

**Система контроля и управления  
доступом «Sigur».**

**Настройка взаимодействия с ключницами  
KeyGuard.**

## Оглавление:

<b>1. Введение .....</b>	<b>3</b>
<b>2. Используемые определения, обозначения и сокращения .....</b>	<b>3</b>
<b>3. Системные требования .....</b>	<b>3</b>
<b>4. Описание интеграции .....</b>	<b>3</b>
<b>5. Подключение и настройка .....</b>	<b>3</b>
5.1. Установка IP-параметров ключницы .....	3
5.2. Добавление ключницы в Sigur .....	4
5.2.1. Вкладка «Ключницы» .....	5
5.2.2. Вкладка «Списки ключей» .....	8
5.2.3. Вкладка «Праздники» .....	9
5.2.4. Вкладка «Временные зоны» .....	10
5.2.5. Вкладка «Права доступа» .....	10
5.3. Редактирование прав по доступу к ключам для объектов доступа. ....	12
5.4. Специальные логики доступа к ключам .....	13
5.4.1. Выдача ключей с санкции оператора.....	13
5.4.2. Выдача ключей с верификацией лица.....	14
5.4.3. Выдача ключей с верификацией лица и санкцией оператора .....	15
5.5. Логика работы с охранными зонами при выдаче/сдаче ключа.....	16
5.6. События от ключницы .....	17
5.7. Возможные сообщения об ошибках.....	17

# 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 системы Sigur](#)» и «[Руководство пользователя системы Sigur](#)».

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

# 2. Используемые определения, обозначения и сокращения

СКУД	Система контроля и управления доступом. Программно-аппаратный комплекс, предназначенный для осуществления функций контроля и управления доступом.
ПО	Программное обеспечение.
ТД	Точка доступа.

# 3. Системные требования

- Версия ПО Sigur 1.0.60.1 и выше
- Операционная система: согласно «[Руководство администратора системы Sigur](#)»
- Лицензирование: необходима лицензия по количеству ключей.

# 4. Описание интеграции

Настроенная интеграция позволяет:

- Добавлять ключницы KeyGuard в ПО Sigur
- Управлять списком ключей и правами сдачи/выдачи ключей конкретным пользователям
- При наличии настроенного взаимодействия с интегрированными в Sigur охраняемыми системами — автоматическая постановка на охрану/снятие с охраны зон при сдаче/выдаче ключей.

# 5. 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.

## 5.1. 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 брелков с ключами) при помощи специального ключа аварийной разблокировки. Затем — надо нажать кнопку Settings (на модуле заряда АКБ, расположен внутри основного блока с правого бока).

На вкладке «IP-настройки»:

## Настройка взаимодействия с ключницами KeyGuard

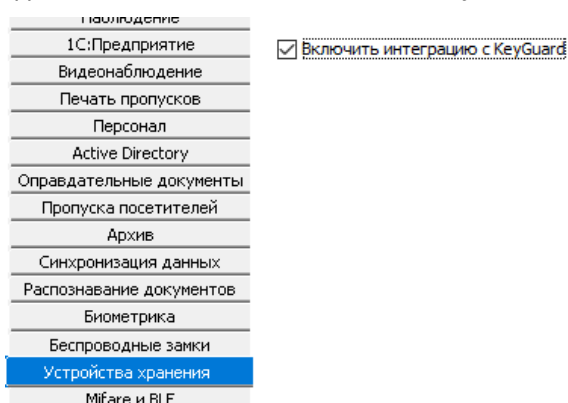
---

- IP Адрес. Поле для установки IP-адреса устройства
- IP Сервер. Указать 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. Оставить в значении по умолчанию, 8000.

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

## 5.2. Добавление ключницы в Sigur

Если это первое добавление ключницы, то сперва необходимо через меню «Файл — Настройки — Устройства хранения» указать, что необходимо «Включить интеграцию с KeyGuard» установкой одноимённой галочки и нажать кнопку «ОК».



**Рисунок 1. Включение интеграции с KeyGuard.**

Функционал будет доступен после перезапуска программы Клиент, о чём будет выведено соответствующее предупреждение.

На вкладке KeyGuard можно добавить необходимое количество ключниц, а так же сформировать настройки для каждой из них (управление списками ключей и временных интервалов на сдачу/выдачу ключей).

Вкладка KeyGuard состоит из следующих подвкладок — Ключницы, Списки ключей, Праздники, Временные зоны, Права доступа.

## Настройка взаимодействия с ключницами KeyGuard

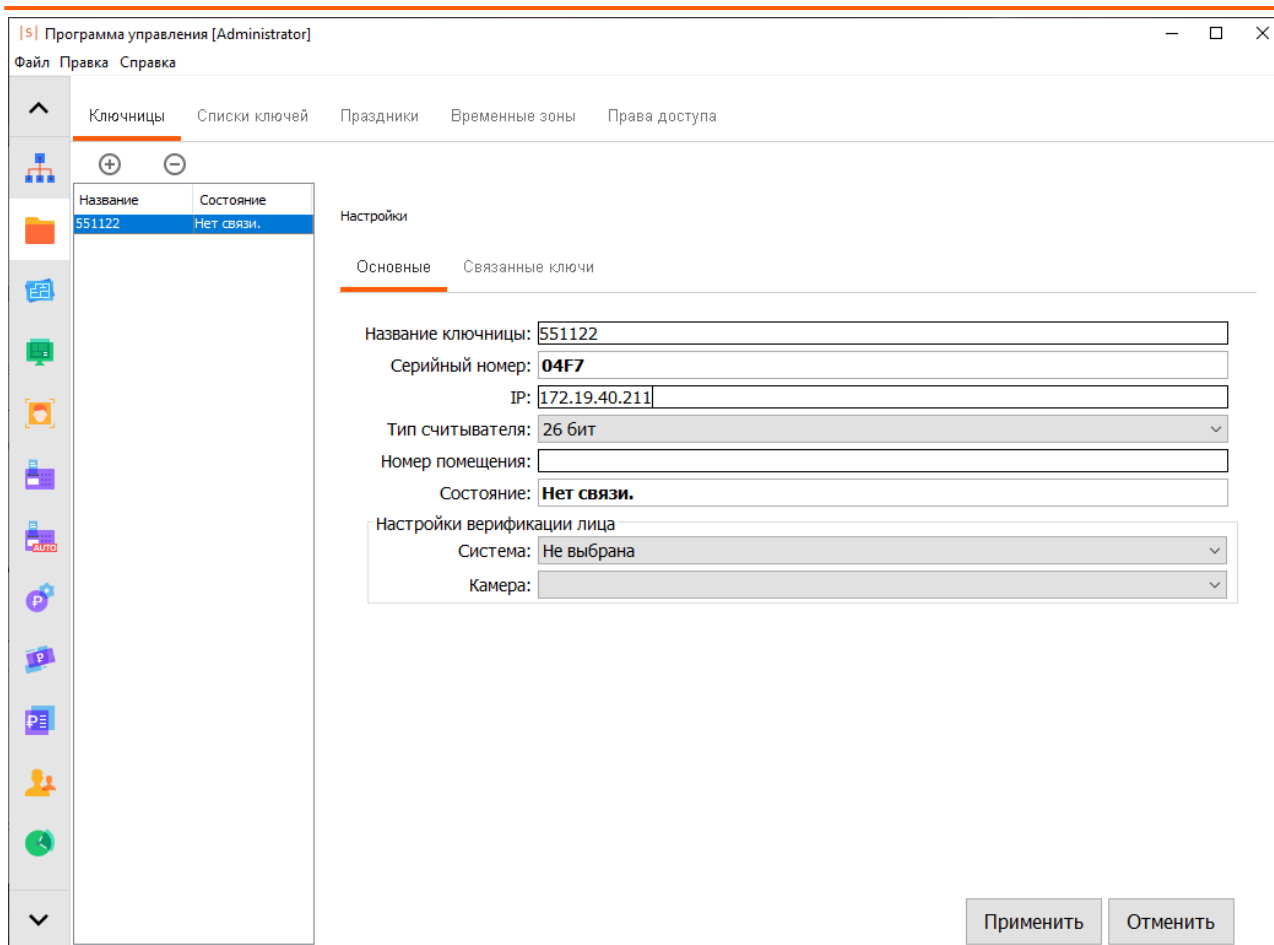


Рисунок 2. Вкладка KeyGuard.

### 5.2.1. 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:

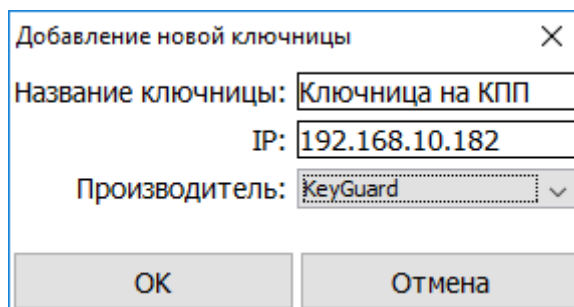


Рисунок 3. Окно добавления ключницы.

- «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 её через её меню настроек или планируемый.
- «Производитель».

## Настройка взаимодействия с ключницами KeyGuard

После указания всех параметров нажмите кнопку «ОК». В случае необходимости прерывания операции добавления нового устройства, нажмите кнопку «Отмена».

После успешного добавления новое устройство появится в списке ключниц. Для каждой ключницы доступны следующие общие параметры настройки:

Название	Состоя...
Ключница на КПП	Есть связь.
Ключница на 1-ом этаже	Нет связи.

Настройки

Основные    Связанные ключи

Название ключницы: Ключница на КПП

Серийный номер: 015F

IP: 192.168.11.44

Тип считывателя: 26 бит

Номер помещения: 23

Состояние: Есть связь.

Настройки верификации лица

Система: Не выбрана

**Рисунок 4. Основные настройки ключницы.**

- «Название ключницы». Строка для указания названия ключницы. Длина строки — от 1 до 23 символов.
- «Серийный номер». Не редактируемое поле, в котором отображается заводской номер устройства, автоматически считанный с ключницы, как только с ней появилась связь.
- «IP». Поле для указания «IP-адреса» ключницы.
- «Тип считывателя». Выпадающий список с выбором битности Wiegand 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. Строка 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 так же при перезапуске серверной службы 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 пункте [Выдача ключей с верификацией лица](#).

Для каждой из заведённых 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, а так же его можно вручную редактировать, добавляя новые ключи и удаляя более ненужные из имеющихся — для этого предназначены кнопки «+» и «-» соответственно на подвкладке «Связанные ключи».

## Настройка взаимодействия с ключницами KeyGuard

Основные Связанные ключи

(+) (-)

Название	Помещение
Ключ #0-8	
Проходная №1	1
Ключ #1-5	
Ключ #1-6	
Ключ #1-7	
Ключ #1-8	
Ключ #1-9	
Ключ #2-0	
Ключ #2-5	
Ключ #2-7	
Ключ #2-8	
Ключ #3-0	
Ключ #3-5	
Ключ #0-7	
Ключ #0-6	

Название ключа: Проходная №1

Номер помещения: 1

Вернуть до: 00:00

Допустимая задержка: 00:00

Номер таблетки iButton: 0xAf00001998791201

Охранные зоны: Проходная №1 ...

Рисунок 5. Окно связанных с ключницей ключей.

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

Добавление нового ключа X

Название ключа: Ключ №5

Номер помещения: 334

ОК Отмена

Рисунок 6. 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 попытке сдать ключ после указанного времени в полях «Вернуть до» и «Допустимая задержка»

- «Номер таблетки iButton». Поле для указания уникального идентификатора, встроенного в брелок ключницы.
- «Охранные зоны». По нажатию на кнопку «...» можно выбрать, какая из заведённых в систему охранных зон (при использовании интеграции с ОПС Болид «Орион» и Рубеж) будет ассоциирована с данным ключом. При задании ключу в соответствии охранной зоны возможна автоматическая постановка и снятие с охраны соответствующей зоны при сдаче или выдаче ключа. Более подробно логика и поведение системы описано в соответствующем 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».

### 5.2.2. 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.

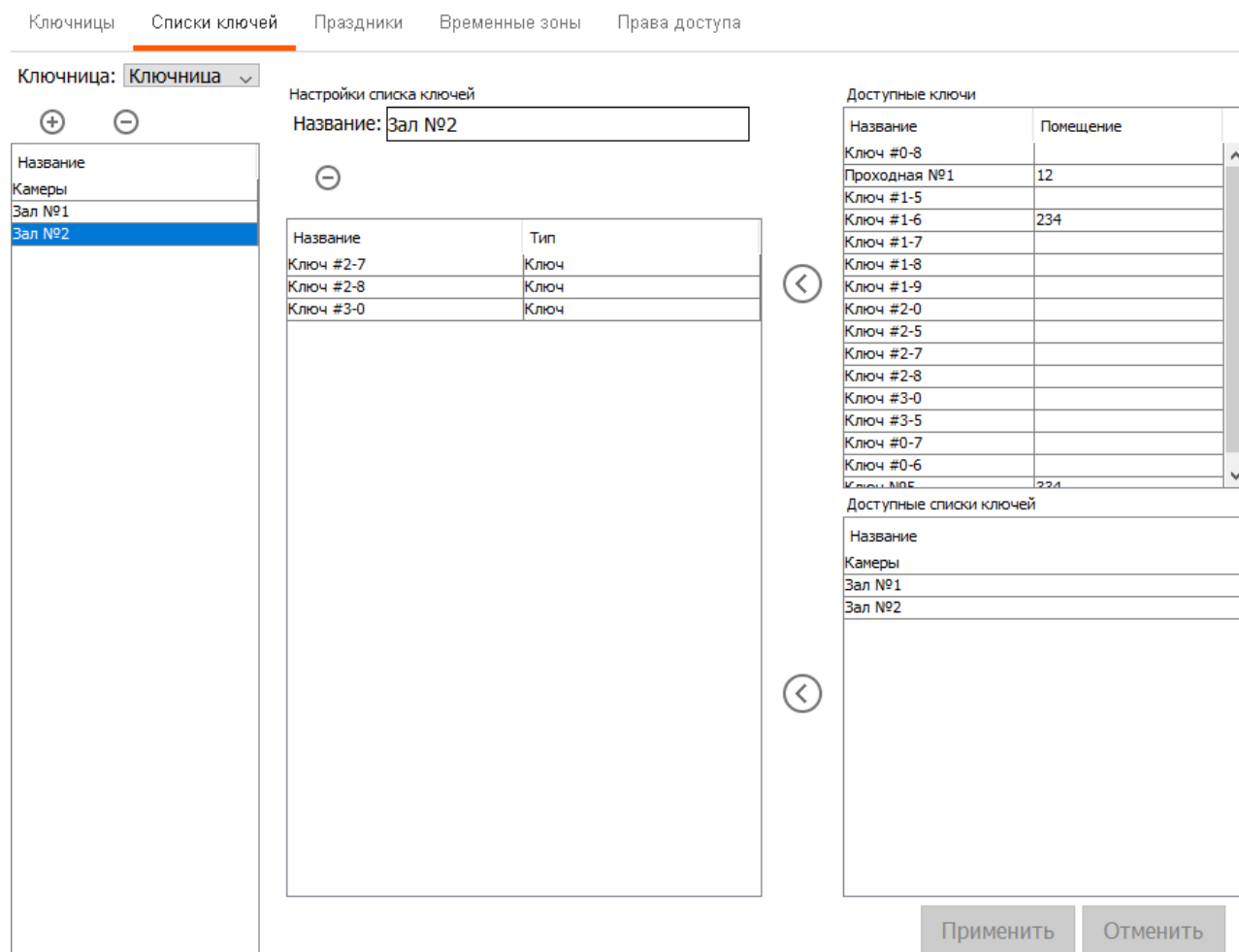


Рисунок 7. Вкладка Списки ключей.

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 заведёнными 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. По нажатию кнопки «ОК» новый список будет добавлен.



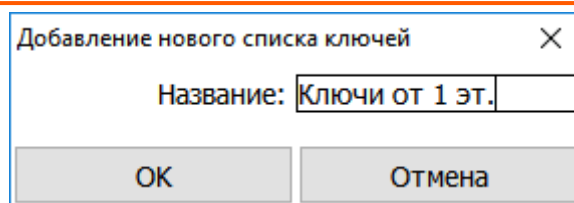


Рисунок 8. Добавление списка ключей.

Название списка ключей — строка длиной от 1 до 31 символа. 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, нажмите кнопку «Применить» для сохранения изменений. Для отмены всех внесённых изменений нажмите кнопку «Отменить».

### 5.2.3. 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-х дней в качестве праздничных.

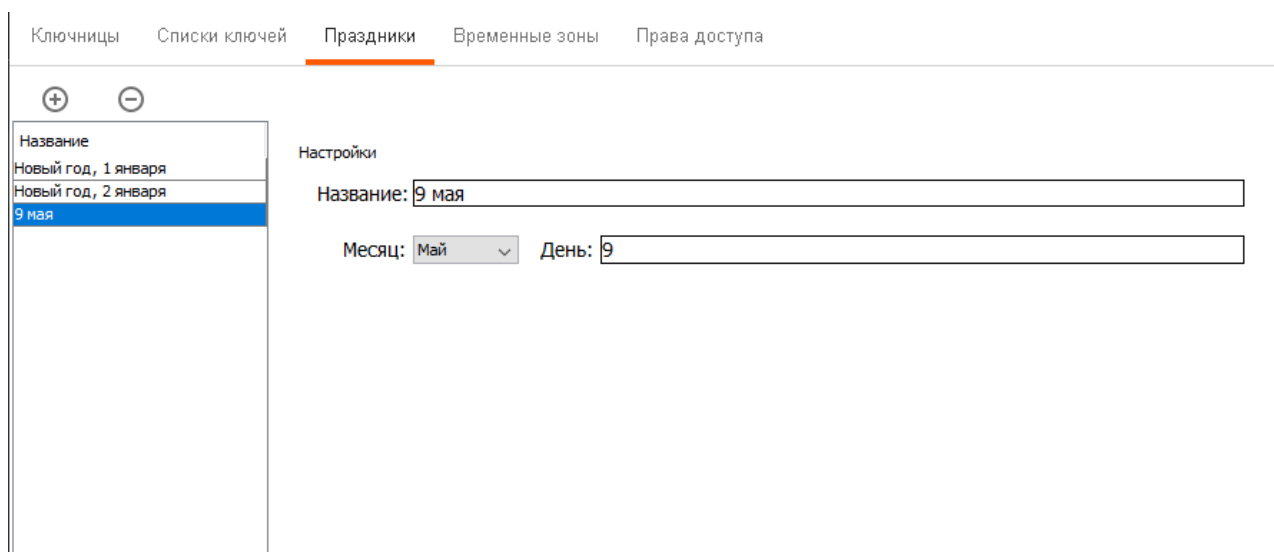


Рисунок 9. Вкладка Праздники.

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

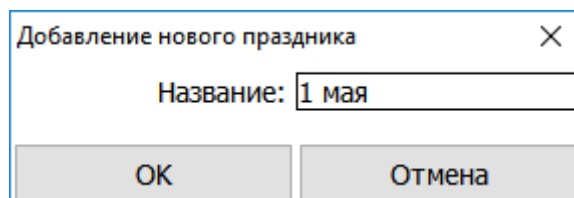


Рисунок 10. Добавление праздничного дня.

Для удаления выбранного — кнопку «-».

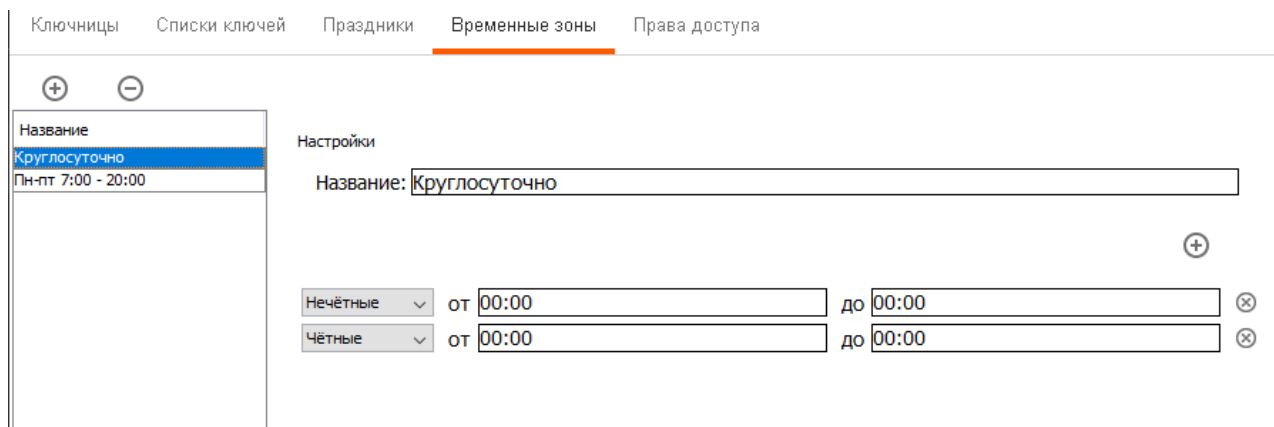
Для каждого созданного дня доступны следующие поля для редактирования:

## Настройка взаимодействия с ключницами KeyGuard

- «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.

### 5.2.4. Вкладка «Временные зоны»

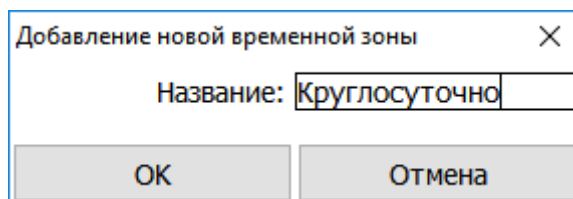
Предназначена для задания временных параметров разрешённых интервалов на выдачу/сдачу ключей. Создаваемые временные правила являются общими для всех ключниц, заносимых в систему.



The screenshot shows the 'Временные зоны' (Time Zones) tab. On the left, there is a list of zones with columns for 'Название' (Name) and 'Пн-пт 7:00 - 20:00'. The 'Круглосуточно' (24/7) zone is selected. On the right, the 'Настройки' (Settings) section is visible. It includes a 'Название:' field containing 'Круглосуточно'. Below this are two rows for 'Нечётные' (Odd) and 'Чётные' (Even) days. Each row has 'от' (from) and 'до' (to) time fields, both set to '00:00'. There are also '+' and 'x' icons for adding and deleting rules.

Рисунок 11. Вкладка Временные зоны.

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



The dialog box is titled 'Добавление новой временной зоны'. It has a close button 'X' in the top right corner. The 'Название:' field contains the text 'Круглосуточно'. At the bottom, there are two buttons: 'ОК' and 'Отмена'.

Рисунок 12. Добавление временной зоны.

Для удаления выбранного — 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-ти интервалов.

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

### 5.2.5. 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».

## Настройка взаимодействия с ключницами KeyGuard

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

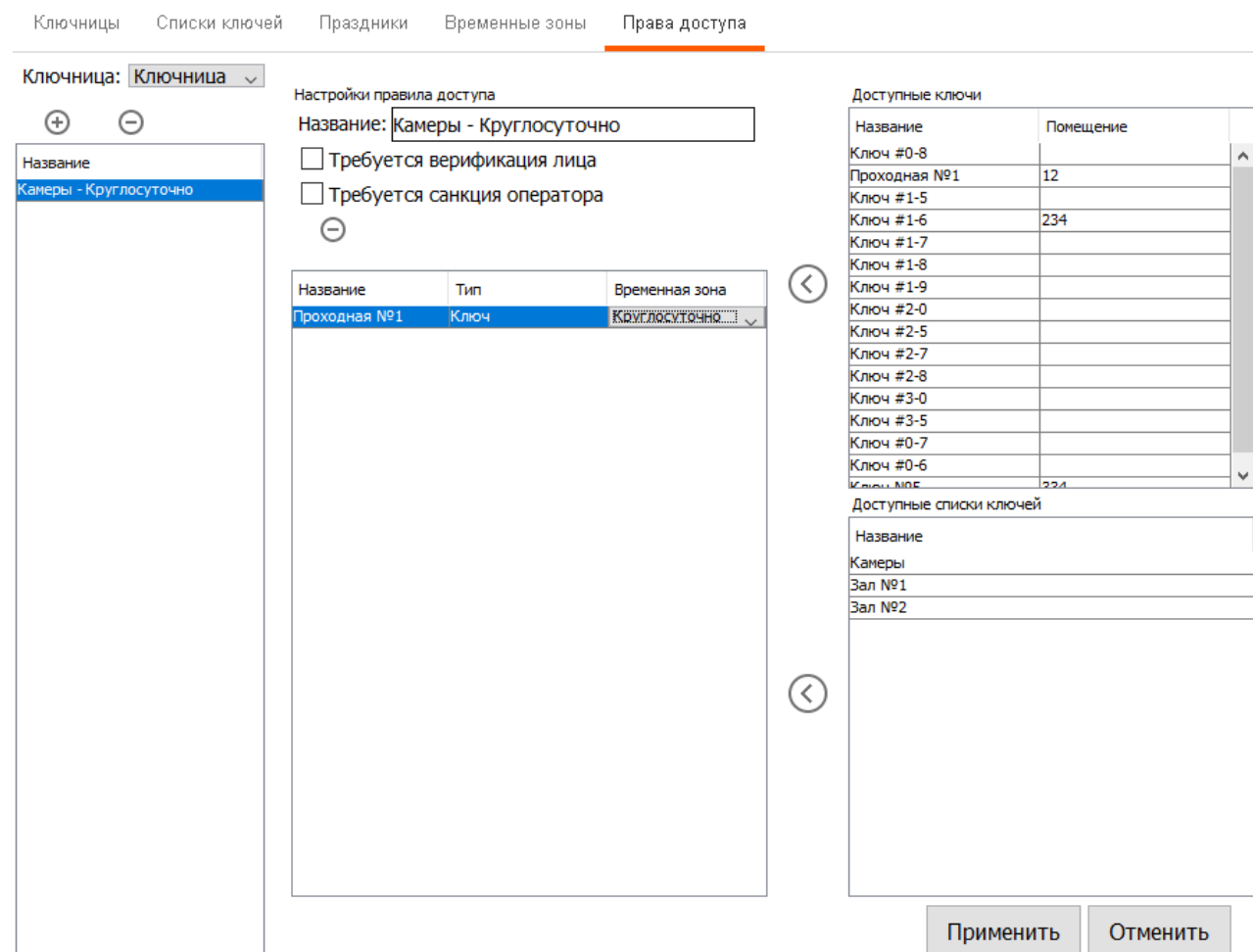


Рисунок 13. Вкладка Права доступа.

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 заведёнными 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 некое название. По нажатию кнопки «OK» оно будет добавлено. Название права доступа — строка длиной от 1 до 31 символа.

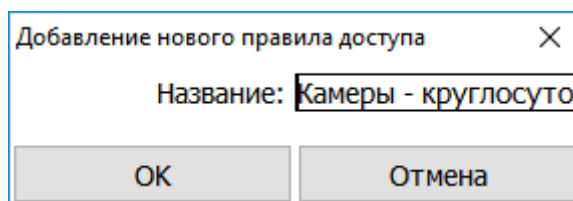


Рисунок 14. Добавление права доступа.

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. Подробнее можно ознакомиться в [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 так же 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».

### **5.3. 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.
- «PIN: » - пин-пароль для пользователя, при помощи которого он может идентифицировать себя на устройстве при вводе ID.
- «Правило доступа к ключам: » - указание правила на доступ к ключам конкретной ключницы, созданному заранее на вкладке «KeyGuard».

## Настройка взаимодействия с ключницами KeyGuard

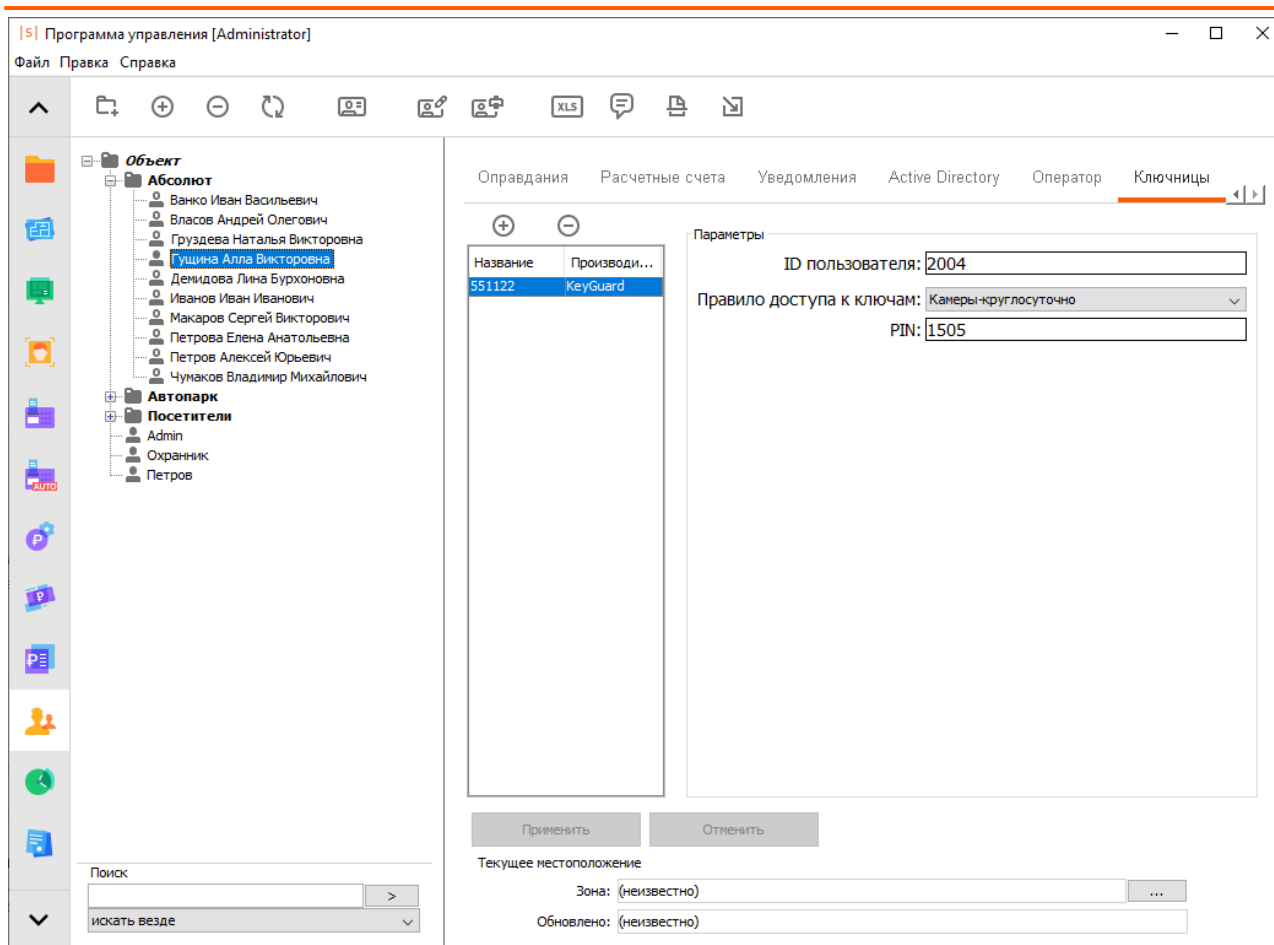


Рисунок 15. Задание права на доступ к ключам конкретной ключницы сотруднику.

## 5.4. 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](#)

### 5.4.1. Выдача ключей с санкции оператора

При включении данной логики после поднесения к считывателю ключницы карты и выбора ключей сотрудник подтверждает действия 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 «Sigur Reader EN» или «ACR 1252», либо запрещает её нажатием кнопки «Отмена».

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

## Настройка взаимодействия с ключницами KeyGuard

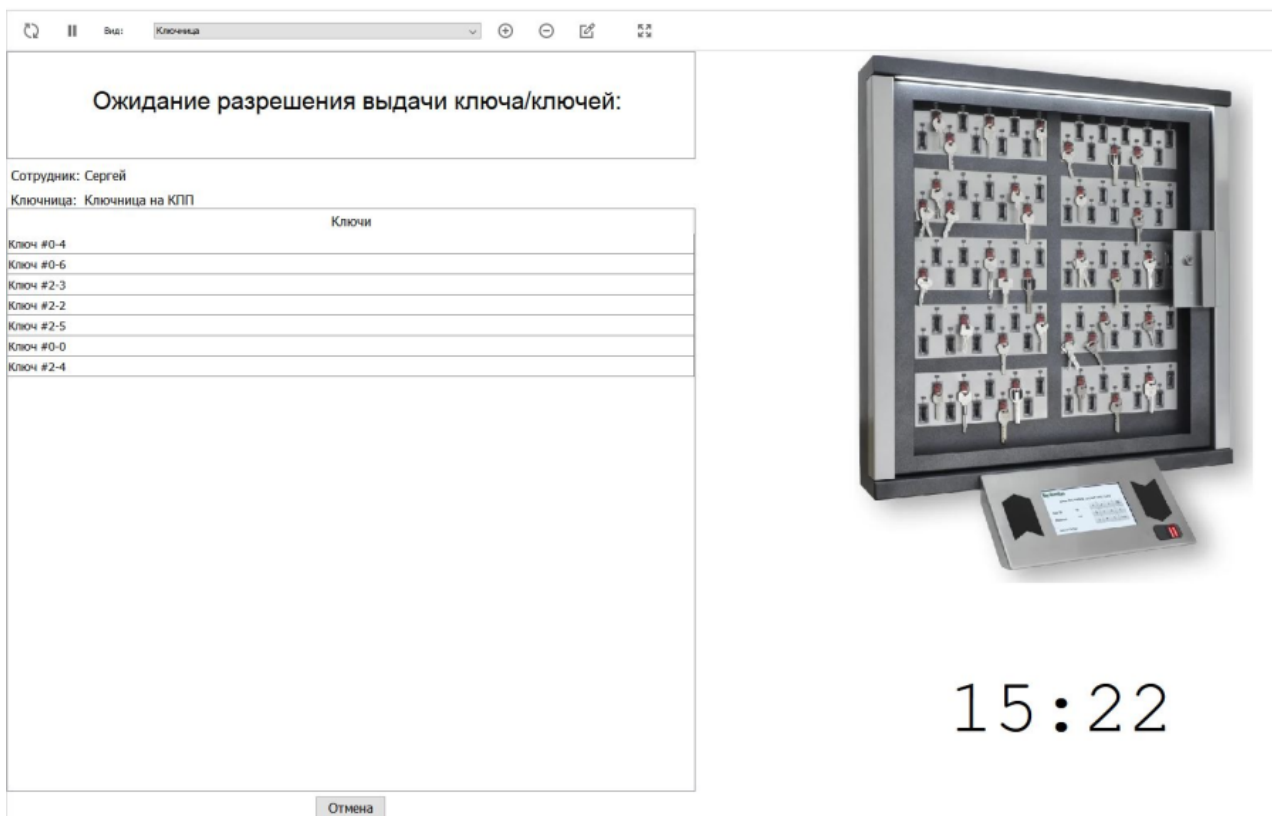
Настройки правила доступа

Название:

- Требуется верификация лица  
 Требуется санкция оператора

**Рисунок 16. Включение санкции оператора.**

2. 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.



**Рисунок 17. Вид наблюдения с добавленным на него объектом Ключница.**

### 5.4.2. Выдача ключей с верификацией лица

При включении данной логики после поднесения к считывателю ключницы карты и выбора ключей сотрудник подтверждает действия 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.

1. Добавление ip-камеры в систему и включение встроенной функции распознавания лиц (Подробнее в пункте Необходимые настройки при использованной функции распознавания лиц)
2. Привязка камеры к ключнице. Производится на вкладке «Ключницы» путём выбора камеры из выпадающего списка «Система»:

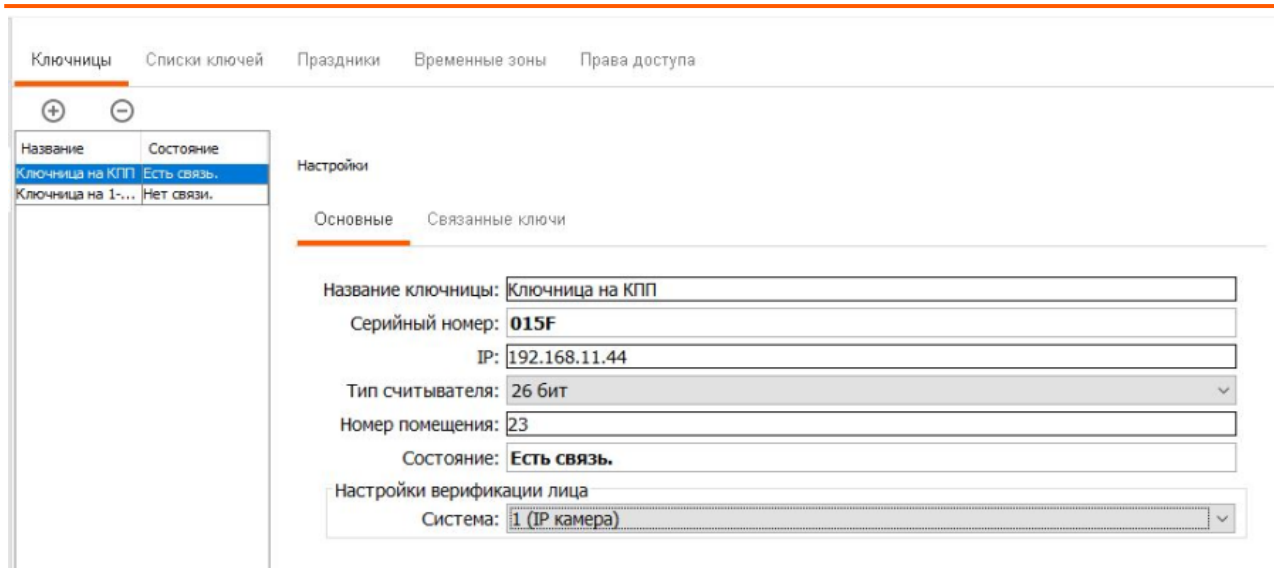


Рисунок 18. Привязка камеры к ключнице.

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

Настройки правила доступа

Название: Камеры-круглосуточно

Требуется верификация лица

Требуется санкция оператора

Рисунок 19. Включение верификации лица.

### 5.4.3. Выдача ключей с верификацией лица и санкцией оператора

При включении данной логики после поднесения к считывателю ключницы карты и выбора ключей сотрудник подтверждает действия 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» в наблюдении.

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.

Настройки правила доступа

Название: Камеры-круглосуточно

Требуется верификация лица

Требуется санкция оператора

Рисунок 20. Включение верификации лица и санкции оператора.

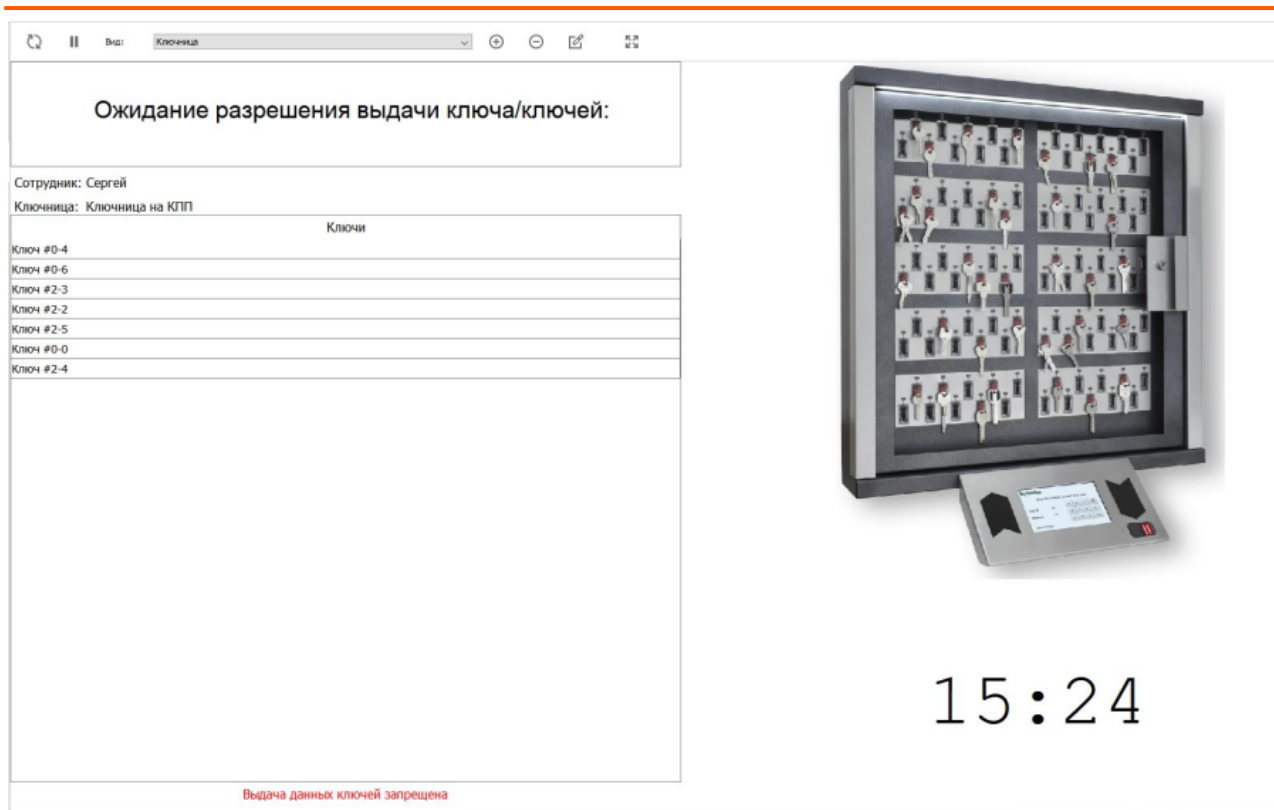


Рисунок 21. Тревожное сообщение в наблюдении.

### 5.5. 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 и «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 происходит 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 отображена тревога. Если все зоны успешно были сняты с охраны, на экране ключницы будет отображено «снято».

Если зоны на момент выдачи ключа не были поставлены на охрану, то ничего не происходит. На экране ключнице отображается, что зоны «сняты» с охраны.

Если зона/одна из группы зоны 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 учёта его в отображаемом на экране ключницы статусе.

Если же это последний, 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 отображена тревога. Если все зоны успешно были 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.

## **5.6. 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».

## **5.7. 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 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».

## Настройка взаимодействия с ключницами KeyGuard

---

- «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.

ООО «Промышленная автоматика – контроль доступа»  
603001, Нижний Новгород, БЦ ESQUIRE, ул. Советская, 18 Б.  
Техническая поддержка: +7 (800) 700 31 83, +7 (495) 665 30 48, +7 (831) 260 12 93

Система контроля и управления доступом «Sigur»

Сайт: [www.sigur.com](http://www.sigur.com)

Электронная почта: [info@sigur.com](mailto:info@sigur.com)