- «Допустимая задержка». Указание в формате «ЧЧ:ММ» величины интервала, допустимого для задержки при сдаче ключа. При сдаче ключа после указанного времени в полях «Вернуть до» и «Допустимая задержка» система сгенерирует событие: «Ключница N: ключ X не был возвращён вовремя сотрудником N».
- «Номер таблетки iButton». Поле для указания уникального идентификатора, встроенного в брелок ключницы.
- «Охранные зоны». По нажатию на кнопку «...» можно выбрать, какая из добавленных в систему охранных зон (при использовании интеграции с ОПС «Болид», «Рубеж» или при подключении охранного шлейфа к контроллерам Sigur E2, E4 и E300H) будет ассоциирована с данным

SEC.RU | Короткий путь к информации Скачано с sec.ru

ключом. При задании ключу в соответствие охранной зоны возможна автоматическая постановка и снятие с охраны соответствующей зоны при сдаче или выдаче ключа. Более подробно логика и поведение системы описаны в разделе «Логика работы с охранными зонами при выдаче/сдаче ключа».

По окончании редактирования нужных параметров ключа нажмите кнопку «Применить» для сохранения изменений. Для отмены всех внесённых изменений нажмите кнопку «Отменить».

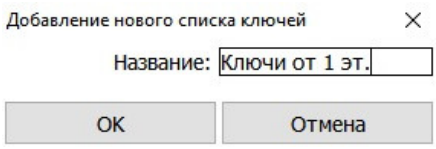
6.2.2. Вкладка «Списки ключей»

Предназначена для организации более удобной работы при большом количестве ключей – для объединения ключей в группы, т. н. «списки ключей». При создании списка ключей и дальнейшего его назначения пользователю как доступного для выдачи, на экране ключницы в диалоге выдачи ключей пользователь сможет разово указать интересующую его группу ключей для выдачи вместо многократного выбора каждого из ключей по отдельности.

Для каждой из ключниц формируются свои собственные «списки ключей» из известных им ключей. Выбор ключницы для просмотра и редактирования списков ключей осуществляется в верхней части вкладки из выпадающего списка. В левой части вкладки под областью выбора ключницы расположена область с добавленными в систему списками ключей для выбранного устройства.

Добавление и удаление списков ключей производится нажатием на кнопки «+» или «-» соответственно.

При добавлении нового списка ключей необходимо ввести для него некое название и нажать кнопку «ОК». Название списка ключей – строка длиной от 1 до 31 символа.

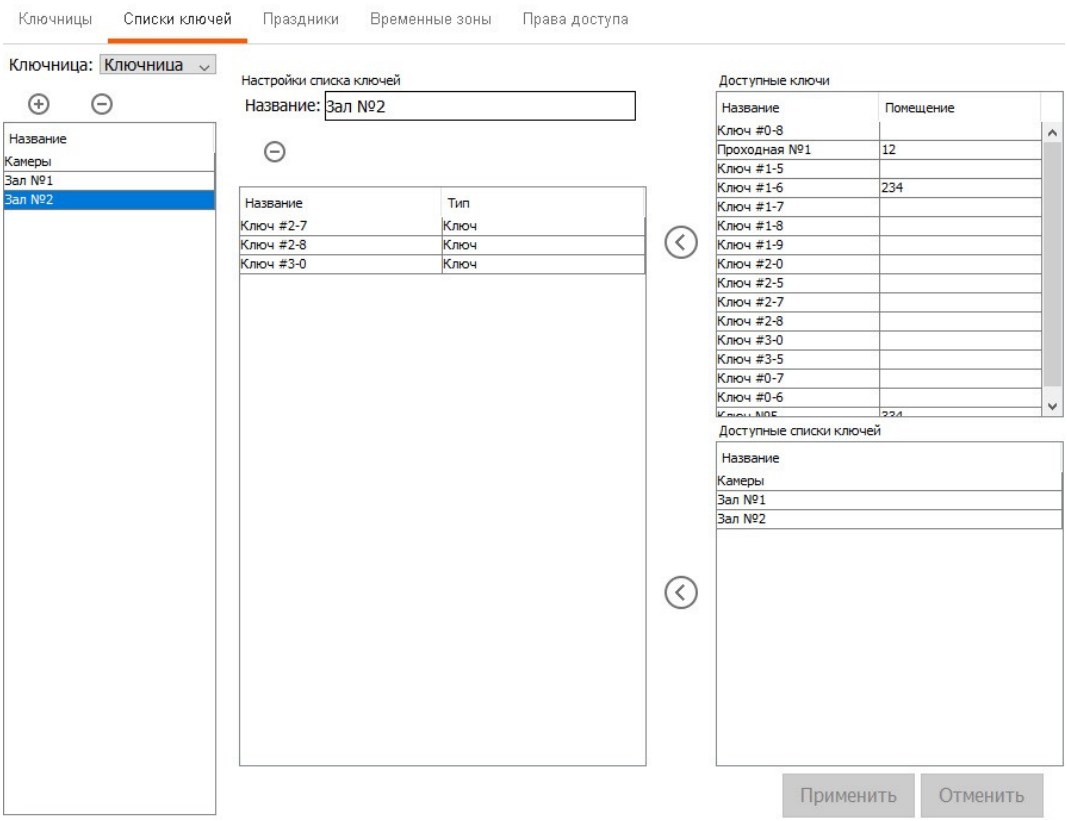


Добавление списка ключей.

В области редактирования списка расположено три панели: в правой части окна панели с доступными ключами и созданными списками ключей выбранной ключницы, в центральной области окна расположен перечень ключей и списков ключей, которые входят в состав редактируемого списка. Перенести ключ/список ключей из списка доступных в редактируемый список можно либо двойным кликом левой кнопки мыши, либо нажатием на кнопку «<». Убрать ненужные ключи/списки ключей из списка – двойным кликом левой кнопки мыши. По окончании редактирования списка ключей

SEC.RU | Короткий путь к информации Скачано с sec.ru

нажмите кнопку «Применить» для сохранения изменений. Для отмены всех внесённых изменений нажмите кнопку «Отменить».

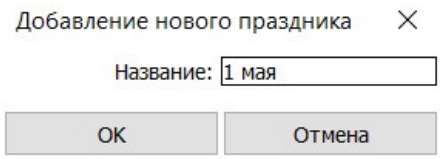


Вкладка «Списки ключей».

6.2.3. Вкладка «Праздники»

Предназначена для задания особых дней-исключений (праздничных), которые используются при формировании правил времени выдачи/сдачи ключей на вкладке «Временные зоны». Создаваемые праздничные дни являются общими для всех ключниц, заносимых в систему. Всего может быть задано до 33 дней в качестве праздничных.

Для добавления нового праздничного дня нажмите кнопку «+». При добавлении нового правила времени введите его название в соответствующее поле и нажмите «ОК».



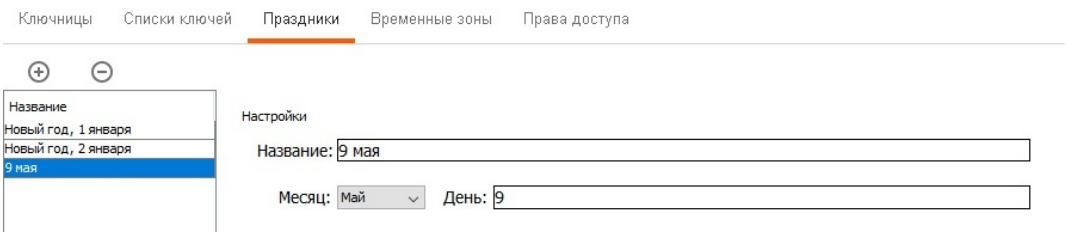
Добавление праздничного дня.

Для удаления выбранного праздничного дня нажмите кнопку «-».

SEC.RU | Короткий путь к информации Скачано с sec.ru

Для каждого созданного дня доступны следующие поля для редактирования:

- «Название». Строка с указанием названия праздничного дня. Длина строки названия временной зоны – от 1 до 23 символов.
- «Месяц». Выпадающий список с указанием одного из месяцев.
- «День». Строка с указанием номера дня в конкретном месяце.

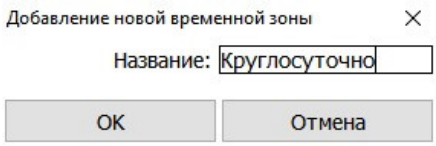


Вкладка «Праздники».

6.2.4. Вкладка «Временные зоны»

Предназначена для задания временных параметров разрешённых интервалов на выдачу/сдачу ключей. Создаваемые временные правила являются общими для всех ключниц, заносимых в систему.

Для добавления нового правила времени нажмите кнопку «+», введите его название в соответствующее поле и нажмите «ОК». Длина строки названия временной зоны – от 1 до 23 символов.



Добавление временной зоны.

Для удаления выбранного правила нажмите кнопку «-».

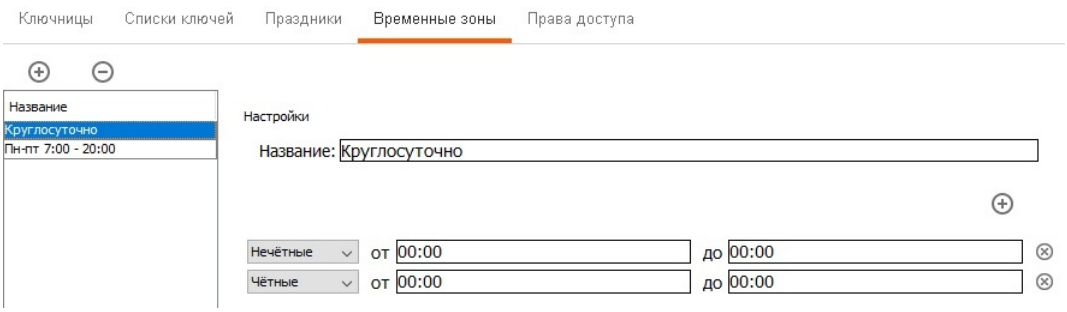
Для каждой выбранной зоны в правой части окна открывается область с её настройками. По нажатию кнопки «+» можно добавить новый интервал. Каждый из интервалов имеет следующую структуру:

- Тип дня – выпадающий список с выбором того, какому дню соответствует описываемый интервал: один из дней стандартной недели (понедельник, вторник и т. д.), праздничный день (какие дни являются праздничными указывается на вкладке «Праздники»), чётный или нечётный.
- Указание разрешённого для сдачи/выдачи времени – поля «От» и «До».
- Кнопка удаления выбранного интервала.

В каждом правиле времени можно указать до 10 временных интервалов.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Нажатие кнопки «Применить» сохраняет все внесённые в правило времени изменения. Кнопка «Отменить» отменяет все внесённые изменения до последнего сохранённого состояния.



Вкладка «Временные зоны».

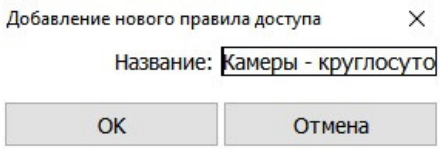
6.2.5. Вкладка «Права доступа»

Предназначена для задания соответствия между известными ключнице ключами/списками ключей и допустимыми временными интервалами на их сдачу/выдачу, а также для включения специальных логик доступа к ключам. Для каждой из ключниц формируются свои собственные «права доступа».

Формировать права доступа к ключам необходимо сразу с учётом того, что конкретному сотруднику можно будет задать только одно право на доступ к ключам.

Выбор ключницы для просмотра и редактирования прав доступа к её ключам осуществляется в верхней части вкладки из выпадающего списка. В левой части вкладки, под областью выбора ключницы, расположена область с добавленными в систему правами доступа для выбранного устройства. Добавление и удаление прав доступа производится нажатием на кнопки «+» или «-» соответственно.

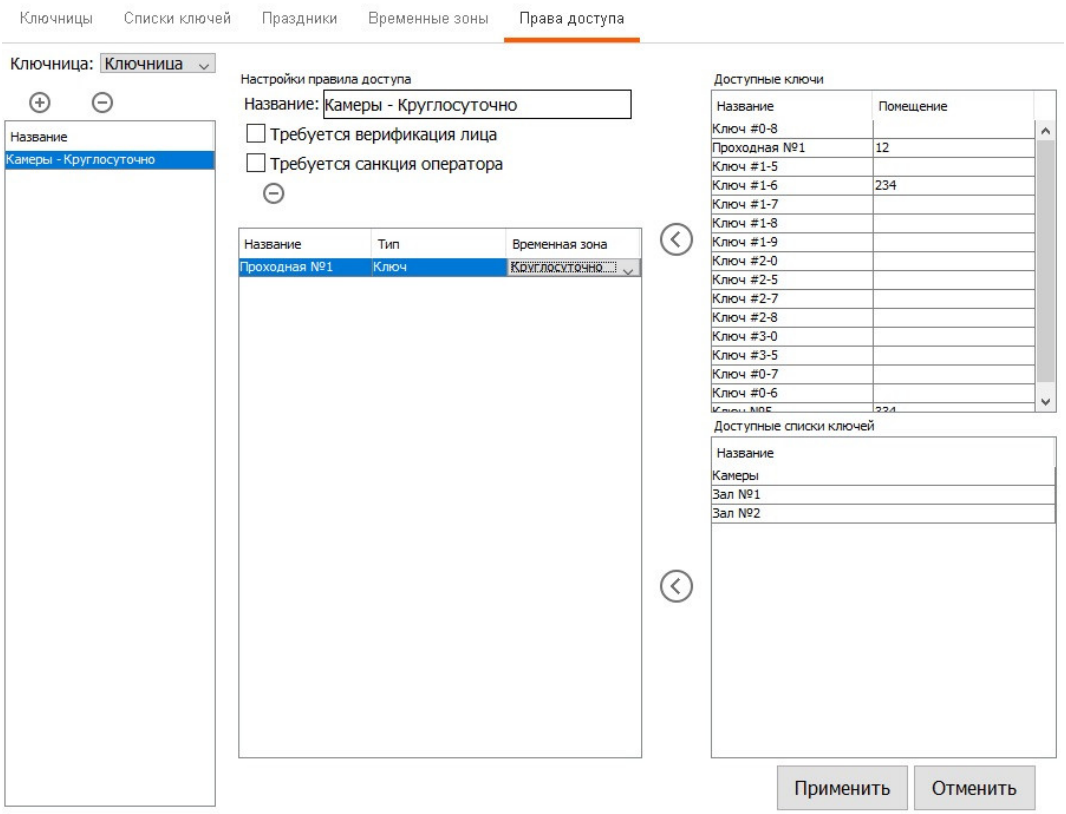
При добавлении нового права доступа необходимо ввести для него название и нажать кнопку «ОК». Название права доступа – строка длиной от 1 до 31 символа.



Добавление права доступа.

По умолчанию список прав доступа отображается в порядке добавления. Для сортировки по алфавиту нажмите на заголовок столбца «Название».

SEC.RU | Короткий путь к информации Скачано с sec.ru



Вкладка «Права доступа».

В области редактирования правила доступа к ключам расположено три панели: в правой части окна панели с доступными ключами и созданными списками ключей выбранной ключницы, в центральной области окна сверху расположены поля включения специальных логик доступа к ключам. Данная функциональность подробно описана в разделе «Специальные логики доступа к ключам». Ниже расположен перечень ключей и списков ключей, которые входят в состав редактируемого правила. Перенести ключ/список ключей из списка доступных в редактируемый список можно либо двойным кликом левой кнопки мыши, либо нажатием на кнопку «<». Убрать ненужные ключи/списки ключей из списка – двойным кликом левой кнопки мыши.

Для ключа/списка ключей, перенесённых в центральную область окна, необходимо также выбрать временную зону из ранее созданных.

По окончании редактирования права доступа нажмите кнопку «Применить» для сохранения изменений. Для отмены всех внесённых изменений нажмите кнопку «Отменить».

SEC.RU | Короткий путь к информации Скачано с sec.ru

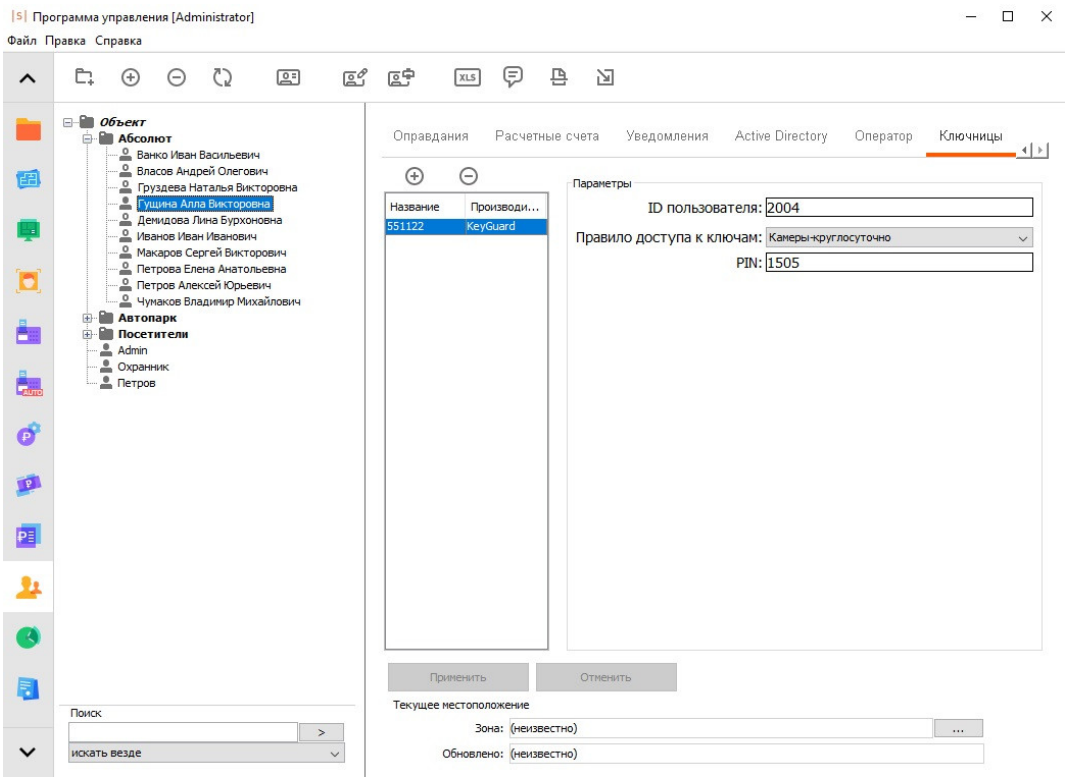
6.3. Редактирование прав по доступу к ключам для объектов доступа

Задание пользователям прав на доступ к ключам осуществляется через вкладку «Персонал».

На вкладке «Персонал» выбирается сотрудник, которому необходимо обеспечить доступ к ключницам, для него открывается подвкладка «Ключницы». В левой части окна находится список ключниц, к которым у сотрудника может иметься доступ. Нажатие на кнопку «+» позволяет выбрать для добавления в доступные ключницу из списка добавленных в систему. Нажатие на кнопку «-» удаляет выбранную ключницу из списка доступных сотруднику.

После добавления ключницы в список доступных в правой области подвкладки можно указать параметры для доступа к ней:

- «ID пользователя» – уникальный ID пользователя, которым он может идентифицировать себя на устройстве при отсутствии/невозможности предъявления карты.
- «Правило доступа к ключам» – указание правила на доступ к ключам конкретной ключницы, созданного заранее на вкладке «KeyGuard».
- «PIN» – пин-пароль для пользователя, при помощи которого он может идентифицировать себя на устройстве при вводе ID.



Задание права на доступ к ключам конкретной ключницы сотруднику.

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.4. Специальные логики доступа к ключам

Возможна организация специальных логик доступа к ключам, хранящимся в ключнице:

- Выдача ключей с санкции оператора
- Выдача ключей с верификацией лица
- Выдача ключей с верификацией лица и санкцией оператора

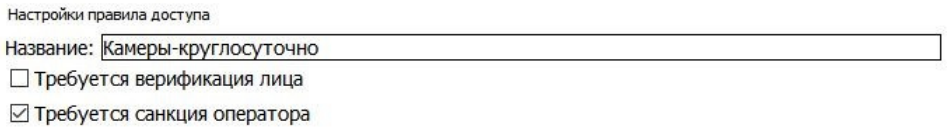
SEC.RU | Короткий путь к информации Скачано с sec.ru

6.4.1. Выдача ключей с санкции оператора

При включении данной логики, после поднесения карты к считывателю ключницы и выбора ключей сотрудник подтверждает действие нажатием соответствующей кнопки на экране ключницы. Ключница формирует запрос-подтверждение на выдачу ключей на сервер СКУД. Данный запрос отображается на АРМ оператора, который либо подтверждает выдачу ключей поднесением своей карты к настольному считывателю ACR1252, Iron Logic Z-2 USB или Sigur Reader EH, либо запрещает её нажатием кнопки «Отмена».

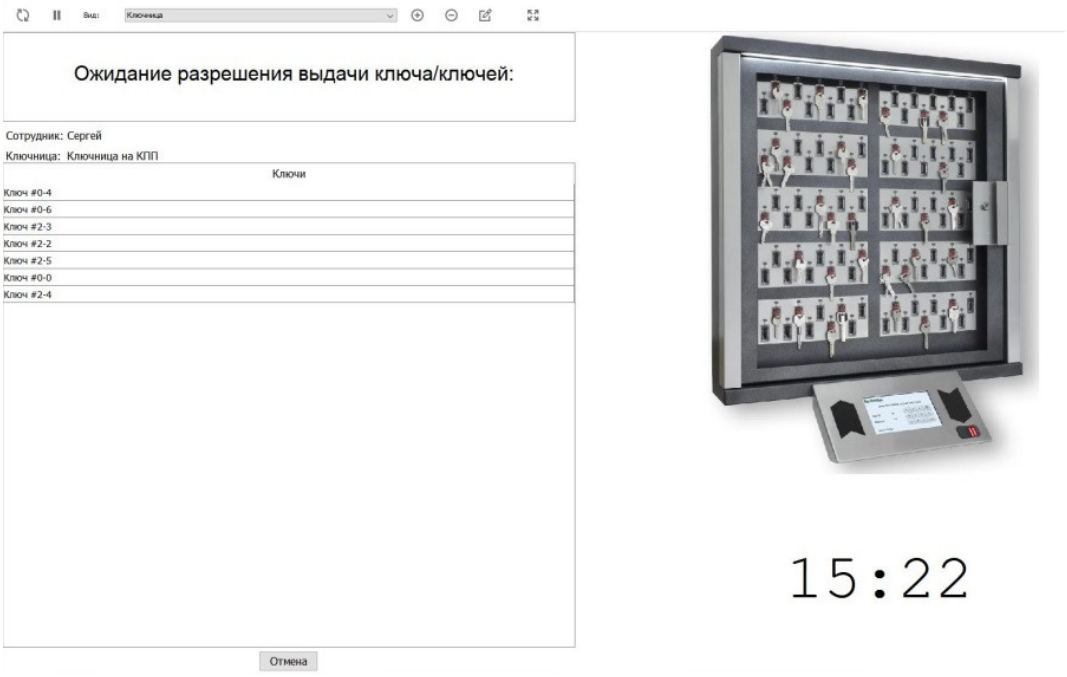
Для настройки данной логики требуется выполнить следующие шаги:

- Включение санкции оператора. Производится на вкладке «Права доступа» путём установки соответствующей галочки.



Включение санкции оператора.

- Настройка вида наблюдения. Для отображения запроса подтверждения на АРМ оператора должен быть настроен вид наблюдения с размещённым на нём объектом «Ключница». Подробнее о создании видов наблюдения – в разделе «Наблюдение событий в реальном времени» «Руководства пользователя ПО Sigur».



Вид наблюдения с добавленным на него объектом «Ключница».

SEC.RU | Короткий путь к информации Скачано с sec.ru

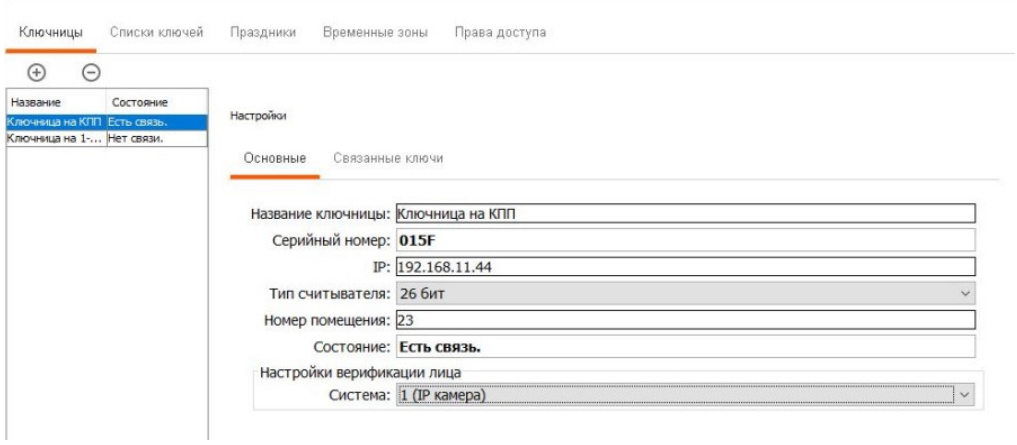
6.4.2. Выдача ключей с верификацией лица

При включении данной логики, после поднесения карты к считывателю ключницы и выбора ключей сотрудник подтверждает действие нажатием соответствующей кнопки на экране ключницы. Ключница формирует запрос-подтверждение на выдачу ключей на сервер СКУД. После получения запроса-подтверждения от ключницы сервером СКУД в автоматическом режиме производится распознавание лица сотрудника с IP-камеры, привязанной к данной ключнице. В случае успешного распознавания сотруднику предоставляется доступ к ключам.

Для настройки данной логики требуется выполнить следующие шаги:

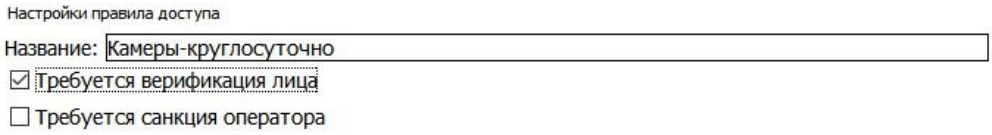
- Добавление IP-камеры в систему и включение встроенной функции распознавания лиц (подробнее – в разделе «Необходимые настройки при использовании встроенной функции распознавания лиц» «Руководства пользователя ПО Sigur»).

- Привязка камеры к ключнице. Производится на вкладке «Ключницы» путём выбора камеры из выпадающего списка «Система».



Привязка камеры к ключнице.

- Включение верификации лица. Производится на вкладке «Права доступа» путём установки соответствующей галочки.



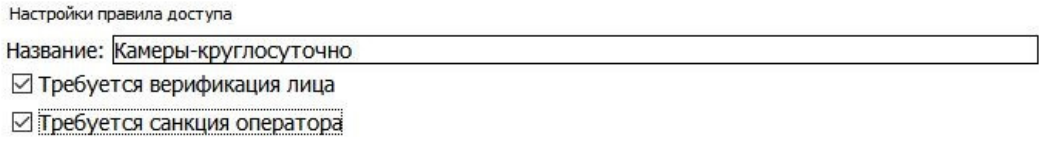
Включение верификации лица.

SEC.RU | Короткий путь к информации Скачано с sec.ru

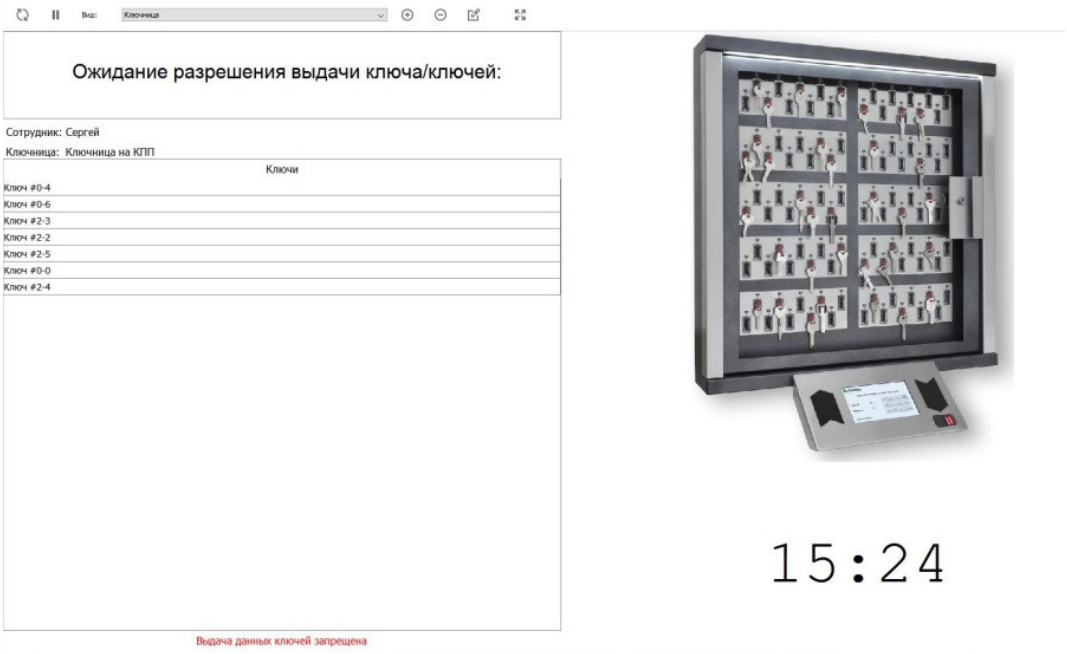
6.4.3. Выдача ключей с верификацией лица и санкцией оператора

При включении данной логики после поднесения карты к считывателю ключницы и выбора ключей сотрудник подтверждает действие нажатием соответствующей кнопки на экране ключницы. Ключница формирует запрос-подтверждение на выдачу ключей на сервер СКУД. После получения запроса-подтверждения от ключницы сервером СКУД в автоматическом режиме производится распознавание лица сотрудника с IP-камеры, привязанной к данной ключнице. В случае успешного распознавания сервер СКУД передаёт запрос на АРМ оператора, который либо подтверждает выдачу ключей поднесением карты к настольному считывателю, либо запрещает нажатием кнопки «Отмена» на виде наблюдения.

В случае если лицо не было опознано, выдача ключей запрещается. На АРМ оператора приходит тревожное сообщение с информацией о сотруднике, попытавшемся получить ключи, и их список.



Включение верификации лица и санкции оператора.



Тревожное сообщение на вкладке «Наблюдение».

SEC.RU | Короткий путь к информации Скачано с sec.ru

6.5. Логика работы с охранными зонами при выдаче/сдаче ключа

При выдаче/сдаче ключей могут производиться действия над охранными зонами и, в зависимости от результата, на экране ключницы будет отображаться сообщение об успешности этого действия. В случае, если с ключом связана только одна зона и системе известен её охранный статус, он отображается на экране ключницы. Если с ключом связано несколько зон, то отображается их суммарный охранный статус:

- «Тревога», если хотя бы над одной из зон действие выполнить не удалось.
- «Снято», если все зоны сняты с охраны.
- «Охрана», если все зоны успешно поставлены под охрану.

Ключница ожидает ответа от системы об успешности действия над зоной/группой зон в течение 20 секунд, после чего включается звуковая сигнализация и ключница переходит в режим ожидания закрытия дверцы.

Выдача ключа.

В момент выдачи любого ключа проверяется состояние связанных с ним зон/групп зон. Если зоны были поставлены на охрану, то произойдет попытка снятия зон с охраны. Если за время ожидания ключницей ответа об успехе данной операции станет известен новый статус зон, то он отобразится на экране ключницы. Если хотя бы одну из зон не удалось снять с охраны, то на экране ключницы будет отображено тревожное сообщение. Если все зоны были успешно сняты с охраны, то на экране ключницы будет отображено «снято».

Если зоны на момент выдачи ключа не были поставлены на охрану, то с зонами ничего не произойдет. На экране ключницы отобразится информация о том, что зоны «сняты» с охраны.

Если зона/одна из группы зон на момент выдачи ключа имеет тревожный статус и системе это известно, то на экране ключницы при извлечении ключа будет высвечено тревожное сообщение. Если остальные связанные с данным ключом зоны не имеют тревожного статуса, то, если среди них есть зоны, поставленные под охрану, будет предпринята попытка снять их с охраны. На отображаемую на экране устройства тревогу это не повлияет.

Возврат ключа.

При сдаче ключа учитывается, является ли сдаваемый ключ последним выданным ключом, ассоциированным с конкретной охранной зоной. В случае если с зоной связаны другие ключи, и они выданы, то над зоной не проводится никаких действий, кроме мониторинга её текущего состояния и его учёта в отображаемом на экране ключницы статусе.

SEC.RU | Короткий путь к информации Скачано с sec.ru

Если же это последний ключ, и более выданных ключей, связанных с данной зоной, нет, то ведётся проверка текущего состояния зоны и, если она имеет статус «снято», происходит попытка постановки зоны на охрану. Если за время ожидания ключницей ответа об успехе данной операции станет известен новый статус зон, то он отобразится на экране ключницы. Если хотя бы одну из зон не удалось поставить на охрану, то на экране ключницы будет отображено тревожное сообщение. Если все зоны были успешно поставлены на охрану, на экране ключницы будет отображено «Охрана».

Если хотя бы одна из связанных с ключом зон на момент попытки сдать ключ уже имеет тревожный статус и системе это известно, то на экране ключницы при попытке возврата ключа будет высвечено тревожное сообщение. Если остальные связанные с данным ключом зоны не имеют тревожного статуса, то для него справедлив один из двух предыдущих абзацев. На отображаемую на экране устройства тревогу это не повлияет.

6.6. События от ключницы

Все зарегистрированные ключницей события записываются в отчёт «Журнал действий операторов».

Возможные сообщения:

- «Ключница N: ошибка wiegand». Пришедшая по Wiegand от встроенного в ключницу считывателя посылка некорректна.
- «Ключница N: неверный PIN для сотрудника(...)». После указания уникального ID сотрудника на данной ключнице для него был введён неверный PIN.
- «Ключница N: неизвестная карта(...)». Ключнице был предъявлена неизвестная для неё карта.
- «Ключница N: предъявлена карта(...)».
- «Ключница N: ключ X не был возвращён вовремя сотрудником N».
- «Ключница N: ключ X был выдан сотруднику N».
- «Ключница N: ключ X был выдан сотруднику N в недопустимое время».
- «Ключница N: ключ X был выдан другому сотруднику N».
- «Ключница N: ключ X был возвращён сотрудником N».
- «Ключница N: ключ X был возвращён сотрудником N в недопустимое время».
- «Ключница N: ключ X был возвращён другим сотрудником N».
- «Ключница N: верификация лица не пройдена».

6.7. Возможные сообщения об ошибках

- «Ключница с заданным именем уже существует». Задайте другое уникальное имя для устройства, ключница KeyGuard с таким названием уже была добавлена ранее.
- «Ключница с заданным IP-адресом уже существует». Проверьте корректность заданного IP-адреса, ключница KeyGuard с таким IP-

SEC.RU | Короткий путь к информации Скачано с sec.ru

адресом уже была добавлена ранее.

- «Ключ/Список ключей/Праздник/Временная зона/Правило с заданным именем уже существует». Задайте другое уникальное имя, объект с таким названием уже был добавлен ранее.
- «Название ключницы/ключа/временной зоны/правила доступа не может быть пустым и не должно превышать длину в 23 символа». Введено пустое или слишком длинное название. Измените его.
- «Название списка ключей не может быть пустым и не должно превышать длину в 31 символ». Введено пустое или слишком длинное название. Измените его.
- «Введите корректный номер помещения». Введён номер помещения не в формате «1-3 цифры + 0-1 буква».
- «Время начала интервала не может быть больше времени его окончания». При создании временной зоны для одного из интервалов время «от» превышает указанное время «до». Задайте корректные временные границы интервала.
- «Правило доступа не может быть пустым». Возникает при попытке сохранить правило на вкладке «Права доступа», для которого не выбраны ни ключ/списки ключей, ни соответствующие для них временные зоны.

SEC.RU | Короткий путь к информации Скачано с sec.ru

7. Контакты

ООО «Промышленная автоматика – контроль доступа»
Адрес: 603001, Нижний Новгород, ул. Керченская, д. 13, 4 этаж.

Система контроля и управления доступом «Sigur»
Сайт: www.sigur.com
По общим вопросам: info@sigur.com
Техническая поддержка: support@sigur.com
Телефон: +7 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260 12 93

SEC.RU | Короткий путь к информации
Скачано с sec.ru